PassQueen
a.k.a dumpsqueen.com

Configuring and Operating Windows Virtual Desktop on Microsoft Azure

Microsoft AZ-140

Version Demo

Total Demo Questions: 34

Total Premium Questions: 344

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Plan an Azure Virtual Desktop implementation	60
Topic 2, Implement an Azure Virtual Desktop infrastructure	68
Topic 3, Manage access and security	80
Topic 4, Manage user environments and apps	74
Topic 5, Monitor and maintain an Azure Virtual Desktop infrastructure	45
Topic 6, Case Study 1	3
Topic 7, Case Study 2	3
Topic 8, Case Study 3	2
Topic 9, Case Study 4	5
Topic 10, Case Study 5	2
Topic 11, Case Study 6	2
Total	344

QUESTION NO: 1

You need to recommend an authentication solution that meets the performance requirements.

Which two actions should you include in the recommendation? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Join all the session hosts to Azure AD.

B. In each Azure region that will contain the Windows Virtual Desktop session hosts, create an Azure Active Directory Domain Service (Azure AD DS) managed domain.

C. C. Deploy domain controllers for the on-premises Active Directory domain on Azure virtual machines.

D. Deploy read-only domain controllers (RODCs) on Azure virtual machines.

E. In each Azure region that will contain the Windows Virtual Desktop session hosts, create an Active Directory site.

ANSWER: C E

Explanation:

Deploying domain controllers for the on-premises Active Directory domain on Azure virtual machines provides session hosts with local, low-latency access to Active Directory Domain Services for domain authentication, computer account operations, Group Policy processing, and user sign-in. Placing writable domain controllers in Azure is an appropriate way to extend an existing on-premises AD DS environment to support Azure-hosted workloads while retaining the same domain and identity management model.

Creating an Active Directory site in every Azure region that contains session hosts complements the regional domain-controller deployment. AD DS sites and subnet mappings allow domain-joined computers to identify their Azure network location and use domain controllers in the closest site. This reduces unnecessary authentication and directory-lookup traffic across regions or back to on-premises infrastructure, helping meet performance requirements for session-host sign-ins. The site design should include the Azure virtual-network subnets used by the session hosts and domain controllers, with appropriate site links and replication scheduling.

Microsoft's guidance for extending AD DS to Azure recommends deploying domain controllers in Azure and configuring sites and subnets so clients can locate suitable local domain controllers. See Extend Active Directory Domain Services to Azure and Designing the AD DS site topology.

QUESTION NO: 2

You have an Azure Virtual Desktop host pool named Pool1.

You need to prevent users from copying files or clipboard content between sessions in Pool1 and their local devices.

Which two RDP properties should you configure? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Set `redirectclipboard:i:0`.

B. Set `drivestoredirect:s:`.

C. Set `redirectprinters:i:0`.

D. Set `audiomode:i:0`.

E. Set `redirectcomports:i:0`.

ANSWER: A B

Explanation:

Configure `redirectclipboard:i:0` to disable clipboard redirection. This prevents users from copying and pasting clipboard content between the local device and the remote session.

Configure an empty `drivestoredirect:s:` value to prevent local drives from being redirected to the remote session. Without redirected drives, users cannot use a local drive through the remote session to copy files between the local device and the Azure Virtual Desktop session.

RDP properties are applied to connections for the host pool and are appropriate for controlling client-device redirection. See Supported RDP properties for Azure Virtual Desktop.

QUESTION NO: 3

You have an Azure Virtual Desktop deployment.

You plan to implement the Start/Stop VMs during off-hours feature.

You need to ensure that you can stop the session hosts automatically based on the CPU utilization.

What should you do on the session hosts?

A. Install the Azure Virtual Desktop Agent

B. Enable change tracking

C. Configure the Power Management settings

D. Configure the Diagnostic settings

ANSWER: D

Explanation:

Configure the Diagnostic settings on the session-host virtual machines so that their CPU-related platform metrics are collected and sent to a monitoring destination, typically a Log Analytics workspace. CPU utilization is a VM platform metric, and configuring diagnostic settings allows Azure Monitor metrics to be exported for use by monitoring, alerting, and automation workflows. The Start/Stop VMs during off-hours solution can use this telemetry to identify virtual machines whose activity is below the configured threshold and initiate an automated shutdown according to the solution's schedule and CPU-based rules.

For an Azure Virtual Desktop environment, this configuration should be applied consistently to the session hosts that are intended to participate in CPU-based power management. The destination workspace and retained metrics provide the operational data needed to evaluate utilization over the relevant period, rather than relying solely on an instantaneous observation. Microsoft documents that Azure Monitor diagnostic settings can route platform metrics to destinations such as Log Analytics, and that Azure Monitor provides monitoring capabilities for Azure Virtual Desktop and its supporting resources. See Diagnostic settings in Azure Monitor and Monitor Azure Virtual Desktop.

QUESTION NO: 4

You have an Azure Virtual Desktop pooled host pool named Pool1. The session hosts are stopped outside business hours.

You need to ensure that authorized users can start a stopped session host when they attempt to connect to Pool1. The solution must use the least amount of administrative effort.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Enable Start VM on connect for Pool1.

B. Assign the Desktop Virtualization Power On Contributor role to the Azure Virtual Desktop service principal.

C. Enable just-in-time VM access for every session host.

D. Assign the Owner role to all users of Pool1.

E. Create an Azure Load Balancer rule for RDP.

ANSWER: A B

Explanation:

Enable Start VM on connect for Pool1 and assign the **Desktop Virtualization Power On Contributor** role to the Azure Virtual Desktop service principal at the appropriate scope. Start VM on connect allows the Azure Virtual Desktop service to start a deallocated or stopped session host when an entitled user attempts to connect and no suitable running host is available.

The Desktop Virtualization Power On Contributor role grants the Azure Virtual Desktop service principal the permissions required to start the virtual machines. Assigning the role at the resource group or subscription scope containing the session hosts provides the required VM power permissions without granting broad Contributor access.

For more information, see Start VM on connect in Azure Virtual Desktop and Azure Virtual Desktop built-in roles.

QUESTION NO: 5

You need to recommend an authentication solution that meets the performance requirements.

Which two actions should you include in the recommendation? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Join all the session hosts to Azure AD.

B. In each Azure region that will contain the Windows Virtual Desktop session hosts, create an Azure Active Directory Domain Service (Azure AD DS) managed domain.

C. Deploy domain controllers for the on-premises Active Directory domain on Azure virtual machines.

D. Deploy read-only domain controllers (RODCs) on Azure virtual machines.

E. In each Azure region that will contain the Windows Virtual Desktop session hosts, create an Active Directory site.

ANSWER: C E

Explanation:

Deploying domain controllers for the on-premises Active Directory domain on Azure virtual machines places writable Active Directory Domain Services authentication infrastructure close to the Azure Virtual Desktop session hosts. This reduces the dependency on WAN connectivity to on-premises domain controllers and provides the directory services required for domain-joined hosts, user sign-in, computer authentication, and Group Policy processing. Microsoft recommends deploying redundant domain controllers and making them available to Azure workloads that need traditional Active Directory authentication.

Creating an Active Directory site in every Azure region that contains session hosts ensures that Active Directory site-awareness directs authentication and directory-service requests to the most appropriate local domain controllers. Site definitions associate subnets with a location and support efficient domain controller location, replication topology, and logon processing. Together, Azure-hosted domain controllers and region-specific AD sites minimize authentication latency while maintaining the organization's existing on-premises Active Directory domain model. See Microsoft guidance for extending Active Directory Domain Services to Azure and for designing Active Directory site topology.

QUESTION NO: 6

You have an Azure Virtual Desktop host pool named Pool1.

You are troubleshooting an issue for a Remote Desktop client that stopped responding.

You need to restore the default Remote Desktop client settings and unsubscribe from all workspaces.

Which command should you run?

A. msrdcw.exe /reset

B. resetengine

C. mstsc

D. resetpluginhost

ANSWER: A

Explanation:

The `msrdcw.exe /reset` command resets the Windows Remote Desktop client's local user data. This action restores the client to its default settings and removes all workspace subscriptions for the signed-in user, which is appropriate when troubleshooting a client that is unresponsive or has potentially corrupted local configuration data. After the reset, the user must subscribe to their Azure Virtual Desktop workspace again and reconfigure any client preferences that were stored locally.

This command applies to the Remote Desktop client used to access Azure Virtual Desktop resources. It is a client-side recovery action; it does not change the host pool, session hosts, published resources, or Azure Virtual Desktop service configuration. Run it from a Command Prompt, Run dialog, or equivalent shell in the context of the affected user. Microsoft documents the reset switch specifically as restoring default settings and unsubscribing from all workspaces. For the client troubleshooting guidance, see Troubleshoot the Remote Desktop client. Additional information about connecting with the Windows Remote Desktop client is available in Connect to Azure Virtual Desktop with the Remote Desktop client for Windows.

