Lab - Implement Azure Private Link for Azure Virtual Desktop

Student lab manual

Lab dependencies

- An Azure subscription you will be using in this lab.
- A Microsoft Entra user account with the Owner role in the Azure subscription you will be using in this lab and with the permissions sufficient to join devices to the Entra tenant associated with that Azure subscription.
- The lab *Deploy host pools and session hosts by using the Azure portal (Entra ID)* completed

Estimated Time

40 minutes

Lab scenario

You have an existing Azure Virtual Desktop environment. You need to implement connection to the environment by using Azure Private Link.

Objectives

After completing this lab, you will be able to:

- implement Azure Private Link for Azure Virtual Desktop

Lab files

- None

Instructions

Exercise 1: Implement Azure Private Link for Azure Virtual Desktop

The main tasks for this exercise are as follows:

1. Re-register the Azure Virtual Desktop resource provider
2. Create an Azure virtual network subnet
3. Implement a private endpoint for connections to a host pool
4. Implement a private endpoint for feed download
5. Implement a private endpoint for initial feed discovery
6. Validate the private endpoint functionality
7. Allow public network access to a host pool and workspace

> **Note**: Azure Virtual Desktop has three workflows with three corresponding resource types to use with private endpoints. These workflows are:

- **Initial feed discovery**: allows RDP clients to discover all workspaces assigned to a user. To implement this workflow via a Private Link, you need to create a single private endpoint to the global sub-resource in any workspace that is part of your Azure Virtual Desktop deployment. However, regardless of the workspace you choose, there can be only a single private endpoint that provides this functionality per deployment
- **Feed download**: allows RDP clients to download connection details for all workspaces that host the current user's application groups. To implement this workflow via a Private Link, you need to create a private endpoint for the feed sub-resource for each workspace you intend make available via the private endpoint.
- **Connections to host pools**: allows RDP clients and session hosts to connect to a host pool. To implement this workflow via a Private Link, you need to create a private endpoint for the connection sub-resource for each host pool you intend make available via the private endpoint.

> **Note**: You can implement these workflows in the following arrangements:

- All parts of the connection - initial feed discovery, feed download, and remote session connections for clients and session hosts - use private routes.
- Feed download and remote session connections for clients and session hosts use private routes, but initial feed discovery uses public routes.
- Only remote session connections for clients and session hosts use private routes, but initial feed discovery and feed download use public routes.
- Both clients and session host VMs use public routes. Private Link isn't used in this scenario.

> **Note**: In this lab, you will implement the first arrangement.

Task 1: Re-register the Azure Virtual Desktop resource provider

> **Note**: Before you can use Private Link with Azure Virtual Desktop, you should re-register the **Microsoft.DesktopVirtualization** resource provider.

1. If needed, from the 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.

   > **Note**: Use the credentials of the `User1-` account listed on the Resources tab on the right side of the lab session window.

2. From the lab computer, in the web browser displaying the Azure portal, search for and select **Subscriptions**, on the **Subscriptions** page, select the Azure subscription you are using in this lab, and, in the vertical navigation menu, in the **Settings** section, select **Resource providers**.

3. On the **Resource providers** tab, in the search text box, enter **Microsoft.DesktopVirtualization**, in the list of results, select the small circle to the left of the **Microsoft.DesktopVirtualization** entry, and then select **Re-register**.

   > **Note**: Wait for the re-registration process to complete. This typically takes less than 1 minute.

Task 2: Create an Azure virtual network subnet

> **Note**: You could use an existing subnet of an Azure virtual network to implement private endpoints in the lab scenario, but it is a common practice to use a dedicated subnet for this purpose.

1. From the lab computer, in the web browser displaying the Azure portal, search for and select **Virtual networks** and, on the **Virtual networks** page, select **az140-vnet11e**.

