Seneca

CPO550 - Lab 06:

Implement Azure Private Link for AVD

Student Lab Manual

Fall 2026

Lab scenario

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

Objectives

- Implement Azure Private Link for Azure Virtual Desktop

Lab requirements

- Lab 01: *Deploy host pools and session hosts by using the Azure portal*

Submission Requirements

Take a screenshot whenever you see the camera icon ( ) alongside task instructions. For better visibility, don't take screenshots in the dark mode.
Compile all screenshots into a single Word (.docx) or PDF file in the order of each task and provide a brief explanation of the significance of each screenshot. Underline or highlight all important information as shown in the provided sample screenshots at the end of this lab manual. Ensure your Odl_user account is clearly visible and underlined in every screenshot. Do not include the lab instructions in your submission.

Important: Use the provided template in the Blackboard to submit your lab reports.

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
8. Summary Questions

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 your local computer, start a web browser, navigate to the Azure portal and sign in by providing credentials of your **Odl_user** account.
2. From 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 Azure portal, search for and select **Virtual networks** and select **cpoF67-vnet11e**.
2. On the **cpoF67-vnet11e** page, in the **Settings** section of the vertical navigation menu, select **Subnets**.
3. On the **cpoF67-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 Azure portal, search for and select **Azure Virtual Desktop**, in the **Manage** section select **Host pools** and, select **<sName>-cpoF67-hp1**.
2. On the **<sName>-cpoF67-hp1** page, in the **Settings** section, select **Networking**.
3. 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

Setting	Value
Resource group	**<sName>-cpoF67-11e-RG**
Name	**<sName>-cpoF67-pehp1**
Network Interface Name	**<sName>-cpoF67-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	**cpoF67-vnet11e (<sName>-cpoF67-11e-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	**<sName>-cpoF67-11e-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 **Next : 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 Azure portal, search for and select **Azure Virtual Desktop** and select **Workspaces**.
2. On the **Workspaces** page, select **<sName>-cpoF67-21-ws1**.
3. On the **<sName>-cpoF67-21-ws1** page, in the **Settings** section, select **Networking**.
4. On the **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	**<sName>-cpoF67-11e-RG**
Name	**<sName>-pefeeddwnld**
Network Interface Name	**<sName>-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	**cpoF67-vnet11e (<sName>-cpoF67-11e-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	**<sName>-cpoF67-11e-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 **Next : 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 Azure portal, search for and select **Azure Virtual Desktop** and then select **Workspaces**.
2. On the **Workspaces** page, select **<sName>-cpoF67-21-ws1**.
3. On the **<sName>-cpoF67-21-ws1** page, in the **Settings** section, select **Networking**.
4. On the **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	**<sName>-cpoF67-11e-RG**
Name	**<sName>-pefeeddisc**
Network Interface Name	**<sName>-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	**cpoF67-vnet11e (<sName>-cpoF67-11e-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	**<sName>-cpoF67-11e-RG**

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

9. On the **Tags** tab of the **Create a private endpoint** page, select **Next : 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 global sub-resource for each workspace you want to use with Private Link.
Note: For the network changes to take effect, you need to restart the session hosts in the target host pool.

11. From the Azure portal, navigate to the **Azure Virtual Desktop** page, in the **Manage** section select **Host pools** and, on the **Host pools** page, select **<sName>-cpoF67-hp1**.
12. On the **<sName>-cpoF67-hp1** page, in the **Manage** section select **Session hosts**.
13. In the list of session hosts, select all checkboxes to the left of each session host and then select **Restart** in the toolbar.

Note: Wait until all session hosts are in the **Running** state.

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 Azure portal, search for and select **Azure Virtual Desktop** and then select **Workspaces**.
2. On the **Workspaces** page, select **<sName>-cpoF67-21-ws1**.
3. On the **<sName>-cpoF67-21-ws1** page, in the **Settings** section, select **Networking**.
4. On the **Networking** page, on the **Public access** tab, select the option **Disable public access and use private access**, and then select **Save**.
5. From the Azure portal, select **Azure Virtual Desktop**, select **Host pools** and then, select **<sName>-cpoF67-hp1**.
6. On the **<sName>-cpoF67-hp1** page, in the vertical navigation menu, in the **Settings** section, select **Networking**.
7. On the **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.