QUESTION NO: 7

You create the virtual machines shown in the following table.

Name	State
SourceVM1	Specialized state
SourceVM2	Generalized state
SourceVM3	Audit mode

You need a source virtual hard disk for new Azure Virtual Desktop session host deployments. The source operating system must have user-specific and machine- specific information removed.

Which virtual machines can you use as the source?

A. SourceVM3 only

B. SourceVM1 only

C. SourceVM1, SourceVM2, and SourceVM3

D. SourceVM1 and SourceVM2 only

E. SourceVM2 only

ANSWER: E

Explanation:

SourceVM2 only is suitable because its operating system has been generalized. Generalizing a Windows VM removes computer-specific configuration and user-specific information from the operating system, preparing its virtual hard disk to be reused as the basis for multiple new session hosts. For Windows, this preparation is performed by using Sysprep with the `/generalize` option. The VM must then be marked as generalized in Azure before its disk or image is used to create new machines.

This process is especially important for Azure Virtual Desktop session hosts because each deployed host must boot with its own unique machine identity and complete its own out-of-box setup. A generalized source VHD provides the reusable, sanitized OS state needed for that deployment model. Microsoft notes that a generalized VM image is intended for creating multiple new VMs, whereas a specialized image preserves machine-specific state. See Generalize a VM before creating an image and Create and manage custom images for Azure Virtual Desktop.

QUESTION NO: 8 - (SIMULATION)

You have an Azure subscription that contains the storage accounts shown in the following table.

You have a custom generalized Windows 10 image.

You plan to deploy an Azure Virtual Desktop host pool that will use the custom image and FSLogix profile containers.

You need to recommend which storage accounts to use for the custom image and the profile containers. The solution must meet the following requirements:

Minimize costs to store the image.

Maximize performance of the profile containers.

Which account should you recommend for each type of content? To answer, drag the appropriate accounts to the correct content type. Each account may be used once, more than once, or not at all. You many need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

ANSWER: See the explanation for the answer

Explanation:

Select the Standard_LRS storage account for the custom generalized Windows 10 image and **select the Premium_LRS (FileStorage) account for the FSLogix profile containers**.

Custom image: The account in the table with `Standard` performance and `LRS` replication. Standard locally redundant storage is the lowest-cost suitable choice for storing the uploaded generalized VHD/image.
FSLogix profile containers: The account in the table with `Premium` performance and `LRS` replication (a `FileStorage` account). Premium Azure Files provides the highest performance for FSLogix profile-container I/O.

Therefore, drag the table's `Standard_LRS` account to *Custom image*, and the table's `Premium_LRS/FileStorage` account to *Profile containers*.

QUESTION NO: 9

You plan to deploy Windows Virtual Desktop session host virtual machines based on a preconfigured master image. The master image will be stored in a shared image.

You create a virtual machine named Image1 to use as the master image. You install applications and apply configuration changes to Image1.

You need to ensure that the new session host virtual machines created based on Image1 have unique names and security identifiers.

What should you do on Image1 before you add the image to the shared image gallery?

A. At a command prompt, run the set computername command.

B. At a command prompt, run the sysprep command.

C. From PowerShell, run the rename-computer cmdlet.

D. From the lock screen of the Windows device, perform a Windows Autopilot Reset.

ANSWER: B

Explanation:

Run the `sysprep` command on Image1 before generalizing it and publishing it to Azure Compute Gallery (previously called Shared Image Gallery). Sysprep prepares a Windows installation for imaging by removing machine-specific information, including the computer name and the machine security identifier (SID). After the VM is created from the generalized image, Windows specializes the operating system during its first boot. Azure can then apply the VM name specified at deployment, while Windows creates a unique SID for that new session host.

For a Windows Virtual Desktop (now Azure Virtual Desktop) session-host image, applications and the required baseline configuration should be completed before Sysprep. The image should then be generalized using Sysprep with the out-of-box experience and generalize settings, such as `sysprep /generalize /oobe /shutdown`. Once shut down, the VM can be marked as generalized and used to create an image version. This ensures each deployed session host is an independently provisioned Windows computer rather than a duplicate of the source VM's machine identity.

Microsoft documents that Sysprep is required when creating a generalized Windows image for deployment to multiple VMs. See Generalize a Windows VM using Sysprep and Azure Compute Gallery documentation.

QUESTION NO: 10

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have the following:

- A Microsoft 365 E5 tenant
- An on-premises Active Directory domain
- A hybrid Azure Active Directory (Azure AD) tenant
- An Azure Active Directory Domain Services (Azure AD DS) managed domain
- An Azure Virtual Desktop deployment

The Azure Virtual Desktop deployment contains personal desktops that are hybrid joined to the on-premises domain and enrolled in Microsoft Intune.

You need to configure the security settings for the Microsoft Edge browsers on the personal desktops.

Solution: You configure a Group Policy Object (GPO) in the Azure AD DS managed domain.

Does this meet the goal?

A. Yes

B. No

ANSWER: B

Explanation:

No is correct because the personal Azure Virtual Desktop desktops are hybrid joined to the on-premises Active Directory domain, not joined to the separate Microsoft Entra Domain Services (Azure AD DS) managed domain. Group Policy processing is based on the Active Directory domain to which a computer is joined. Therefore, a GPO created in Azure AD DS is not in the policy scope of these session hosts and cannot configure their Microsoft Edge settings.

Because the desktops are enrolled in Microsoft Intune, Edge security settings can be deployed through Intune by using a Settings Catalog profile, Administrative Templates, or applicable security policies targeted to the enrolled devices or users. Microsoft documents Microsoft Edge management through Intune policy configuration, including the use of the Settings Catalog and Edge policy settings. Alternatively, where Group Policy is required for these hybrid-joined hosts, the policy must be created and linked in the on-premises Active Directory domain so that it is processed by the desktops. Azure AD DS provides managed-domain capabilities for resources joined to that managed domain; it does not extend GPO scope to devices joined to a different on-premises domain.

See Configure Microsoft Edge policy settings with Microsoft Intune and Microsoft Entra Domain Services overview.

QUESTION NO: 11

You have an Azure Active Directory Domain Services (Azure AD DS) managed domain named contoso.com.

You create an Azure Virtual Desktop host pool named Pool1. You assign the Virtual Machine Contributor role for the Azure subscription to a user named Admin1.

You need to ensure that Admin1 can add session hosts to Pool1. The solution must use the principle of least privilege.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Assign Admin1 the Desktop Virtualization Host Pool Contributor role for Pool1

B. Assign Admin1 the Desktop Virtualization Session Host Operator role for Pool1

C. Add Admin1 to the AAD DC Administrators group

D. Assign a Microsoft 365 Enterprise E3 license to Admin1

E. Generate a registration token

ANSWER: B E

Explanation:

Assign Admin1 the **Desktop Virtualization Session Host Operator** role scoped to Pool1. This Azure Virtual Desktop built-in role provides the permissions required to manage session hosts in a host pool, including adding and removing session hosts. Scoping the assignment directly to Pool1 limits the permissions to the required Azure Virtual Desktop resource and supports least-privilege access. Admin1 already has Virtual Machine Contributor at the subscription scope, which supplies the Azure Resource Manager permissions needed to create and manage the virtual machines that will become session hosts.

Generate a registration token for Pool1. A session host must be registered with its target host pool during deployment. The registration token is supplied to the Azure Virtual Desktop agent installation or configuration process and authorizes the host to register with that host pool. Registration tokens have an expiration time and should be created with an appropriate lifetime for the deployment activity. Together, the scoped session-host management role and a Pool1 registration token allow Admin1 to create the virtual machine and register it as a session host without granting unnecessary host-pool-wide administrative permissions. For details, see Azure Virtual Desktop built-in roles and Add session hosts to a host pool.

QUESTION NO: 12

You have an Azure storage account that contains the generalized Windows 10 disk images shown in the following table.

Name	Format	Disk type
Disk1	VHD	Fixed size
Disk2	VHD	Dynamically expanding
Disk3	VHDX	Fixed size
Disk4	VHDX	Dynamically expanding

You need to create an image that will be used to deploy an Azure Virtual Desktop session host.

Which disk should you use?