2. On the **az140-vnet11e** page, in the **Settings** section of the vertical navigation menu, select **Subnets**.

3. On the **az140-vnet11e | Subnets** page, select **+ Subnet**.

4. In the **Add a subnet** pane, specify the following settings and select **Add** (leave other settings with their default values):

Setting	Value
Name	**pe-Subnet**
Starting address	**10.20.255.0**
Enable private subnet (no default outbound access)	disabled

Task 3: Implement a private endpoint for connections to a host pool

1. From the lab computer, in the web browser displaying the Azure portal, search for and select **Azure Virtual Desktop**, on the **Azure Virtual Desktop** page, in the **Manage** section of the vertical navigation menu, select **Host pools** and, on the **Azure Virtual Desktop | Host pools** page, select **az140-21-hp1**.

2. On the **az140-21-hp1** page, in the vertical navigation menu, in the **Settings** section, select **Networking**.

3. On the **az140-21-hp1 | Networking** page, select the **Private endpoint connections** tab and then, select **+ New private endpoint**.

4. On the **Basics** tab of the **Create a private endpoint** page, specify the following settings and select **Next: Resource >**:

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource group	**az140-11e-RG**
Name	**az140-11-pehp1**
Network Interface Name	**az140-11-pehp1-nic**
Region	the name of the Azure region where you deployed your Azure Virtual Desktop environment

5. On the **Resource** tab of the **Create a private endpoint** page, specify the following settings and select **Next: Virtual network >**:

Setting	Value
Target sub-resource	**connection**

6. On the **Virtual network** tab of the **Create a private endpoint** page, specify the following settings and select **Next: DNS >** (leave other settings with their default values):

Setting	Value
Virtual network	**az140-vnet11e (az140-11e-RG)**
Subnet	**pe-Subnet**
Network policy for private endpoints	**Disabled**
Private IP configuration	**Dynamically allocate IP address**

7. On the **DNS** tab of the **Create a private endpoint** page, specify the following settings and select **Next: Tags >**:

Setting	Value
Integrate with private DNS zone	**Yes**
Subscription	the name of the Azure subscription you are using in this lab
Resource group	**az140-11e-RG**

   > **Note**: This step will result in creation of a private DNS zone named **privatelink.wvd.microsoft.com**.

8. On the **Tags** tab of the **Create a private endpoint** page, select **Review + create**.

9. On the **Review + create** tab of the **Create a private endpoint** page, select **Create**.

   > **Note**: Wait for the deployment to complete. The deployment might take about 3 minutes.

   > **Note**: You would need to create a private endpoint for the connection sub-resource for each host pool you want to use with Private Link.

Task 4: Implement a private endpoint for feed download

1. From the lab computer, in the web browser displaying the Azure portal, search for and select **Azure Virtual Desktop** and, on the **Azure Virtual Desktop** page, select **Workspaces**.

2. On the **Azure Virtual Desktop | Workspaces** page, select **az140-21-ws1**.

3. On the **az140-21-ws1** page, in the vertical navigation menu, in the **Settings** section, select **Networking**.

4. On the **az140-21-ws1 | Networking** page, select the **Private endpoint connections** tab and then, select **+ New private endpoint**.

5. On the **Basics** tab of the **Create a private endpoint** page, specify the following settings and select **Next: Resource >**:

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource group	**az140-11e-RG**
Name	**az140-11-pefeeddwnld**
Network Interface Name	**az140-11-pefeeddwnld-nic**
Region	the name of the Azure region where you deployed your Azure Virtual Desktop environment

6. On the **Resource** tab of the **Create a private endpoint** page, specify the following settings and select **Next: Virtual network >**:

Setting	Value
Target sub-resource	**feed**

7. On the **Virtual network** tab of the **Create a private endpoint** page, specify the following settings and select **Next: DNS >** (leave other settings with their default values):

Setting	Value
Virtual network	**az140-vnet11e (az140-11e-RG)**
Subnet	**pe-Subnet**
Network policy for private endpoints	**Disabled**
Private IP configuration	**Dynamically allocate IP address**

8. On the **DNS** tab of the **Create a private endpoint** page, specify the following settings and select **Next: Tags >**:

Setting	Value
Integrate with private DNS zone	**Yes**
Subscription	the name of the Azure subscription you are using in this lab
Resource group	**az140-11e-RG**

> **Note**: This step will leverage the private DNS zone named **privatelink.wvd.microsoft.com** you created in the previous task.

