Lab - Manage host pools and session hosts by using the Azure portal (Entra ID)

Student lab manual

Lab dependencies

- An Azure subscription you will be using in this lab.
- A Microsoft Entra user account with the Owner or Contributor 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

30 minutes

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

After completing this lab, you will be able to:

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

Lab files

- None

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

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

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. 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 **az140-21-hp1**.

4. On the **az140-21-hp1** page, in the in the vertical menu bar, in the **Manage** section, select **Session hosts** and verify that the pool consists of two hosts.

5. On the **az140-21-hp1 | Session hosts** page, select **+ Add**.

6. On the **Basics** tab of the **Add virtual machines to a host pool** page, review the preconfigured settings and select **Next: Virtual Machines**.

7. 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):

   > **Note**: When setting the **Name prefix** value, switch to the Resources tab on the right side of the lab session window and identify the string of characters between *User1-* and the @ character. Use this string to replace the *random* placeholder.

Setting	Value
Resource group	**az140-21e-RG**
Name prefix	**sh**-*random*
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 - Gen2**

Setting	Value
Virtual machine size	**Standard DC2s_v3**
Number of VMs	**1**
OS disk type	**Standard SSD**
OS disk size	**Default size (128GB)**
Boot Diagnostics	**Enable with managed storage account (recommended)**
Virtual network	**az140-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 *Deploy host pools and session hosts by using the Azure portal (Entra ID)*
Confirm password	the same password you specified previously

> **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.

> **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.

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

> **Note**: Do not wait for the provisioning process to complete but instead proceed to the next task. The provisioning process might take about 20 minutes.

Task 2: Review and configure the host pool properties

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 **Settings** section, select **Properties**.

3. On the **az140-21-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.
   - **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. On the **az140-21-hp1|Properties** page, in the **Load balancing algorithm** drop-down list, select **Depth-first**.

5. In the **Max session limit** text box, enter **8**.

6. On the **az140-21-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 **az140-21-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 the lab 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**: The Scheduled Agent Updates feature lets you create up to two maintenance windows for the updates of the Azure Virtual Desktop 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 **az140-21-hp1** host pool page.
2. On the **az140-21-hp1** page, in the in the vertical menu bar, in the **Settings** section, select the **Scheduled agent updates** entry and, on the **az140-21-hp1|Scheduled agent updates** page, 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 **az140-21-hp1** page, in the in the vertical menu bar, in the **Settings** section, select the **RDP Properties** entry.

2. On the **Connection information** tab of the **az140-21-hp1|RDP Properties** page, review the available configuration options, including:

   - **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.
   - **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.
    - **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.
    - **KDC proxy name**: This option provide 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 Microsft 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, hence are not included in the instructions. For the full listing of actions necessary to implement single sign-on for Microsoft Entra ID, refer to Configure single sign-on for Azure Virtual Desktop using Microsoft Entra ID authentication.

4. On the **az140-21-hp1|RDP Properties** page, select the **Session behavior** tab and review the available configuration options, including:

    - **Reconnection**: This option determines whether the client computer will automatically try to reconnect to the remote computer if the connection is dropped.
    - **Bandwidth auto detect**: This option determines whether to use automatic network bandwidth detection or not.
    - **Network auto detect**: This option allows you to enable automatic detection of the network type. It is used in conjunction with **Bandwidth auto detect**.
    - **Compression**: This option determines whether the connection should use bulk compression.
    - **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. On the **az140-21-hp1|RDP Properties** page, select the **Device redirection** tab and review the available configuration options, including two main categories:

    - **Audio and video**
    - **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. On the **az140-21-hp1|RDP Properties** page, 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 **az140-21-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.