A. Disk1

B. Disk2

C. Disk3

D. Disk4

ANSWER: A

Explanation:

Disk1 is the appropriate disk to use for the Azure Virtual Desktop session-host image because it meets the Azure requirements for importing and using a generalized Windows operating-system disk as an image. Before a custom Windows image can be used to deploy session hosts, the source virtual machine must be generalized, typically by using Sysprep, so that each new session host receives its own unique machine-specific configuration during provisioning. The resulting operating-system disk must also be in an Azure-supported virtual hard disk format. Azure supports fixed-size VHD files for uploaded virtual-machine images; this ensures that the virtual disk can be imported into Azure and used to create a managed image or Azure Compute Gallery image version. A properly generalized, supported disk image is then suitable as the source for repeatable Azure Virtual Desktop session-host deployments. Microsoft's Azure Virtual Desktop guidance describes preparing and generalizing a custom image before deploying hosts, while Azure's VHD guidance details the supported VHD requirements for uploaded images. See Prepare and customize a master image for Azure Virtual Desktop and Prepare a Windows VHD or VHDX to upload to Azure.

QUESTION NO: 13 - (DRAG DROP)

DRAG DROP

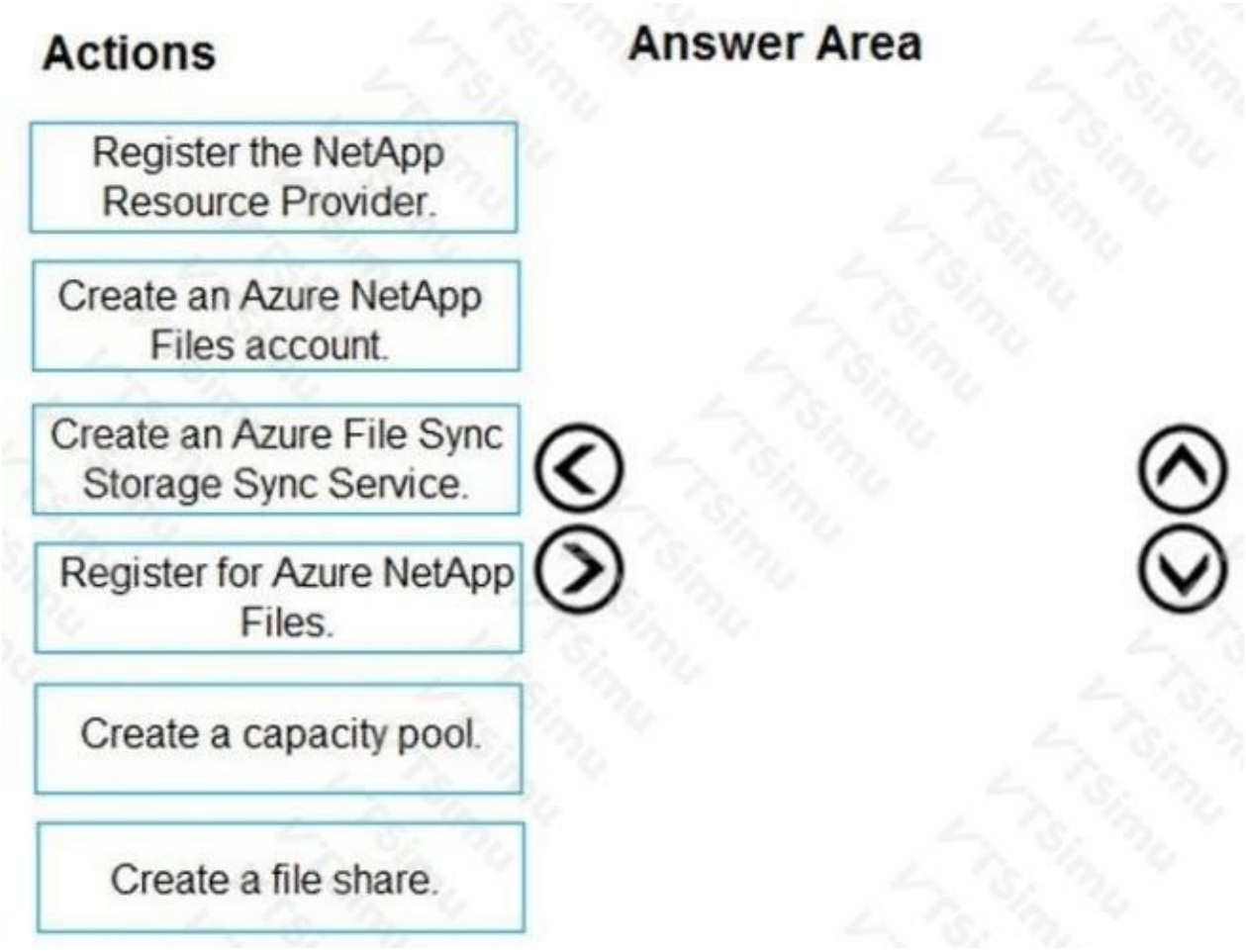
You have an Azure Virtual Desktop host pool named Pool1.

You need to ensure that you can create an Azure NetApp Files volume that will host user profiles for Pool1.

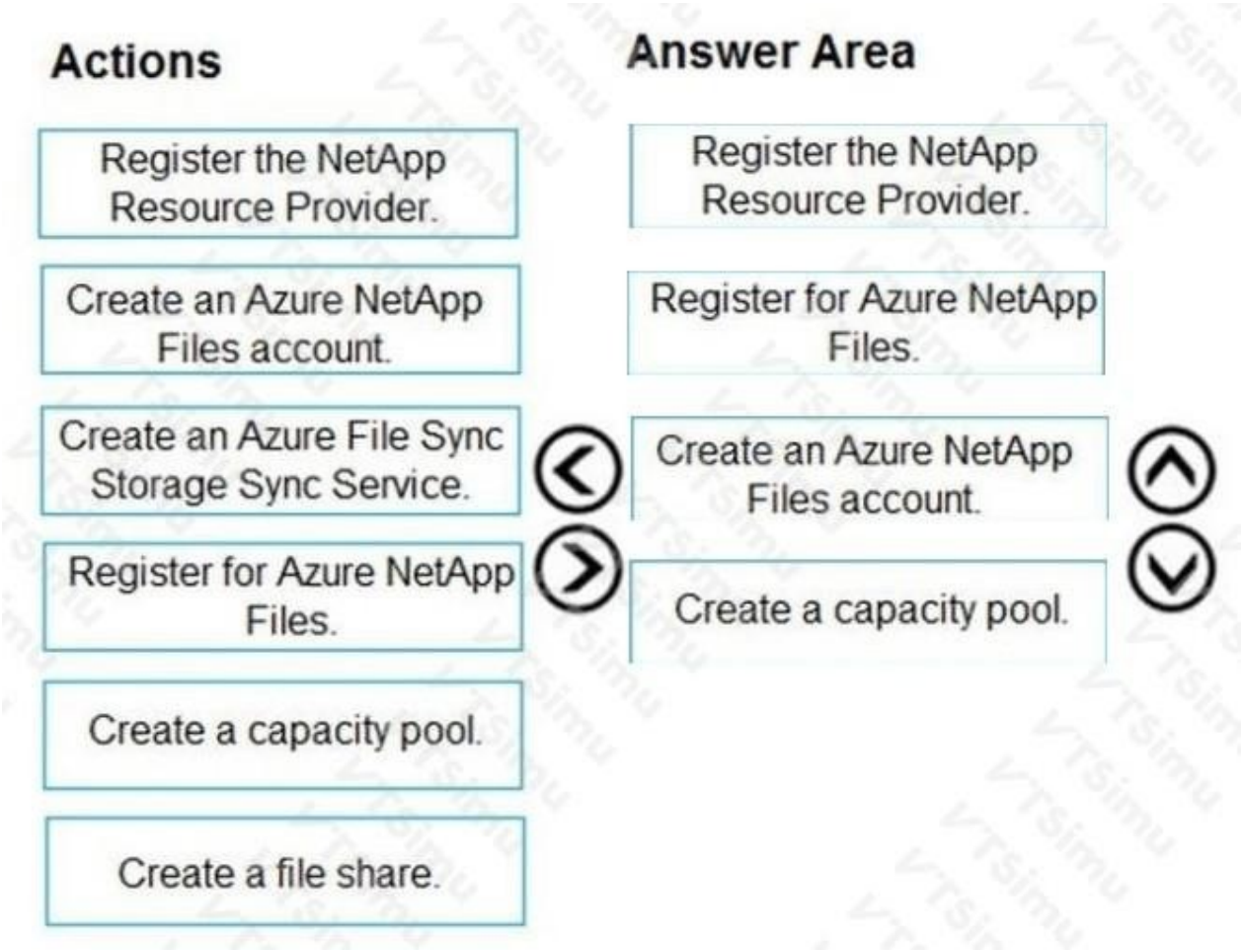
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

Select and Place:


Actions
Answer Area
Register the NetApp Resource Provider.
Create an Azure NetApp Files account.
Create an Azure File Sync Storage Sync Service.
Register for Azure NetApp Files.
Create a capacity pool.
Create a file share.

