



CPO550 - Lab 02:

Manage host pools and session hosts by using the Azure portal

Student Lab Manual

Fall 2026

Lab scenario

You have an existing Azure Virtual Desktop environment. You need to configure host pool with Microsoft Entra joined session hosts to support a range of functional and business requirements. These requirements include:

- Deploy additional session hosts to accommodate increased number of remote users
- Minimize the cost of the Azure Virtual Desktop environment by optimizing the host pool load balancing configuration and leveraging the *Start VM on Connect* functionality
- Maximize the availability of session hosts during business hours by implementing maintenance windows
- Enable single sign-on to Microsoft Entra-joined session hosts
- Maximize usability and user experience (such as automatic reconnection of disconnected sessions)

Objectives

- Configure Microsoft Entra joined Azure Virtual Desktop session hosts to support a range of functional and business requirements

Lab dependencies

- The lab 01: *Deploy host pools and session hosts by using the Azure portal* completed.

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

Include your answers to the summary questions at the end of your report.

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

Instructions

Exercise 1: Manage an Azure Virtual Desktop environment containing Microsoft Entra joined session hosts

The main tasks for this exercise are as follows:

1. Deploy additional Azure Virtual Desktop host pool session hosts
2. Review and configure the host pool properties
3. Assign the required RBAC role to an Azure Virtual Desktop service principal
4. Configure scheduled agent updates
5. Configure RDP properties of the host pool
6. Summary questions

Task 1: Deploy additional Azure Virtual Desktop host pool session hosts

1. If needed, from your local computer, start a web browser, navigate to the Azure portal and sign in by providing your **Odl_user** credentials.
2. In the web browser displaying the Azure portal, search for and select **Azure Virtual Desktop** and, on the **Azure Virtual Desktop** page, in the vertical menu bar, in the **Manage** section, select **Host pools**.
3. On the **Azure Virtual Desktop | Host pools** page, in the list of host pools, select **<sName>-cpoF67-hp1**.
4. Select **Registration key** from the top menu. Click **Generatate new key**. Select the next day for the Expiration date. Click **OK**. Download the file and close.
5. Back on the **<sName>-cpoF67-hp1**, In the **Manage** section, select **Session hosts** and verify that the pool consists of two *Running* hosts. Select **+ Add**.
6. On the **<sName>-cpoF67-hp1 | Session hosts** page, select **+ Add**.
7. On the **Basics** tab of the **Add virtual machines to a host pool** page, review the preconfigured settings and select **Next : Virtual Machines**.
8. On the **Virtual Machines** tab of the **Add virtual machines to a host pool** page, specify the following settings and select **Review + create** (leave others with their default settings):

Setting	Value
Resource group	<sName>-cpoF67-21e-RG
Name prefix	<sName>-sh
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, Version 23H2 + Microsoft 365 Apps

Setting	Value
Virtual machine size	Standard D2s_v3
Number of VMs	1
OS disk type	Standard HDD
OS disk size	Default size (128GB)
Boot Diagnostics	Enable with managed storage account (recommended)
Virtual network	cpoF67-vnet11e
Subnet	hp1-Subnet
Network security group	Basic
Public inbound ports	No
Select which directory you would like to join	Microsoft Entra ID
Enroll VM with Intune	No
User name	Student
Password	The same password you used when deploying the session hosts in the lab 01
Confirm password	The same password you specified previously

- On the **Review + create** tab of the **Add virtual machines to a host pool** page, select **Create**

Note: The provisioning process might take about 20 minutes.



Task 2: Review and configure the host pool properties

- From your local 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 **<sName>-cpoF67-hp1**.
- In the **Settings** section, select **Properties**.
- On the **<sName>-cpoF67-hp1 | Properties** page, review the available configuration options including:
 - Preferred app group type:** This option sets the preferred app group type for the host pool to either **Desktop** or **RemoteApp**. If end users have both RemoteApp and Desktop apps published to them in the host pool, they will only see the selected app type in their feed.
 - Start VM on connect:** Enabling this option allows users to start individual virtual machines in the host pool from the deallocated state.
 - Validation environment:** Validation host pool is intended for testing service changes before they are deployed to production.