9. On the **Tags** tab of the **Create a private endpoint** page, select **Review + create**.

10. On the **Review + create** tab the **Create a private endpoint** page, select **Create**.

    > **Note**: Do not wait for the deployment to complete but instead proceed to the next task. The deployment might take about 1 minute.

    > **Note**: You would need to a create private endpoint for the feed sub-resource for each workspace you want to use with Private Link.

Task 5: Implement a private endpoint for initial feed discovery

1. From the lab computer, in the web browser displaying the Azure portal, search for and select **Azure Virtual Desktop** and, on the **Azure Virtual Desktop** page, select **Workspaces**.

2. On the **Azure Virtual Desktop | Workspaces** page, select **az140-21-ws1**.

3. On the **az140-21-ws1** page, in the vertical navigation menu, in the **Settings** section, select **Networking**.

4. On the **az140-21-ws1 | Networking** page, select the **Private endpoint connections** tab and then, select **+ New private endpoint**.

5. On the **Basics** tab of the **Create a private endpoint** page, specify the following settings and select **Next: Resource >**:

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource group	**az140-11e-RG**
Name	**az140-11-pefeeddisc**
Network Interface Name	**az140-11-pefeeddisc-nic**
Region	the name of the Azure region where you deployed your Azure Virtual Desktop environment

6. On the **Resource** tab of the **Create a private endpoint** page, specify the following settings and select **Next: Virtual network >**:

Setting	Value
Target sub-resource	**global**

7. On the **Virtual network** tab of the **Create a private endpoint** page, specify the following settings and select **Next: DNS >** (leave other settings with their default values):

Setting	Value
Virtual network	**az140-vnet11e (az140-11e-RG)**
Subnet	**pe-Subnet**

Setting	Value
Network policy for private endpoints	**Disabled**
Private IP configuration	**Dynamically allocate IP address**

8. On the **DNS** tab of the **Create a private endpoint** page, specify the following settings and select **Next: Tags >**:

Setting	Value
Integrate with private DNS zone	**Yes**
Subscription	the name of the Azure subscription you are using in this lab
Resource group	**az140-11e-RG**

> **Note**: This step will leverage the private DNS zone named **privatelink.wvd.microsoft.com** you created in one of the earlier task.

9. On the **Tags** tab of the **Create a private endpoint** page, select **Review + create**.

10. On the **Review + create** tab the **Create a private endpoint** page, select **Create**.

> **Note**: Do not wait for the deployment to complete but instead proceed to the next task. The deployment might take about 1 minute.

> **Note**: You would need to a create private endpoint for the feed sub-resource for each workspace you want to use with Private Link.

Task 6: Validate the private endpoint functionality

> **Note**: By default, connectivity to Azure Virtual Desktop workspaces and host pools is allowed from public networks. You will start by changing the default settings and enforcing private access.

1. From the lab computer, in the web browser displaying the Azure portal, search for and select **Azure Virtual Desktop** and, on the **Azure Virtual Desktop** page, select **Workspaces**.
2. On the **Azure Virtual Desktop | Workspaces** page, select **az140-21-ws1**.
3. On the **az140-21-ws1** page, in the vertical navigation menu, in the **Settings** section, select **Networking**.
4. On the **az140-21-ws1 | Networking** page, on the **Public access** tab, select the option **Disable public access and use private access**, and then select **Save**.
5. From the lab computer, in the web browser displaying the Azure portal, search for and select **Azure Virtual Desktop**, on the **Azure Virtual Desktop** page, in the **Manage** section of the vertical navigation menu, select **Host pools** and, on the **Azure Virtual Desktop | Host pools** page, select **az140-21-hp1**.
6. On the **az140-21-hp1** page, in the vertical navigation menu, in the **Settings** section, select **Networking**.
7. On the **az140-21-hp1 | Networking** page, on the **Public access** tab, select the option **Disable public access and use private access**, and then select **Save**.