ANSWER:



Explanation:

To prepare Azure NetApp Files storage for Azure Virtual Desktop user profiles, the subscription first needs access to the Azure NetApp Files service and the Microsoft.NetApp resource provider must be registered. Registering the provider makes the Azure resource types required for NetApp accounts, capacity pools, and volumes available in the subscription. Service registration ensures the subscription is enabled to use Azure NetApp Files in the intended deployment process.

After the service is available, create an Azure NetApp Files account in the Azure region where the profile storage will be hosted. The NetApp account is the logical Azure NetApp Files container for the storage configuration. Within that account, create a capacity pool. A capacity pool establishes the service level and the amount of provisioned storage capacity that can be allocated to volumes. A volume for profile data can then be created from this capacity pool, using the required protocol and network configuration for the Azure Virtual Desktop environment.

This sequence correctly establishes the Azure NetApp Files hierarchy: subscription enablement and provider registration, followed by a NetApp account, followed by a capacity pool. Microsoft documents this workflow in its Azure NetApp Files quickstart for setting up an account, capacity pool, and volume. For profile containers, Azure Virtual Desktop documentation also describes using Azure NetApp Files to store FSLogix profiles, where the resulting volume provides the high-performance shared storage location for user profile data.

QUESTION NO: 14

You plan to deploy Azure Virtual Desktop to meet the department requirements shown in the following table.

A. 1

B. 2

C. 3

D. 4

ANSWER: C

Explanation:

3 is the minimum number of host pools because the departmental requirements require three distinct host-pool configurations. An Azure Virtual Desktop host pool defines fundamental characteristics shared by the session hosts and users assigned to it, including whether the pool is personal or pooled. For pooled host pools, the configured load-balancing algorithm is also a host-pool setting and determines how Azure Virtual Desktop distributes user sessions among available session hosts.

To minimize cost while still meeting the specified requirements, departments that can use the same host-pool type and load-balancing configuration can share a host pool. However, requirements that need a different personal-versus-pooled assignment model or a different load-balancing behavior require separate host pools. Combining such workloads would prevent the individual departmental requirement from being applied correctly. Autoscaling can then be configured for each host pool to start, stop, and scale session hosts according to demand, helping reduce compute cost without reducing the required separation of configurations.

Microsoft documents host pool types and load-balancing behavior in Azure Virtual Desktop load balancing and explains autoscaling configuration in Autoscale scenarios and examples.

QUESTION NO: 15

You have an Azure Virtual Desktop deployment that contains the host pools shown in the following table.

You need to create a disaster recovery environment in the West US region. The solution must minimize costs and administrative effort.

What should you do?

A. Regenerate the token and reregister the virtual machines in the host pools.

B. Create two new host pools in the West US region.

C. Run the Invoke-RdsUserSessionLogoff cmdlet.

D. Create an Azure Site Recovery plan.

ANSWER: B

Explanation:

Create two new host pools in the West US region. Azure Virtual Desktop host pools are Azure-region-specific resources, so a disaster-recovery design requires corresponding host pools in the recovery region. Creating two host pools matches the existing host-pool structure while providing a dedicated West US endpoint for users if the primary region is unavailable. This approach keeps the recovery configuration aligned with the production design and avoids attempting to move or reuse regional host-pool metadata across regions.

For cost-efficient recovery, the West US host pools can be configured as standby capacity rather than continuously operating at full production scale. For example, session hosts can be deployed from standardized images and started or scaled only when a recovery event requires them. User profile data should be made available independently of individual session hosts, commonly by using FSLogix profiles on resilient storage that is accessible in the recovery design. Microsoft's Azure Virtual Desktop disaster-recovery guidance recommends deploying a parallel environment in a secondary region and planning host pools, session hosts, profiles, applications, networking, and user access for that region. See Azure Virtual Desktop disaster recovery and Azure Virtual Desktop host pool configuration.

QUESTION NO: 16

You need to modify the custom virtual machine images to meet the deployment requirements.

What should you install?

A. the RSAT: Remote Desktop Services Tools optional feature

B. the Azure Virtual Desktop Agent

C. the Microsoft Monitoring Agent

D. the FSLogix agent

ANSWER: D

Explanation:

The FSLogix agent should be installed in the custom virtual machine image when the Azure Virtual Desktop deployment requires FSLogix profile containers or related FSLogix functionality. FSLogix Apps is installed on each session host and provides the profile-container technology that redirects a user's profile to centrally stored VHD or VHDX files. This enables users to receive a consistent, portable profile when they sign in to different session hosts in a pooled host pool, while avoiding the delays and management complexity associated with traditional roaming profiles. Including the agent in the reference image ensures that every session host created from that image has the required FSLogix components before users connect. Configuration details, such as the profile storage location and enabled features, can then be applied through policy or registry settings as part of the deployment. Microsoft documents FSLogix as a component to install and configure on Azure Virtual Desktop session hosts, and its profile-container guidance describes the required session-host installation and profile storage configuration. See FSLogix overview and Configure FSLogix profile containers for Azure Virtual Desktop.

QUESTION NO: 17

You have an Azure Virtual Desktop deployment that contains several host pools.

You need to retain Azure Virtual Desktop connection and management diagnostic data for 90 days. Administrators must be able to query the data by using Azure Monitor Logs.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Create a Log Analytics workspace.

B. Configure diagnostic settings for the Azure Virtual Desktop resources.

C. Create an Azure Recovery Services vault.

D. Enable Microsoft Defender for Cloud on each session host.

E. Create an Application Insights resource.

ANSWER: A B

Explanation:

Create a Log Analytics workspace and configure diagnostic settings on the Azure Virtual Desktop resources to send the required diagnostic log categories to that workspace. Log Analytics provides the storage and query engine used by Azure Monitor Logs, including Kusto Query Language queries and Azure Virtual Desktop monitoring workbooks.

Azure Virtual Desktop diagnostic settings can collect categories such as management activity, connection activity, host registration, errors, and checkpoints. Sending these logs to a Log Analytics workspace allows the organization to retain and analyze the data according to the workspace retention configuration.

For more information, see Use Azure Monitor Logs with Azure Virtual Desktop diagnostics and Diagnostic settings in Azure Monitor.

QUESTION NO: 18

You have a Windows Virtual Desktop host pool named Pool1 and an Azure Automation account named account1. Pool1 is integrated with an Azure Active Directory Domain Services (Azure AD DS) managed domain named contoso.com.

You plan to configure scaling for Pool1 by using Azure Automation runbooks.

You need to authorize the runbooks to manage the scaling of Pool1. The solution must minimize administrative effort.

What should you configure?

A. a managed identity in Azure Active Directory (Azure AD)

B. a group Managed Service Account (gMSA) in Azure AD DS

C. a Connections shared resource in Azure Automation

D. a Run As account in Azure Automation

ANSWER: A

Explanation:

A managed identity in Azure Active Directory (Azure AD) is the appropriate configuration because it gives the Azure Automation account's runbooks an automatically managed Microsoft Entra identity for authenticating to Azure Resource Manager. Assign the identity only the Azure RBAC permissions required to perform the scaling operations at the appropriate scope, such as the resource group or subscription containing the host pool and its session-host virtual machines. The runbook can then authenticate noninteractively by using the managed identity, without storing a password, certificate, client secret, or service-principal credential in the Automation account.

This approach minimizes administration because Azure manages the identity lifecycle and credential rotation. It also follows the least-privilege model: permissions can be granted directly to the Automation account identity and reviewed through Azure role assignments. The fact that session hosts join an Azure AD DS managed domain is relevant to the hosts' domain integration, but it does not replace the Azure identity and Azure RBAC authorization required for runbooks to manage Azure Virtual Desktop and VM resources. Microsoft recommends managed identities for Azure Automation authentication scenarios. See Enable managed identity for Azure Automation and Azure Automation security overview.

QUESTION NO: 19

You have an Azure Virtual Desktop host pool named Pool1 that runs Windows 10 Enterprise multi-session hosts.

You need to use Performance Monitor to troubleshoot a low frame quality issue that is affecting a current use session to Pool1.

What should you run to retrieve the user session ID?

A. Get-ComputerInfo

B. qwinsta

C. whoami

D. Get-LocalUser

ANSWER: B

Explanation:

`qwinsta` is the appropriate command because it queries the Remote Desktop Services session state on the Azure Virtual Desktop session host and displays the sessions currently present on that host. Its output includes key details such as the user name, session name, state, idle time, logon time, and—most importantly for this task—the numeric session ID. The session ID lets an administrator identify the specific affected user session and select or correlate the appropriate per-session counters while investigating graphics performance and frame-quality symptoms in Performance Monitor. Run `qwinsta` in a Command Prompt or PowerShell session on the relevant Windows 10 Enterprise multi-session host. If several users are connected, use the listed user name and session state to locate the active session, then record its ID for the Performance

Monitor troubleshooting workflow. Microsoft's Azure Virtual Desktop guidance specifically uses `qwinsta` to retrieve a user session ID when collecting performance information for graphics-related issues. For command syntax and output details, see qwinsta | Microsoft Learn. For Azure Virtual Desktop troubleshooting guidance, see Troubleshoot Azure Virtual Desktop session host configuration.