8. From the Azure portal, search for and select **Virtual networks** and, on the **Virtual networks** page, select **cpoF67-vnet11e**.
9. On the **cpoF67-vnet11e** page, in the **Settings** section of the vertical navigation menu, select **Subnets**.
10. On the **cpoF67-vnet11e | Subnets** page, select **+ Subnet**.
11. 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

12. From 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**.
13. 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 **cp0F67-111e-RG**
Virtual machine name	**<sName>-client-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 24H2 - x64 Gen2**
Size	**Standard D2s_v3**
Username	**Adminuser**
Password	Any valid password of your choice
Public inbound ports	**None**
Licensing	Enable the checkbox

14. 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 >**.
15. 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	**cpoF67-vnet11e**
Subnet	**client-Subnet**
Public IP	**(new) <sName>-client-vm0-ip**
NIC network security group	**Advanced**

16. On the **Networking** tab of the **Create a virtual machine** page, next to the **Configure network security group** drop-down list, select **Create new**.
17. On the **Create network security group** page, delete the pre-created inbound rule **1000: default-allow-rdp** and then select **+ Add an inbound rule**.
18. 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.
19. 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**
Name	**AllowCidrBlockRDPInbound**

20. Back on the **Create network security group** page, select **OK**.
21. Back on the **Networking** tab of the **Create a virtual machine** page, select **Next : Management >**:
22. 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
Patch orchestration options	**Manual updates**

23. 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**

24. On the **Review + create** tab of the **Create a virtual machine** page, select **Create**.

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

25. From the Azure portal, search for and select **Virtual machines**, on the **Virtual machines** page, select **<sName>-client-vm0** and connect to it using the **RDP** file.
26. When prompted, enter the user name and password you specified when deploying the Azure VM.
27. Within the Remote Desktop session 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.
28. Open File Explorer, navigate to the **Downloads** folder, and launch the installation of the newly downloaded MSI file.

29. 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.
30. 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.
31. Within the Remote Desktop session to **<sName>-client-vm0**, in the **Remote Desktop** client window, select **Subscribe** and, when prompted, sign in with the credentials of the **cpoF67-User2** Entra ID user account.
32. Ensure that the **Remote Desktop** page displays four icons, including Command Prompt, Microsoft Word, Microsoft Excel, Microsoft PowerPoint.
33. Double-click the Command Prompt icon.
34. 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.
35. Verify that a **Command Prompt** window appears shortly afterwards.
36. Type **Whoami/upn** and press the Enter key.
37. Type **Ipconfig/all** and pres the Enter key.
38. At the Command Prompt, type **logoff** and press the **Enter** key to log off from the current Remote App session.
39. From your local computer, open a new incognito tab or from a different browser, type https://client.wvd.microsoft.com/arm/webclient/index.html and login with **cpoF67-User2** credentials.
40. A message validates that the connection failed.

Note: Don't close this tab. You will refresh it after task 7.

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

1. From your local computer, in the Azure portal, search for and select **Azure Virtual Desktop** and select **Workspaces**.
2. On the **Workspaces** page, select **<sName>-cpoF67-21-ws1**. In the **Settings** section, select **Networking**.
3. On the **Networking** page, on the **Public access** tab, select the option **Enable public access from all networks**, and then select **Save**.
4. From the **Azure Virtual Desktop** page, select **Host pools** and then select **<sName>-cpoF67-hp1**.
5. On the **<sName>-cpoF67-hp1** page, in the vertical navigation menu, in the **Settings** section, select **Networking**.
6. On the **<sName>-cpoF67-hp1 | Networking** page, on the **Public access** tab, select the option **Enable public access from all networks**, and then select **Save**.
7. Refresh, or redo the task 6, step 39.
8. You should see the remote apps icons.

Note: This time, you should see the remote application icons.

Task 8: Summary Questions

Please answer the following questions in *your own words*, and submit with your lab report:

Question 1: Why is Azure Private Link used with Azure Virtual Desktop, and how does it improve the security of the environment compared to public access?

Question 2: Azure Virtual Desktop uses three workflows with Private Link (initial feed discovery, feed download, and host pool connections). What is the purpose of each workflow and which private endpoint sub-resource is used for each one?