- o **Load balancing algorithm:** This option provides the choice between the breadth-first and depth-first load balancing. The breadth-first load balancing distributes new user sessions across all available session hosts in the host pool. Depth-first load balancing distributes new user sessions to an available session host with the highest number of connections which has not reached the maximum session limit threshold.
4. In the **Load balancing algorithm** drop-down list, select **Depth-first**.
 5. In the **Max session limit** text box, enter **8**.
 6. On the <sName>-cpoF67-hp1 | **Properties** page, set **Start VM on connect** to **Yes**.

Note: *Start VM on Connect* lets you reduce costs by enabling end users to power on the virtual machines (VMs) used as session hosts only when they're needed. For personal host pools, *Start VM on Connect* only powers on an existing session host VM that is already assigned or can be assigned to a user. For pooled host pools, *Start VM on Connect* only powers on a session host VM when none are turned on and more VMs are only be turned on when the first VM reaches the session limit.

7. On the <sName>-cpoF67-hp1 | **Properties** page, select **Save**.

Note: Using *Start VM on Connect* requires assigning the *Desktop Virtualization Power On Contributor* role-based access control (RBAC) role to the *Azure Virtual Desktop* service principal at the Azure subscription scope.



Task 3: Assign the required RBAC role to an Azure Virtual Desktop service principal

1. From your local computer, in the web browser displaying the Azure portal, start a PowerShell session in the Azure Cloud Shell.

Note: If prompted, in the **Getting started** pane, in the **Subscription** drop-down list, select the name of the Azure subscription you are using in this lab and then select **Apply**.

2. In the PowerShell session in the Azure Cloud Shell pane, run the following command to retrieve the value of the Id property of the Azure subscription you are using in this lab and store it in a variable \$subId:

```
$subId = (Get-AzSubscription).Id
```

3. Run the following command to create a \$parameters variable, which stores a hash table that contains the values of the RBAC role definition name, Microsoft Entra application representing the **Azure Virtual Desktop** service principal, and the subscription scope:

```
$parameters = @{
    RoleDefinitionName = "Desktop Virtualization Power On Contributor"
    ApplicationId = "9cdead84-a844-4324-93f2-b2e6bb768d07"
    Scope = "/subscriptions/$subId"
}
```

4. Run the following command to create the RBAC role assignment:

```
New-AzRoleAssignment @parameters
```



5. Close the Cloud Shell pane.

Task 4: Configure scheduled agent updates

Note: By default, the AVD agent updates itself automatically whenever a new version is released. This feature lets you restrict those updates to specific maintenance windows to prevent potential session disruptions during peak business hours.

The *Scheduled Agent Updates* lets you create up to two maintenance windows for the updates of the AVD agent, side-by-side stack, and Geneva Monitoring agent, so these updates take place outside of business hours.

1. In the web browser displaying the Azure portal, navigate back to the <sName>-cpoF67-hp1 host pool page.
2. In the **Settings** section, select the **Scheduled agent updates** entry and select the **Scheduled agent updates** checkbox.
3. In the **Schedule** section, select the **Use local session host time zone** checkbox.
4. In the **Maintenance window** section, in the **Day** drop-down list, select **Saturday** and, in the **Time** drop-down list, select **11:00 PM**.
5. Select **Apply**.



Task 5: Configure RDP properties of the host pool

1. In the web browser displaying the Azure portal, on the <sName>-cpoF67-hp1 page, in the vertical menu bar, in the **Settings** section, select the **RDP Properties** entry.
2. Review the available **RDP Properties** configuration options, including:
 - o **Microsoft Entra single sign-on:** This option determines if connections will attempt to leverage Microsoft Entra authentication to sign in to Microsoft Entra-joined session hosts and, effectively, provide a single sign-on experience. Note that it's not required for the client computer to be Microsoft Entra-joined.
 - o **Credential Security Support Provider:** This option controls the use of CredSSP for authentication. CredSSP provides the ability to securely forward user credentials from the client device to the remote desktop session host. However, its capabilities do not include support for Entra ID authentication.
 - o **Alternate shell:** This option allows you to specify an executable to start whenever a new connection to a session host is established. This setting applies only to session hosts running Windows Server.
 - o **KDC proxy name:** This option provides the ability to proxy Kerberos authentication traffic to Active Directory domain controllers.

Note: Considering that three of these options are not applicable in our scenario (which involves Microsoft Entra-joined session hosts without any presence of Active Directory Domain Services), you will configure only the first one. This option corresponds to the `enablerdsaadauth:i:value` RDP property.

3. In the **Microsoft Entra single sign-on** drop-down list, select the option **Connections will use Microsoft Entra authentication to provide single sign-on** and then select **Save**.