QUESTION NO: 20

You have a Windows Virtual Desktop deployment that contains the following:

You need to prevent users from copying and pasting between App1 and their local device.

What should you do?

A. Create an AppLocker policy.

B. Modify the locks of RemoteAppGroup1.

C. Modify the locks of RemoteAppGroup1.

D. Modify the RDP Properties of Pool1.

ANSWER: D

Explanation:

Modify the RDP Properties of Pool1. Clipboard redirection between an Azure Virtual Desktop RemoteApp, such as App1, and the user's local device is governed by the RDP property `redirectclipboard`. Configure this property as `redirectclipboard:i:0` on the host pool that publishes the RemoteApp. This prevents the Remote Desktop client from redirecting the local clipboard into the remote session and prevents content in the remote application from being copied to the local clipboard.

RDP properties are configured at the host-pool level and apply to user connections made to resources published from that host pool. This is the appropriate configuration scope for controlling device and resource redirection behavior, including clipboard use. After the setting is saved, users should reconnect so that new sessions receive the updated RDP configuration. Microsoft documents clipboard redirection as a supported custom RDP property for Azure Virtual Desktop host pools. See Customize Remote Desktop Protocol properties for Azure Virtual Desktop and Supported RDP properties.

QUESTION NO: 21 - (HOTSPOT)

You need to configure a conditional access policy to meet the authentication requirements.

What should you include in the policy configuration? To answer, select the appropriate options in the answer area.

NOTE Each correct selection is worth one point.

ANSWER:

Explanation:

The policy should include the **Azure Virtual Desktop** cloud application and the **Sign-in frequency** session control. Azure Virtual Desktop is the Microsoft Entra protected application that represents user access to Azure Virtual Desktop resources. Targeting it causes the Conditional Access policy to be evaluated as users authenticate to access their desktops and remote applications. This is the appropriate policy scope when the requirement concerns authentication for Azure Virtual Desktop users.

Sign-in frequency is the session control that defines the maximum time between required interactive authentications. It can be configured to require users to reauthenticate at the organization's required interval, rather than allowing a prior sign-in and its associated session to continue indefinitely. When a user reaches the configured interval, Microsoft Entra ID requires a fresh authentication before continuing access, so the setting directly implements a periodic authentication requirement.

These two settings work together: the cloud application identifies Azure Virtual Desktop user access as the workload to protect, and the session control applies the required reauthentication cadence to that access. Microsoft documents Conditional Access support for Azure Virtual Desktop and describes how Conditional Access policies are applied to Azure Virtual Desktop connections in the Azure Virtual Desktop Conditional Access documentation. Details on configuring periodic authentication are available in the Microsoft Entra Conditional Access session lifetime documentation.

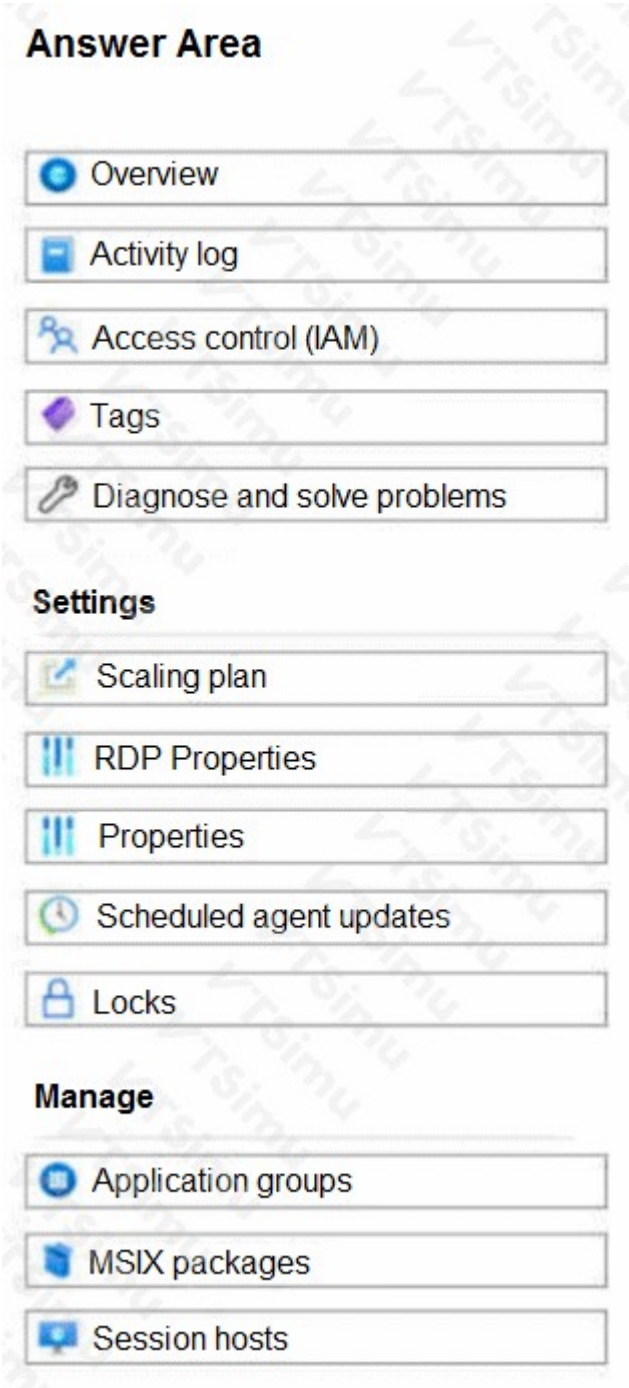
QUESTION NO: 22 - (HOTSPOT)

-You have an Azure Virtual Desktop deployment that contains a host pool named HostPool1.
You need to perform the following configurations for HostPool1:
• Set the scale factor of the remote session to 125 percent.
• Generate a registration key that expires after five days.
• Enable Start VM on connect.Which three settings should you modify?

To answer, select the appropriate settings in the answer area.

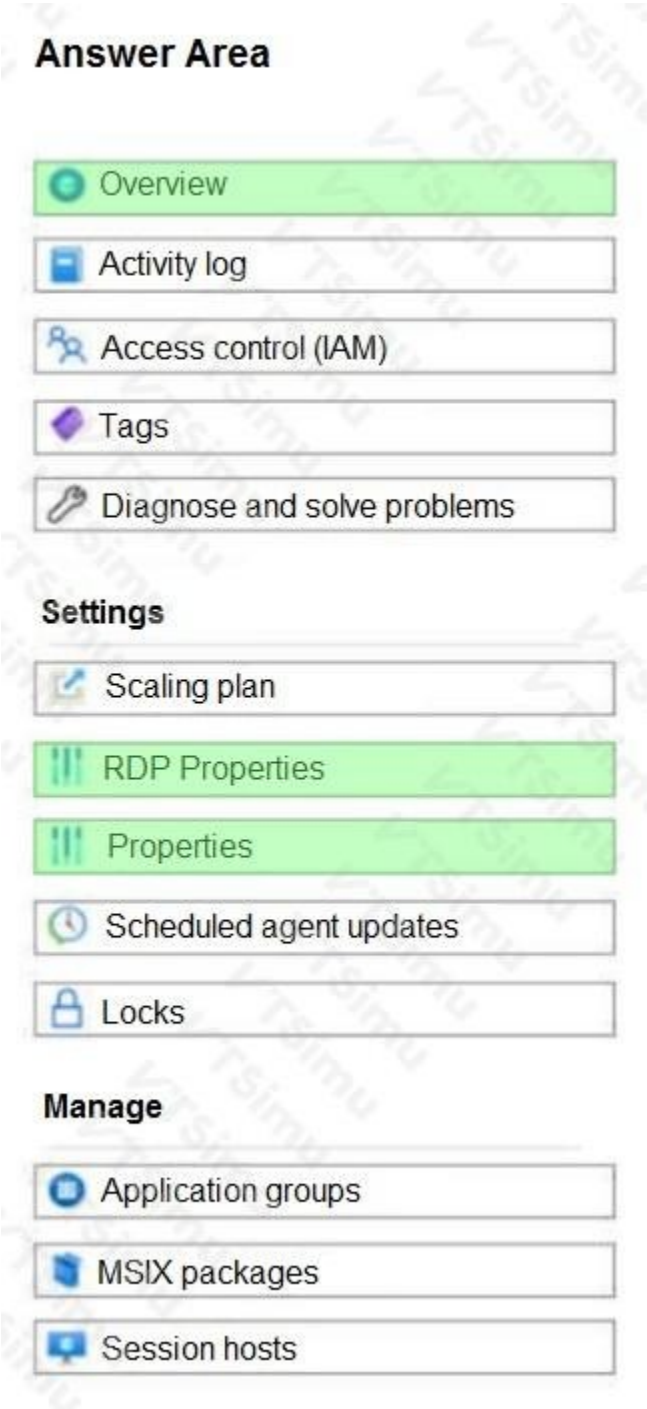
NOTE: Each correct selection is worth one point.