Question 3: Why did the connection in Task 6, step 40 fail?

Lab Reflection: *(Note: Answer based on your own personal experience doing the lab; do not use general or textbook statements)*

Question 4: After completing this lab, what challenges did you encounter while implementing Azure Private Link for Azure Virtual Desktop, and how did the lab help you better understand how private connectivity improves the security and accessibility of cloud resources? Explain your experience and what you learned.

Important Lab Cleanup Instructions after you have completed the lab.

Reducing Azure Credit Usage

Reduce the cost of your Azure credit by deleting resources that are no longer required.

Step 1 — Delete the Lab Resource Group

1. Open the **Azure Portal**.
2. Navigate to **Resource Groups**.
3. Locate the resource group created for this lab:
    - **cp0F67-111e-RG**
4. Select the resource group and **delete it**.

Step 2 — Remove Extra Session Hosts

1. Navigate to **yourName-cpoF67-hp1 Host Pool**.
2. Select **Session Hosts**.
3. Locate and select the following session hosts:
    - **yourName-sh-1**
    - **yourName-sh-2**
4. Remove these two session hosts.

Note: After completing this step, the session host list should show only:

- **yourName-sh-0**

Step 3 — Delete the Corresponding Virtual Machines

1. Go to **Virtual Machines** in the Azure portal.
2. Locate the following virtual machines:
    - **yourName-sh-1**
    - **yourName-sh-2**
3. Select both VMs and **delete them**.

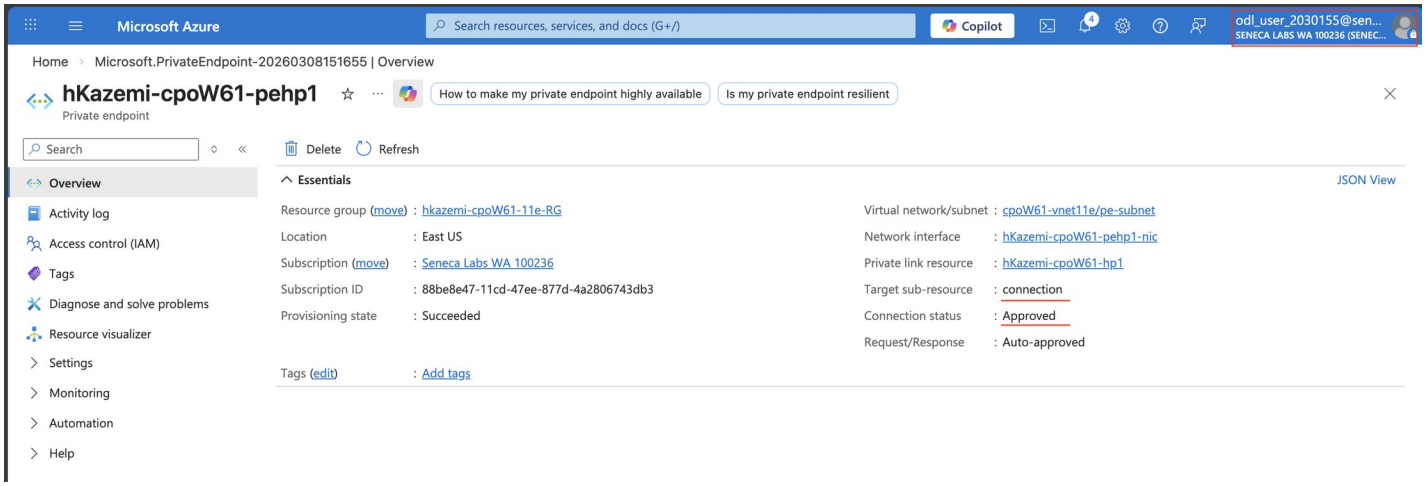
Final Step — Stop Remaining Virtual Machines

To further minimize your Azure costs, **stop all remaining virtual machines**.
Restart them **only when needed for the next lab**.