Important: It is essential to keep in mind that enabling this specific RDP property is just one of several steps required to implement single sign-on functionality. Other actions applicable to this scenario include enabling Microsoft Entra authentication for RDP in the Entra tenant and configuring device groups, which are not supported in the current version of the lab environment.

4. On the <sName>-cpoF67-hp1 | RDP Properties page, select the **Session behavior** tab and review the available configuration options, including:
 - o **Reconnection:** This option determines whether the client computer will automatically try to reconnect to the remote computer if the connection is dropped.
 - o **Bandwidth auto detect:** This option determines whether to use automatic network bandwidth detection or not.
 - o **Network auto detect:** This option allows you to enable automatic detection of the network type. It is used in conjunction with **Bandwidth auto detect**.
 - o **Compression:** This option determines whether the connection should use bulk compression.
 - o **Video playback:** This option enables the use of RDP efficient multimedia streaming for video playback.
5. On the **Session behavior** tab, in the **Reconnection** drop-down list, select **Client automatically tries to reconnect** and then select **Save**.
6. Now select the **Device redirection** tab and review the available configuration options, including two main categories:
 - o **Audio and video**
 - o **Local devices and resources**

Note: By default, redirection applies to all disk drives, including the ones which are mounted after the initial connection is established.

7. Then select the **Display settings** tab and review the available configuration options, including support for multiple displays, smart sizing, and specific desktop sizes (in pixels).
8. On the <sName>-cpoF67-hp1 | RDP Properties page, select the **Advanced** tab and review the existing configuration settings. Note that these settings reflect the changes you made earlier in this task.



Task 6: Summary Questions

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

Task 1 – Deploy additional Azure Virtual Desktop session hosts

- Why is it important to add additional session hosts to an Azure Virtual Desktop host pool as user demand increases?

Explain how session host scaling impacts performance, user experience, and overall availability.

Task 2 – Review and configure host pool properties

- How do the selected host pool settings (load balancing algorithm, max session limit, and Start VM on Connect) support cost optimization and efficient resource utilization?

In your answer, describe how these settings influence session distribution and VM power management.

Task 3 – Assign the required RBAC role to the Azure Virtual Desktop service principal

- Why is assigning the Desktop Virtualization Power On Contributor role to the Azure Virtual Desktop service principal necessary when using Start VM on Connect?

Discuss what would happen if this role were missing or incorrectly scoped.

Task 4 – Configure scheduled agent updates

- How do scheduled agent update maintenance windows help balance system stability and business availability in an Azure Virtual Desktop environment?

Provide an example of how improper update timing could affect end users.

Task 5 – Configure RDP properties of the host pool

- How do the configured RDP properties (Microsoft Entra single sign-on and automatic session reconnection) improve usability and security for end users?

Explain how these settings enhance the remote desktop experience in a Microsoft Entra-joined environment.

Important Lab Cleanup Instructions

Do **NOT** delete any resources created in this lab. They are required for subsequent labs.

To minimize costs, stop all virtual machines (VMs) immediately. Restart them only when beginning the next lab.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

odl_user_2030155@sen...
SENECA LABS WA 100236 (SENEC...)

Home > Compute infrastructure

Compute infrastructure

Virtual machines

Get started

Search

Overview

All resources

Infrastructure

Virtual machines

Virtual Machine Scale Set (VMSS)

Compute Fleet

Disks + images

Capacity + placement

Related services

Monitoring+Policy

Help

Support + Troubleshooting

Create

Reservations

Manage view

Refresh

Export to CSV

Open query

Assign tags

Start

Restart

Stop

Group by none

You are viewing a new version of Browse experience. Click here to access the old experience.

Filter for any field...