Answer Area



ANSWER:

Answer Area



Explanation:

Use **RDP Properties**, **Overview**, and **Properties** for these host-pool configurations. RDP Properties is the location for settings that are delivered to users as Remote Desktop Protocol properties. To make remote sessions use a 125 percent scale factor, add or edit the applicable custom RDP display-scaling property, such as `desktopscalefactor:i:125`. This setting is applied when the client establishes a session with a session host, allowing the session display to use the required scaling behavior. Microsoft describes the host pool RDP-properties configuration process in its Customize Remote Desktop Protocol properties for Azure Virtual Desktop documentation.

Use Overview to create the host-pool registration key. From the registration-key action on that page, generate a new key and set its expiration to five days. The registration key is the credential session hosts use when registering with the Azure Virtual Desktop service, and the selected expiration determines how long that generated key remains valid. The process is documented in Add session hosts to a host pool.

Use Properties to enable Start VM on connect. This host-pool setting lets Azure Virtual Desktop start an available deallocated session host when a user connects, subject to the supported configuration and permissions. It is a host-pool behavior setting, so it belongs on the Properties page rather than in the RDP connection settings. Microsoft documents the feature and its host-pool configuration requirements in Start VM on connect.

QUESTION NO: 23

You need to prepare the disk on VM1 for use with the Azure Virtual Desktop deployment. Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Convert the disk format to VHD.

B. Merge the disk.

C. Convert the disk type to Fixed size.

D. Compact the disk.

E. Convert the disk type to Differencing.

ANSWER: A C

Explanation:

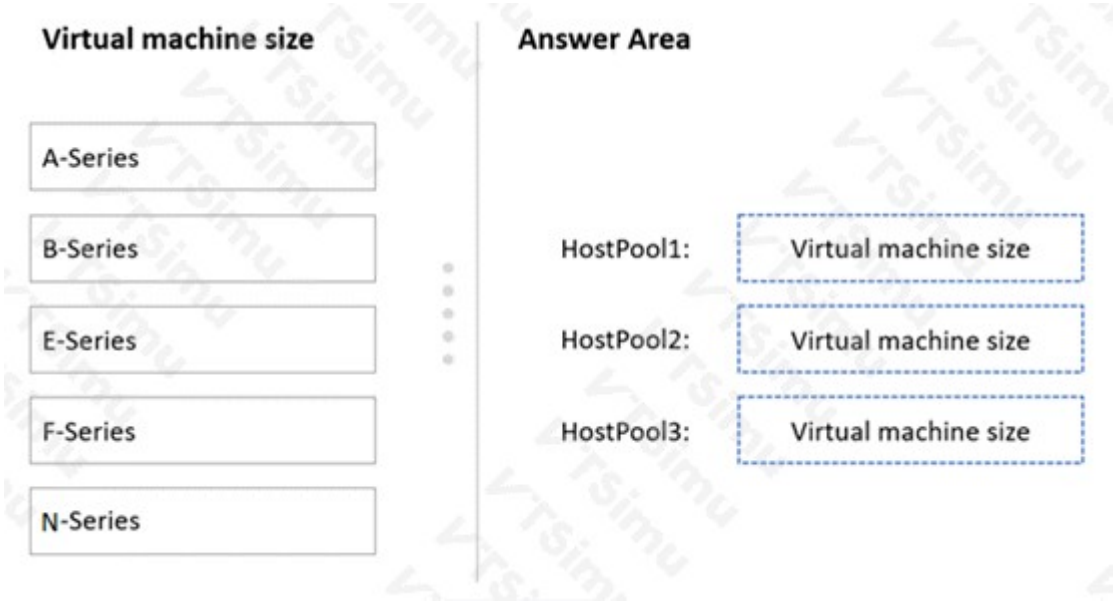
Convert the disk format to VHD. and **Convert the disk type to Fixed size.** are required when preparing a Hyper-V virtual machine disk for upload and use as an Azure managed disk image. Azure supports the VHD disk format for this upload scenario; a VHDX file must therefore be converted before it can be uploaded. The resulting VHD must also be a fixed-size virtual hard disk. Fixed-size VHDs have a defined virtual size and are formatted in the layout Azure expects for creating an image or managed disk. These requirements ensure that the operating-system disk from VM1 can be uploaded to Azure storage and used to create the Azure Virtual Desktop session-host image or deployment resources. Perform the conversions after the VM has been properly prepared for imaging, such as by generalizing it when the deployment process requires a generalized image. Microsoft's guidance for uploading a Windows VHD explicitly specifies that the file must be a fixed-size VHD, rather than VHDX or a dynamically expanding VHD. See Prepare a Windows VHD or VHDX to upload to Azure and Upload a generalized Windows VM image and use it to create new VMs in Azure.

QUESTION NO: 24 - (DRAG DROP)

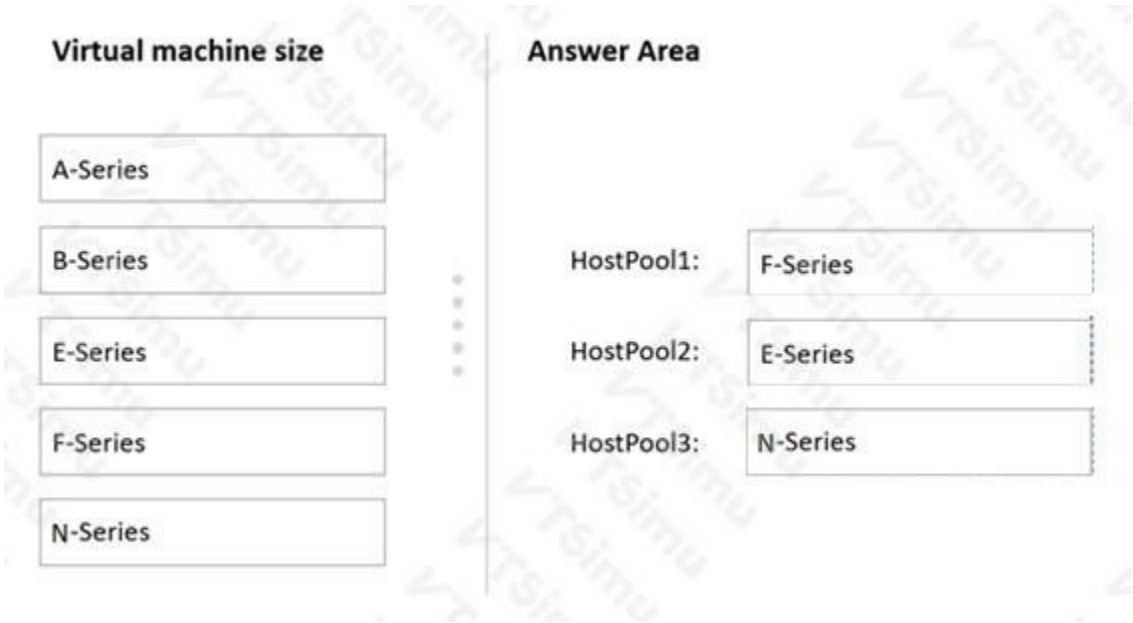
-You have an Azure Virtual Desktop deployment.You plan to create the host pools shown in the following table.

Name	Session host requirement
HostPool1	Compute optimized with a high CPU-to-memory ratio
HostPool2	Memory optimized with a high memory-to-CPU ratio
HostPool3	GPU optimized for graphic rendering and video editing

You need to recommend the virtual machine size for each host pool to meet the session host requirements.



ANSWER:



Explanation:

Azure Virtual Desktop session-host sizing should match the resource profile of the applications and user sessions that each host pool will run. The completed mapping correctly uses **F-Series** for HostPool1, **E-Series** for HostPool2, and **N-Series** for HostPool3.

F-Series virtual machines are compute optimized. They provide a higher CPU-to-memory ratio, making them appropriate for the host pool whose sessions need substantial processor capacity. This type of sizing is useful where the primary constraint is CPU processing performed by the session-host workloads, rather than exceptionally large RAM requirements.