> **Note**: To validate the private endpoint functionality, an RDP client needs to be connected to a network that has private connectivity to the Azure virtual network containing subnet hosting the private endpoints you created earlier in this lab. To simulate this scenario, you will create another subnet in the same virtual network used to create private endpoints and deploy an Azure VM running Windows 11 into that subnet.

1. From the lab computer, in the web browser displaying the Azure portal, search for and select **Virtual networks** and, on the **Virtual networks** page, select **az140-vnet11e**.

2. On the **az140-vnet11e** page, in the **Settings** section of the vertical navigation menu, select **Subnets**.

3. On the **az140-vnet11e | Subnets** page, select **+ Subnet**.

4. In the **Add a subnet** pane, specify the following settings and select **Add** (leave other settings with their default values):

Setting	Value
Name	**client-Subnet**
Starting address	**10.20.2.0**
Enable private subnet (no default outbound access)	disabled

5. From the lab computer, in the web browser displaying the Azure portal, search for and select **Virtual machines**, on the **Virtual machines** page, select **+ Create** and, in the drop-down list, select **Azure virtual machine**.

6. On the **Basics** tab of the **Create a virtual machine** page, specify the following settings (leave other settings with their default values) and select **Next: Disks >**:

Setting	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource group	the name of a new resource group **az140-111e-RG**
Virtual machine name	**az140-111e-vm0**
Region	the name of the Azure region where you deployed your Azure Virtual Desktop environment
Availability options	**No infrastructure redundancy required**
Security type	**Standard**
Image	**Windows 11 Pro, version 22H2 - x64 Gen2**
Size	**Standard DC2s_v3**
Username	any valid user name of your choice
Password	any valid password of your choice

Setting	Value
Public inbound ports	**None**
Licensing	enable the checkbox

> **Note**: The password should be at least 12 characters in length and consist of a combination of lower-case characters, upper-case characters, digits, and special characters. For details, refer to the information about the password requirements when creating an Azure VM.

7. On the **Disks** tab of the **Create a virtual machine** page, set the **OS disk type** to **Standard HDD (locally-redundant storage)** and select **Next: Networking >**.

8. On the **Networking** tab of the **Create a virtual machine** page, specify the following settings (leave other settings with their default values):

Setting	Value
Virtual network	**az140-vnet11e**
Subnet	*a new subnet named* **client-Subnet**
Public IP	**(new) az140-111e-vm0-ip**
NIC network security group	**Advanced**

9. On the **Networking** tab of the **Create a virtual machine** page, next to the **Configure network security group** drop-down list, select **Create new**.

10. On the **Create network security group** page, delete the pre-created inbound rule **1000: default-allow-rdp** and then select **+ Add an inbound rule**.

11. In the **Add inbound security rule** pane, in the **Source** drop-down list, select **My IP address** to identify the public IP address representing your connection to the internet.

12. In the **Add inbound security rule** pane, specify the following settings (leave other settings with their default values), and then select **Add**:

Setting	Value
Source	**IP Addresses**
Source IP addresses/CIDR ranges	leave unchanged (this should still contain your public IP address)
Source port ranges	*
Destination	**Any**
Service	**RDP**
Action	**Allow**
Priority	**300**

Setting	Value
Name	**AllowCidrBlockRDPInbound**

13. Back on the **Create network security group** page, select **OK**.

14. Back on the **Networking** tab of the **Create a virtual machine** page, select **Next: Management >**:

15. On the **Management** tab of the **Create a virtual machine** page, specify the following settings (leave other settings with their default values), and then select **Next: Monitoring >**:

Setting	Value
Enable basic plan for free	disabled
Patch orchestration options	**Manual updates**

16. On the **Monitoring** tab of the **Create a virtual machine** page, specify the following settings (leave other settings with their default values), and then select **Review + create**:

Setting	Value
Boot diagnostics	**Disable**

17. On the **Review + create** tab the **Create a private endpoint** page, select **Create**.

> **Note**: Wait for the deployment to complete. The deployment might take about 5 minutes.