Subscription equals all

Type equals all

Resource Group equals all

Location equals all

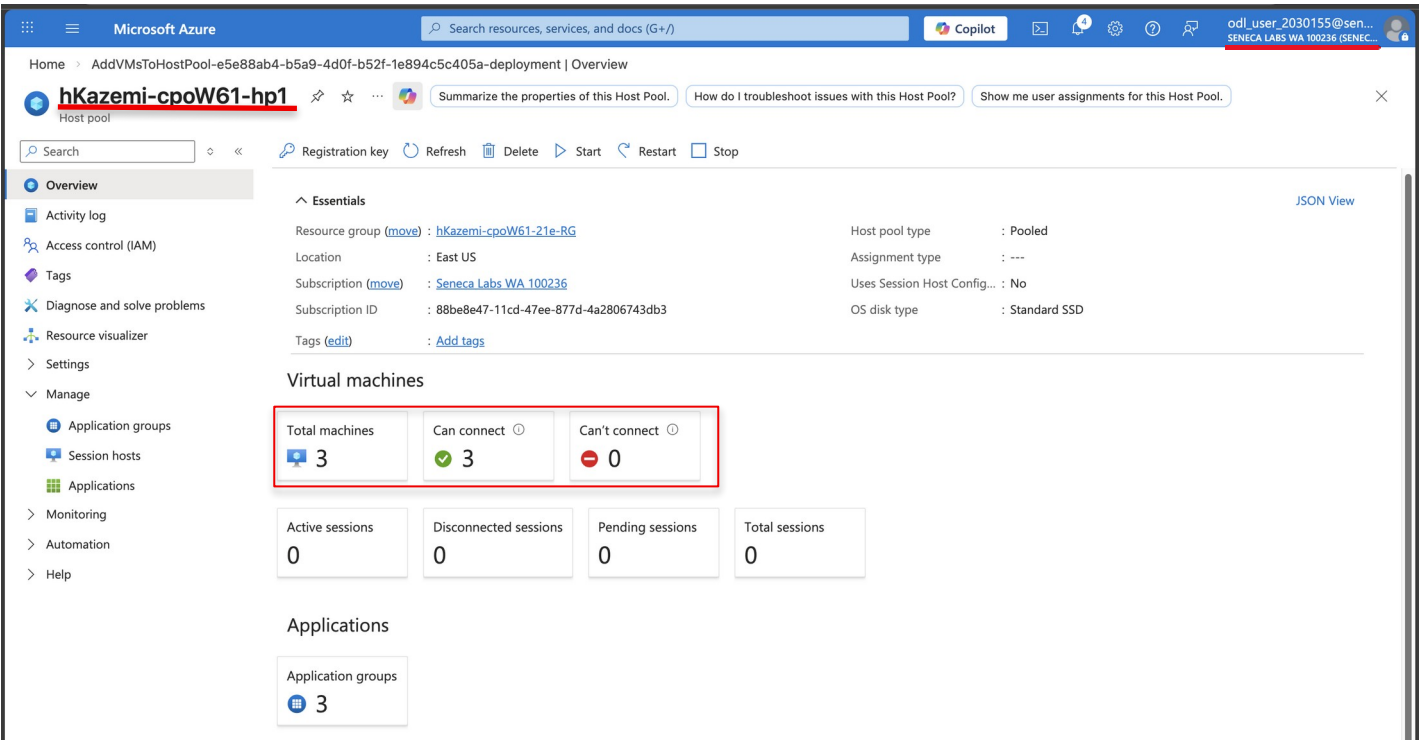
Add filter

Name	Subscription	Resource Group	Location	Status	Operating syst...	Size	Public IP addr...	Disks
hKazemi-sh-0	Seneca Labs W...	hKazemi-cpoW...	East US	Stopped	Windows	Standard_D2s_v3	-	1
hKazemi-sh-1	Seneca Labs W...	hKazemi-cpoW...	East US	Stopped	Windows	Standard_D2s_v3	-	1
hKazemi-sh-2	Seneca Labs W...	hKazemi-cpoW...	East US	Stopped	Windows	Standard_D2s_v3	-	1