E-Series virtual machines are memory optimized. They provide high memory capacity relative to the number of vCPUs and are the appropriate choice for the host pool with memory-intensive user sessions or applications. In Azure Virtual Desktop, the memory needed by the operating system, user sessions, applications, and any background services must all be considered when determining session-host capacity. A memory-optimized series supports this workload profile while maintaining a suitable CPU allocation.

N-Series virtual machines provide GPU capabilities. This makes them the correct choice for the host pool that requires graphics acceleration, such as workloads involving visual rendering, graphics-heavy applications, or applications designed to use GPU resources. Azure Virtual Desktop can use GPU-enabled session hosts where the application and user experience requirements call for that hardware acceleration.

Microsoft recommends selecting Azure VM families based on the CPU, memory, storage, networking, and GPU needs of the actual workload, then validating the selected configuration through monitoring and testing. The mapping shown follows those VM-family roles. See Microsoft's Azure VM sizes overview and Azure Virtual Desktop sizing guidelines for sizing guidance.

QUESTION NO: 25

You have an Azure subscription that contains an Azure Virtual Desktop host pool. The host pool uses FSLogix profile containers.

You need to create a configuration file to prevent specific folders from syncing to the FSLogix profile containers when a user signs out.

How should you name the file?

A. redirections.xml

B. fslogix.config

C. folders.json

D. profile.xm1

ANSWER: A

Explanation:

`redirections.xml` is the required FSLogix redirections configuration filename. FSLogix Profile Container uses this XML file to define folders that should be excluded from the user profile container and redirected to a local location on the session host. This is useful for data that is temporary, easily recreated, large, or unsuitable for persistence in the profile VHD/VHDX, such as selected application caches. At user sign-in, FSLogix reads the redirections rules and applies the folder exclusions; because the excluded folders are redirected outside the mounted profile container, their contents are not written back to the container when the user signs out. For Profile Container, the file must be named exactly `redirections.xml` and placed in `C:\ProgramData\FSLogix\Profiles` on each applicable session host. The XML content must use the FSLogix-supported redirection schema and entries. Microsoft documents the required filename, location, and XML structure in its FSLogix redirections guidance: FSLogix redirections.xml. For broader Profile Container behavior and configuration context, see FSLogix Profile Container.

QUESTION NO: 26

You have an Azure Virtual Desktop host pool in the East US region.

You need to implement a disaster recovery solution that meets the following requirements:

▪ If users cannot connect to the Azure Virtual Desktop resources in the East US region, the users must be able to connect to the equivalent resources in the West US region. ▪ Users must connect to the Azure Virtual Desktop resources in either the East US or the West US region by selecting a single icon in the Remote Desktop clientю ▪ In the event of a disaster, failover between the Azure regions must be initiated manually by an administrator. ▪ Failover times must be minimized.

What should you do?

A. Configure a shared image gallery that has replicas in the East US and West US regions

B. Create new session hosts in the West US region and add the session hosts to an existing host pool

C. Create an additional host pool in the West US region

D. Enable Azure Site Recovery replication of the virtual machines to the West US region

E. Enable Azure Backup to a Recovery Services vault in the West US region

ANSWER: A B

Explanation:

Configure a shared image gallery that has replicas in the East US and West US regions, and create new session hosts in the West US region and add the session hosts to an existing host pool. Replicating the approved session-host image to West US ensures that an equivalent, validated image is locally available in the recovery region. This avoids the cross-region image-copy delay that could occur during a regional outage and supports rapid, consistent deployment or replacement of session hosts.

Adding pre-provisioned West US session hosts to the existing host pool provides the required single Remote Desktop client resource icon because users continue to access the same Azure Virtual Desktop host-pool resource. The administrator can manually control the failover by preventing new connections to the East US session hosts, such as by placing them in drain mode, and allowing connections to the West US hosts. Because the secondary session hosts already exist and are registered to the host pool, users can be routed to the recovery-region capacity without waiting for virtual-machine replication or a separate host-pool publication process. Azure Virtual Desktop host pools can contain session hosts deployed in more than one Azure region within the supported geography. See Azure Virtual Desktop disaster recovery and Azure Virtual Desktop host pool load balancing.

QUESTION NO: 27 - (SIMULATION)

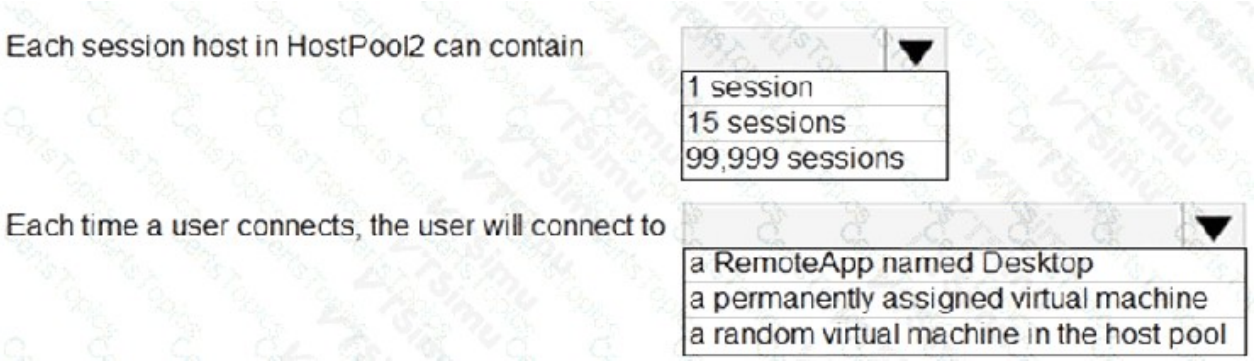
You are automating the deployment of an Azure Virtual Desktop host pool.

You deploy the Azure Resource Manager (ARM) template shown in the following exhibit.

```
{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "hostpools_HostPool2_name": {
            "defaultValue": "HostPool2",
            "type": "String"
        }
    },
    "variables": {},
    "resources": [
        {
            "type": "Microsoft.DesktopVirtualization/hostpools",
            "apiVersion": "2020-11-02-preview",
            "name": "[parameters('hostpools_HostPool2_name')]",
            "location": "eastus",
            "properties": {
                "hostPoolType": "Personal",
                "personalDesktopAssignmentType": "Automatic",
                "maxSessionLimit": 999999,
                "loadBalancerType": "Persistent",
                "validationEnvironment": false,
                "registrationInfo": {
                    "registrationTokenOperation": "None"
                },
                "preferredAppGroupType": "Desktop",
                "startVMOnConnect": false
            }
        }
    ]
}
```

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the Dockerfile.

NOTE: Each correct selection is worth one point.



ANSWER: See the explanation for the answer

Explanation:

Select:

The template configures `hostPoolType` as `Personal`. A personal Azure Virtual Desktop host pool provides one session per session host and assigns a dedicated session host to each user. Because `personalDesktopAssignmentType` is `Automatic`, a user is automatically assigned an available VM on their first connection and subsequently reconnects to that same permanently assigned VM.

QUESTION NO: 28

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure Virtual Desktop deployment

You need to ensure that users are signed out automatically when they disconnect from a session.

Solution: From the Local Group Policy Editor, you configure the Connections settings.

Does this meet the goal?

A. Yes

B. No

ANSWER: B

Explanation:

No is correct. Configuring policies in the Remote Desktop Session Host *Connections* node does not configure automatic sign-out after a user disconnects. To achieve the stated goal on Azure Virtual Desktop session hosts, configure the *Set time limit for disconnected sessions* policy in Local Group Policy Editor under Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Session Time Limits. This policy specifies how long a disconnected Remote Desktop session can remain active before it is ended. Ending the disconnected session signs the user out and releases the session's processes and resources. A time value appropriate to the organization's security and user-experience requirements must be selected; for example, a short timeout ensures disconnected users do not remain signed in indefinitely. Microsoft documents this policy as part of Remote Desktop Services session-time-limit management, and Azure Virtual Desktop supports applying these policies to session hosts through local policy, Active Directory Group Policy, or Microsoft Intune. See Azure Virtual Desktop session host configuration and Remote Desktop Services policy and configuration documentation.

QUESTION NO: 29

You need to recommend an authentication solution that meets the performance requirements.

Which two actions should you include in the recommendation? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Join all the session hosts to Azure AD.

B. In each Azure region that will contain the Azure Virtual Desktop session hosts, create an Azure Active Directory Domain Service (Azure AD DS) managed domain.