18. From the lab computer, in the web browser displaying the Azure portal, search for and select **Virtual machines**, on the **Virtual machines** page, select **az140-111e-vm0**.

19. On the **az140-111e-vm0** page, select **Connect** and, in the drop-down menu, select **Connect**.

20. On the **az140-111e-vm0 | Connect** page, in the **Most common** section, select **Download RDP file**.

21. In the **Download** pop-up window, select **Keep** and then select **Open file**.

22. When prompted, select **Connect** and then, in the **Windows Security** dialog box, enter the user name and password you specified when deploying the Azure VM.

23. When prompted for confirmation, select **Connect** again.

24. Within the Remote Desktop session to **az140-111e-vm0**, choose and accept your preferred privacy settings.

25. Within the Remote Desktop session to **az140-111e-vm0**, start Microsoft Edge, navigate to the Connect to Azure Virtual Desktop with the Remote Desktop client for Windows page, scroll down to the section **Download and install the Remote Desktop client (MSI)**, and select the Windows 64-bit link.

26. Open File Explorer, navigate to the **Downloads** folder, and launch the installation of the newly downloaded MSI file.

27. When prompted, accept the terms of the licensing agreement and choose the option to **Install for all users of this machine**. If prompted, accept the User Account Control prompt to proceed with the installation.

28. Once the installation completes, ensure that the **Launch Remote Desktop when setup exits** checkbox is selected and select **Finish** to start the Microsoft Remote Desktop client.

29. Within the Remote Desktop session to **az140-111e-vm0**, in the **Remote Desktop** client window, select **Subscribe** and, when prompted, sign in with the credentials of the `User2` Entra ID user account which you can locate on the **Resources** tab in the right pane of the lab interface window.

    > **Note**: Select the user account which is the member of the Entra group with the **AVD-RemoteApp** prefix.

30. Ensure that the **Remote Desktop** page displays four icons, including Command Prompt, Microsoft Word, Microsoft Excel, Microsoft PowerPoint.

31. Double-click the Command Prompt icon.

32. When prompted to sign in, in the **Windows Security** dialog box, enter the password of the same Microsoft Entra user account you used to connect to the target Azure Virtual Desktop environment.

33. Verify that a **Command Prompt** window appears shortly afterwards.

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

    > **Note**: Optionally, you might consider attempting to subscribe to the feed and connect to The Azure Virtual Desktop workspace from the lab computer to validate that this connection will fail.

    > **Note**: To minimize charges associated with running the lab environment, you will stop and deallocate the newly provisioned Azure VM.

35. Switch to the console session to the lab computer, in the web browser displaying the Azure portal, on the **az140-111e-vm0** page, select **Overview** and then, in the toolbar, select **Stop**.

36. In the **Stop this virtual machine** pop-up window, seletct **Yes**.

Task 7: Allow public network access to a host pool and workspace

> **Note**: To eliminate impact on other labs that use the same Azure Virtual Desktop environment, you will revert the changes applied in the previous task and allow public network access to the host pool and workspace that are part of the Azure Virtual Desktop environment.

1. From the lab computer, in the web browser displaying the Azure portal, search for and select **Azure Virtual Desktop** and, on the **Azure Virtual Desktop** page, select **Workspaces**.
2. On the **Azure Virtual Desktop | Workspaces** page, select **az140-21-ws1**.
3. On the **az140-21-ws1** page, in the vertical navigation menu, in the **Settings** section, select **Networking**.
4. On the **az140-21-ws1 | Networking** page, on the **Public access** tab, select the option **Enable public access from all networks**, and then select **Save**.

5. From the lab computer, in the web browser displaying the Azure portal, search for and select **Azure Virtual Desktop**, on the **Azure Virtual Desktop** page, in the **Manage** section of the vertical navigation menu, select **Host pools** and, on the **Azure Virtual Desktop | Host pools** page, select **az140-21-hp1**.
6. On the **az140-21-hp1** page, in the vertical navigation menu, in the **Settings** section, select **Networking**.
7. On the **az140-21-hp1 | Networking** page, on the **Public access** tab, select the option **Enable public access from all networks**, and then select **Save**.