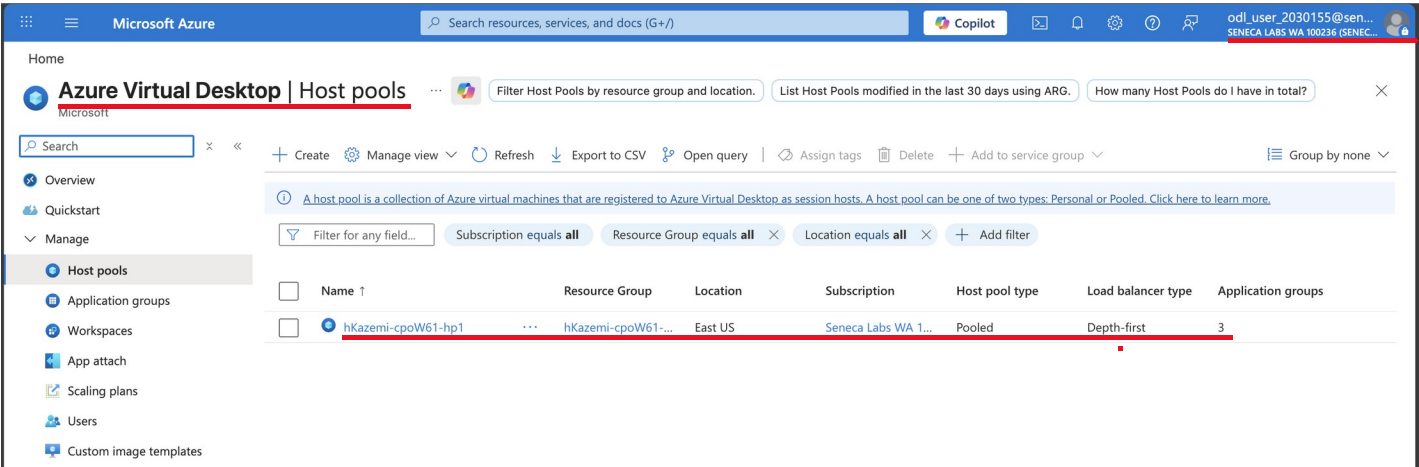
Sample Screenshots

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

Task 1:



Task 2:



Task 3:

Host pools

Name	Resource Group	Location	Subscription	Host pool type	Load balancer type	Application groups
hKazemi-cpoW61-hp1	hKazemi-cpoW61...	East US	Seneca Labs WA 1...	Pooled	Depth-first	3

```

>> }
PS /home/odl_user> New-AzRoleAssignment @parameters

RoleAssignmentName : c40a65c3-e747-474e-9e78-ee2c8c195284
RoleAssignmentId   : /subscriptions/88be8e47-11cd-47ee-877d-4a2806743db3/providers/Microsoft.Authorization/roleAssignments/c40a65c3-e747-474e-9e78-ee2c8c195284
Scope              : /subscriptions/88be8e47-11cd-47ee-877d-4a2806743db3
DisplayName        : Azure Virtual Desktop
SignInName        :
RoleDefinitionName : Desktop Virtualization Power On Contributor
RoleDefinitionId   : 489581de-a3bd-480d-9518-53dea7416b33
ObjectId          : 0db3a64f-3263-432f-8ff6-c34e0deaeb42
ObjectType        : ServicePrincipal
CanDelegate       : False
Description        :
ConditionVersion   :
Condition          :
  
```

Task 4:

hKazemi-cpoW61-hp1 | Scheduled agent updates

Scheduled agent updates ☒

Disabling scheduled updates means that agent updates will automatically be installed by AVD when they become available. [Learn more](#)

Schedule

Specify up to 2 maintenance windows during which the agent update will happen. If after 4 retries, the agent fails to update all the session hosts in the host pool, the update will happen the next time the session hosts are turned on. [Learn more](#)

Use local session host time zone ☒

Time zone

Maintenance window

Day *

Time *

Additional maintenance window

Add Additional window ☐

[Apply](#) [Discard changes](#)

Task 5:

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

odl_user_2030155@sen...
SENECA LABS WA 100236 (SENEC...

Home > Azure Virtual Desktop | Host pools > hKazemi-cpoW61-hp1

hKazemi-cpoW61-hp1 | RDP Properties ☆ ...
Host pool

Search Download template

Changes to RDP Properties have been saved

Each host pool has a set of default RDP properties and values. You can add other properties to the default set or override the default values by setting custom RDP properties [Learn more](#)

Connection information Session behaviour Device redirection Display settings **Advanced**

RDP Properties ⓘ

```
drivestoredirects;usbdevicestoredirects;redirectclipboard;i:0;redirectprinters;i:0;audiomode;i:0;videoplaybackmode;i:1;devicestoredirects;redirectcomports;i:1;redirectsmartcards;i:1;enablecredsspsupport;i:1;redirectwebauthn;i:1;usemultimon;i:1;enablersaadauth;i:1;autoreconnection enabled;i:1
```

The characters \ ; : must be escaped with a backslash character '\' from properties values. e.g. 'C:' should be 'C\.'

Before you enable Microsoft Entra single sign-on (enablersaadauth), make sure to follow the directions in our documentation for the best experience. [Learn more](#)

Save Discard changes Restore to default settings

Add or remove favorites by pressing Cmd+Shift+F