C. Deploy domain controllers for the on-premises Active Directory domain on Azure virtual machines to the new sites..

D. Deploy read-only domain controllers (RODCs) on Azure virtual machines to the new sites.

E. In each Azure region that will contain the Azure Virtual Desktop session hosts, create an Active Directory site.

ANSWER: C E

Explanation:

Deploying domain controllers for the on-premises Active Directory domain on Azure virtual machines in the new sites places writable Active Directory Domain Services capacity close to the Azure Virtual Desktop session hosts. This reduces dependency on WAN latency for domain logons, Kerberos authentication, Group Policy processing, and directory lookups. Azure Virtual Desktop hosts that are joined to an Active Directory domain require reliable connectivity to domain controllers, so locally available domain controllers help provide predictable authentication performance and resiliency.

Creating an Active Directory site in every Azure region containing session hosts lets Active Directory map the Azure virtual network subnets to the appropriate regional site. Clients and session hosts can then use the AD site topology to locate nearby domain controllers rather than selecting remote controllers across regions. The site design should include the Azure subnets and appropriate site links, allowing authentication traffic and replication to follow an intentional topology. Together, regional AD sites and regional domain controllers provide low-latency directory services for the Azure Virtual Desktop deployment. Microsoft's guidance for Azure Virtual Desktop domain join scenarios and Active Directory site topology is available in Azure AD-joined session hosts and Designing the site topology for Active Directory Domain Services.

QUESTION NO: 30

You have an Azure Virtual Desktop deployment that contains a host pool. The host pool contains 10 session hosts. The session hosts are configured by using a custom image and ephemeral disks.

You need to deploy Microsoft OneDrive for Business.

Which two actions should you perform for each session host? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Install FSLogix.

B. Install the OneDrive sync app by using the per-machine installation option.

C. Implement Application Masking.

D. Install the OneDrive sync app by using the per-user installation option.

E. Deploy an MSIX app attach package.

ANSWER: A B

Explanation:

Install FSLogix and install the OneDrive sync app by using the per-machine installation option. In a multi-session Azure Virtual Desktop environment, several users can sign in to the same session host. FSLogix Profile Containers store each user's profile data in a centrally located container, which follows the user across session hosts. This is particularly important when the hosts use ephemeral OS disks, because changes written to the local operating-system disk are not persistent after a host is reimaged or redeployed. FSLogix also supports the OneDrive sync client in virtual desktop infrastructure scenarios by ensuring that the user-specific OneDrive configuration and synchronized content are associated with the user profile rather than the disposable local host.

The OneDrive sync app must be installed once for all users on a shared or virtualized Windows device. The per-machine installation places the application in the system program-files location and makes it available to every user who signs in, avoiding separate per-user application installations on each session host. Microsoft documents the per-machine OneDrive installation command and specifically identifies it as the appropriate installation model for computers used by multiple users. Together, profile persistence through FSLogix and a shared per-machine OneDrive client provide a supported, durable deployment for this host pool. See FSLogix Profile Containers and Per-machine installation for the OneDrive sync app.

QUESTION NO: 31

You have an Azure Virtual Desktop deployment that contains a host pool named Pool1. Pool1 contains three session hosts.

You need to implement a private endpoint connection for Pool1.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Create a private endpoint by using the global target sub-resource.

B. Create a private endpoint by using the connection target sub-resource.

C. Create a private endpoint by using the feed target sub-resource.

D. Reregister the Microsoft.Desktopvirtualization resource provider for the Azure subscription.

E. Reregister the Microsoft.virtualMachinceImages resource provider for the Azure subscription.

ANSWER: B D

Explanation:

To provide Private Link connectivity for an Azure Virtual Desktop host pool, create the private endpoint with the **connection** target sub-resource. This sub-resource is specifically used for the Azure Virtual Desktop connection service, allowing session hosts in the host pool to communicate with the service through a private endpoint rather than through its public endpoint. The private endpoint is placed in a virtual network subnet, and appropriate private DNS resolution must be available so that the relevant Azure Virtual Desktop service name resolves to the private IP address.

You must also reregister the **Microsoft.Desktopvirtualization** resource provider in the subscription. Microsoft documents this as a required preparation step when configuring Azure Virtual Desktop Private Link. Reregistering updates the subscription's resource-provider registration so that it supports the Azure Virtual Desktop Private Link functionality and its associated private endpoint target sub-resources. After registration has completed, the connection private endpoint can be created and associated with the host pool's service connectivity requirements.

For implementation details and the required DNS configuration, see Azure Virtual Desktop Private Link and Azure resource providers and types.

QUESTION NO: 32

You have an Azure Virtual Desktop deployment.

You use Hyper-V to create a virtual machine that runs Windows 11 and has the following configurations:

• Virtual machine generation: Generation 2

• Disk type: Dynamically expanding

• Disk format: VHDX

• Disk size: 2 TB

You need to prepare the virtual machine before uploading it to Azure.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Change the disk type to fixed.

B. Change the virtual machine generation to generation 1.

C. Change the disk type to differencing.

D. Decrease the disk size to 1 TB.

E. Change the disk format to VHD.

ANSWER: A E

Explanation:

Change the disk type to fixed. is required because Azure requires an uploaded virtual hard disk to be a fixed-size VHD. A dynamically expanding disk must be converted before upload so that the disk has a defined physical size and is in an Azure-supported upload format. In Hyper-V, this can be done by using the Edit Disk wizard or the `Convert-VHD` PowerShell cmdlet, selecting a fixed disk as the destination type.

Change the disk format to VHD. is also required. Although Hyper-V supports the newer VHDX format, Azure uploads for creating managed disks require the legacy VHD format. The conversion process should therefore produce a fixed-size VHD, retaining the virtual disk's content while making it suitable for Azure storage and managed-disk creation. Generation 2 virtual machines are supported in Azure, so the generation does not need to be changed as part of this preparation. Microsoft's image-upload guidance explicitly states that the source disk must be converted to a fixed VHD before it is uploaded. See Prepare a Windows VHD or VHDX to upload to Azure and Upload a VHD to Azure or copy a managed disk to another region.

QUESTION NO: 33

You have an Azure Virtual Desktop deployment that uses Microsoft Entra ID.

You need to require users to perform multifactor authentication when they access Azure Virtual Desktop resources.

Which two settings should you configure in a Conditional Access policy? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Target the Azure Virtual Desktop cloud app.

B. Configure the Require multifactor authentication grant control.

C. Target the Azure Resource Manager cloud app.

D. Configure the Require device to be marked as compliant grant control only.

E. Configure a device compliance policy in Microsoft Intune only.

ANSWER: A B

Explanation:

Target the **Azure Virtual Desktop** cloud app and configure the grant control to require multifactor authentication. Conditional Access evaluates user access to cloud applications. Targeting Azure Virtual Desktop applies the policy to Azure Virtual Desktop connection and resource access scenarios for the selected users or groups.

The Require multifactor authentication grant control enforces MFA before access is granted. The policy can also include exclusions for emergency access accounts and can be scoped to specific users, groups, device platforms, locations, or risk conditions as required by the organization's security design.

For more information, see Configure multifactor authentication for Azure Virtual Desktop and What is Conditional Access in Microsoft Entra ID?.

QUESTION NO: 34

You have an Azure Virtual Desktop host pool named Pool1 and an Azure Storage account named Storage1. Storage1 stores FSLogix profile containers in a share folder named share1.

You create a new group named Group1. You provide Group1 with permission to sign in to Pool1.

You need to ensure that the members of Group1 can store the FSLogix profile containers in share1. The solution must use the principle of least privilege.

Which two privileges should you assign to Group1? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. the Storage Blob Data Contributor role for storage1

B. the List folder / read data NTFS permissions for share1

C. the Modify NTFS permissions for share1

D. the Storage File Data SMB Share Reader role for storage1

E. the Storage File Data SMB Share Elevated Contributor role for storage1

F. the Storage File Data SMB Share Contributor role for storage1

ANSWER: C F

Explanation:

Assign **the Storage File Data SMB Share Contributor role for storage1** and **the Modify NTFS permissions for share1**. Access to an Azure Files share through SMB using Active Directory-based authentication requires both an Azure RBAC data-plane role and appropriate Windows file and directory permissions. The Storage File Data SMB Share Contributor role provides the data-plane authority needed to read, create, modify, and delete files and directories in the Azure file share without granting storage-account management permissions. This is the least-privileged built-in Azure role that supports normal FSLogix profile-container use.

FSLogix mounts a user’s profile container as a virtual hard disk and must be able to create the user’s container when necessary and update its contents throughout the session. Applying Modify NTFS permissions to Group1 on share1 provides the needed file-system-level access for these operations, including creating and changing the profile container, while avoiding unnecessarily broad ownership or full-control permissions. Together, the SMB Share Contributor role and Modify permissions satisfy the two authorization layers evaluated for SMB access to Azure Files. Microsoft describes the Azure RBAC and NTFS permission requirements for Azure Files SMB access in Enable Active Directory authentication over SMB for Azure file shares and FSLogix profile storage guidance in Store FSLogix profiles.