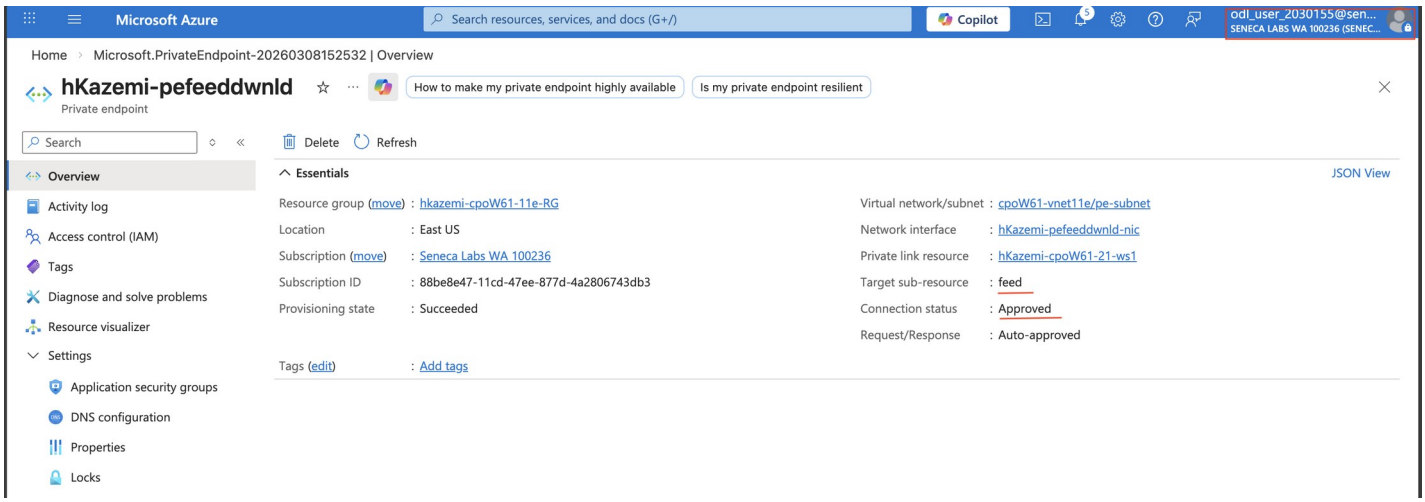
Sample Screenshots

Please ensure that all marked information in the samples is included, clearly visible, and underlined in your screenshots.

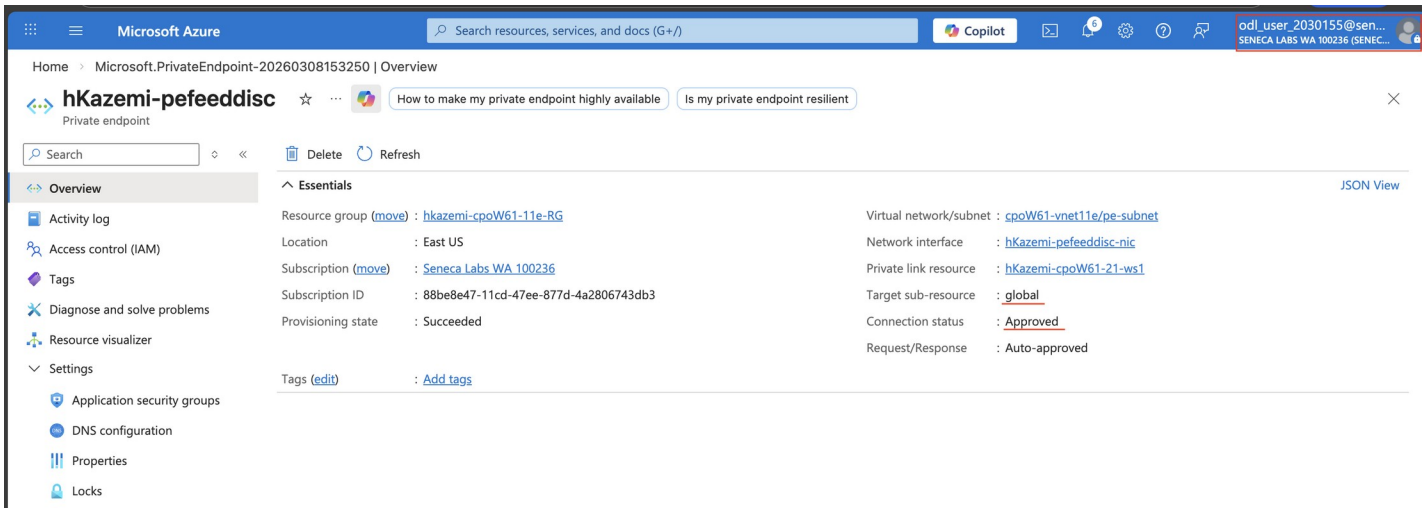
Task 3:



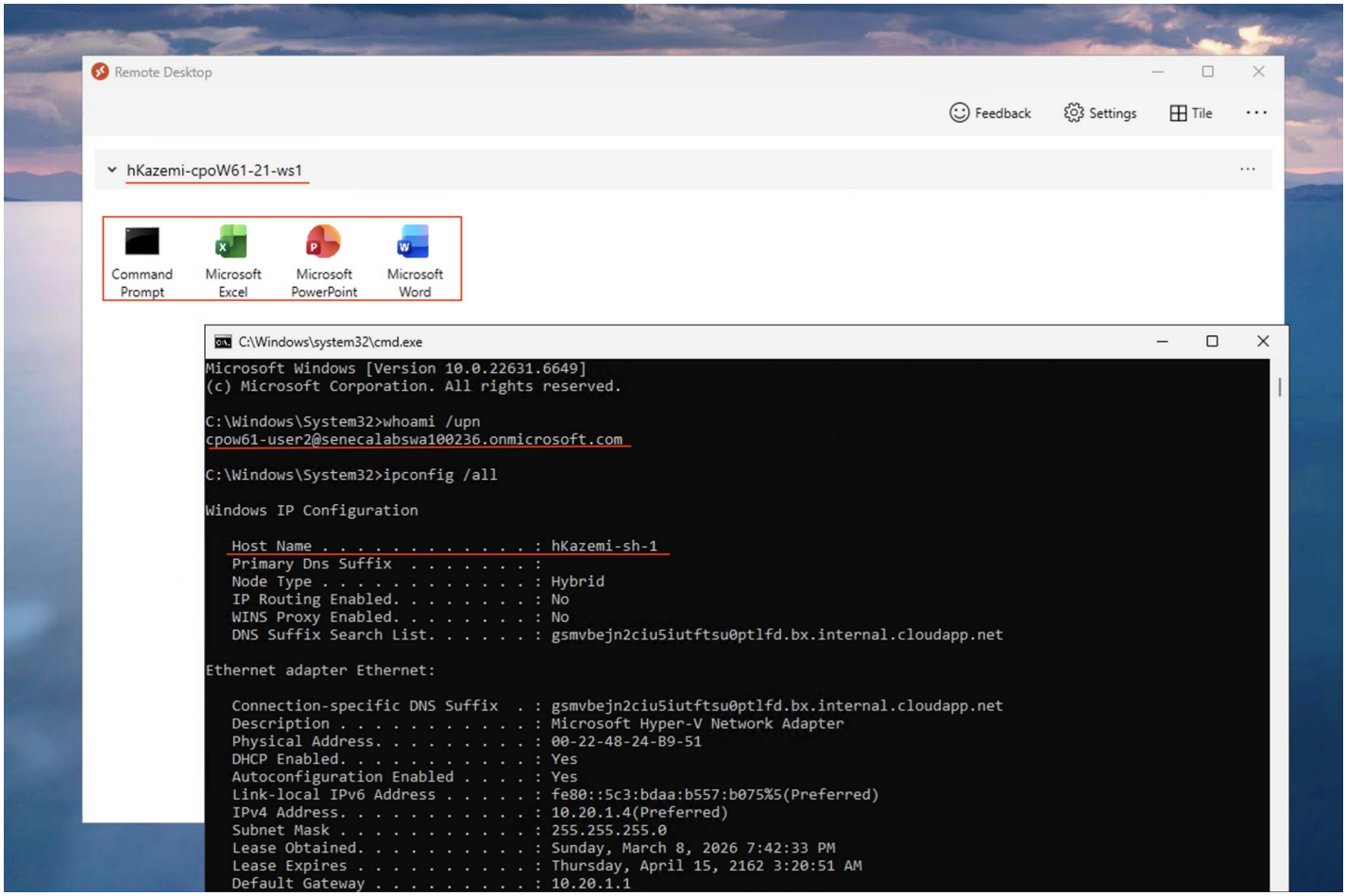
Task 4:



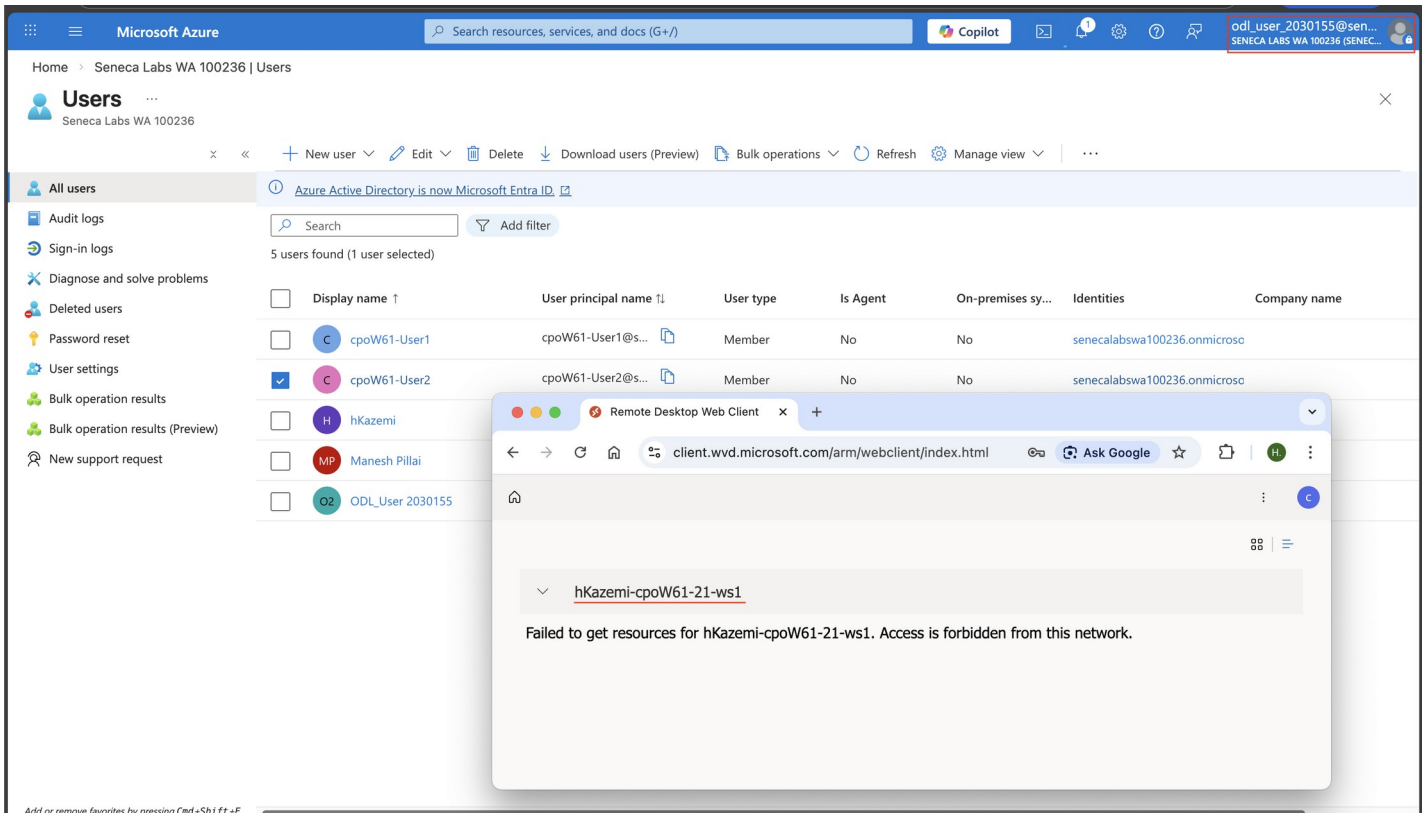
Task 5(s10):



Task 6(s37):



Task 6(s40):



Task 7: