AZ-600$^{Q\&As}$

Configuring and Operating a Hybrid Cloud with Microsoft Azure Stack Hub

Pass Microsoft AZ-600 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/az-600.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

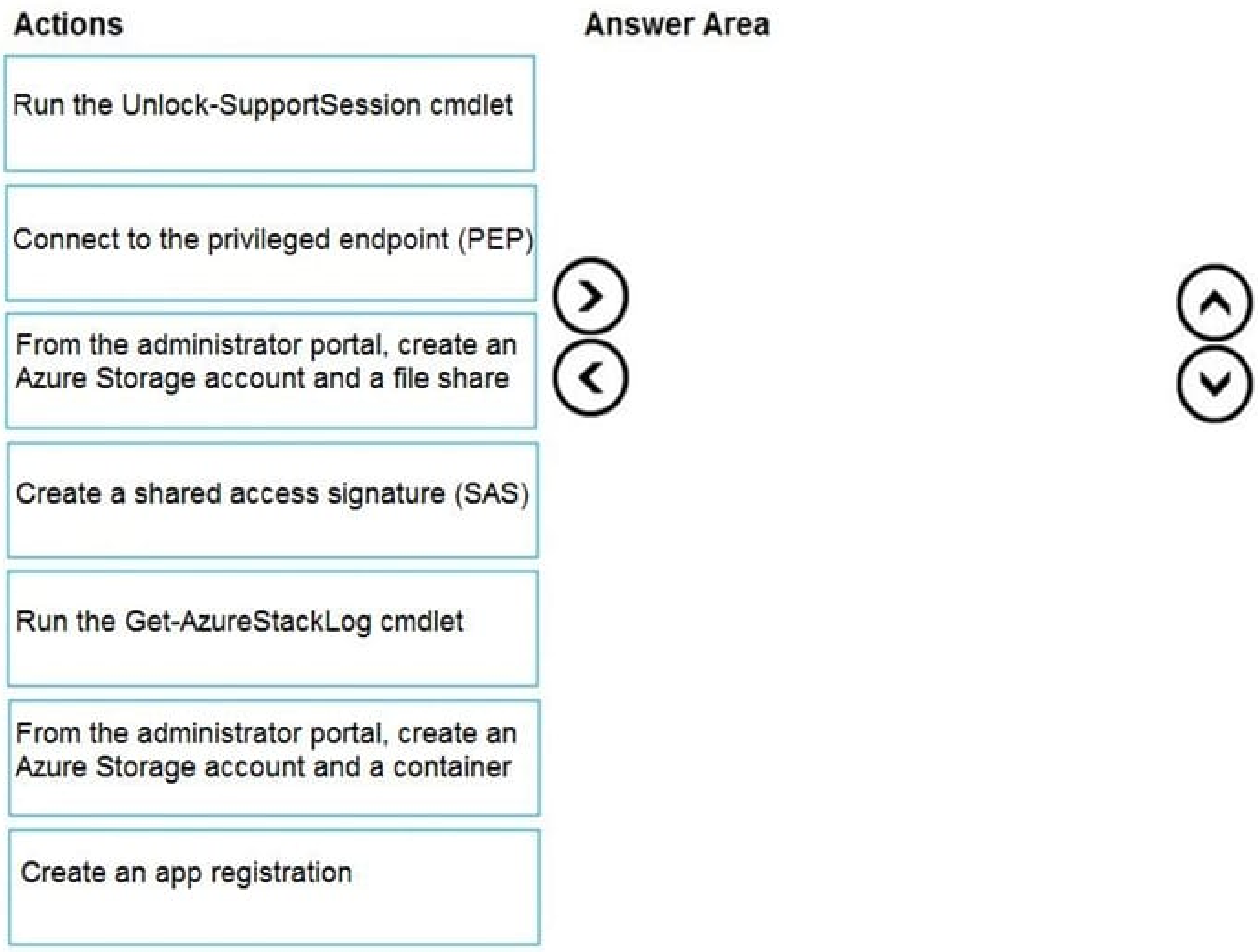
DRAG DROP

You have an Azure Stack Hub integrated system that is disconnected from the Internet.

You need to collect diagnostic logs, but do not have access to an SMB share.

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.

Select and Place:



Actions

Run the Unlock-SupportSession cmdlet

Connect to the privileged endpoint (PEP)

From the administrator portal, create an Azure Storage account and a file share

Create a shared access signature (SAS)

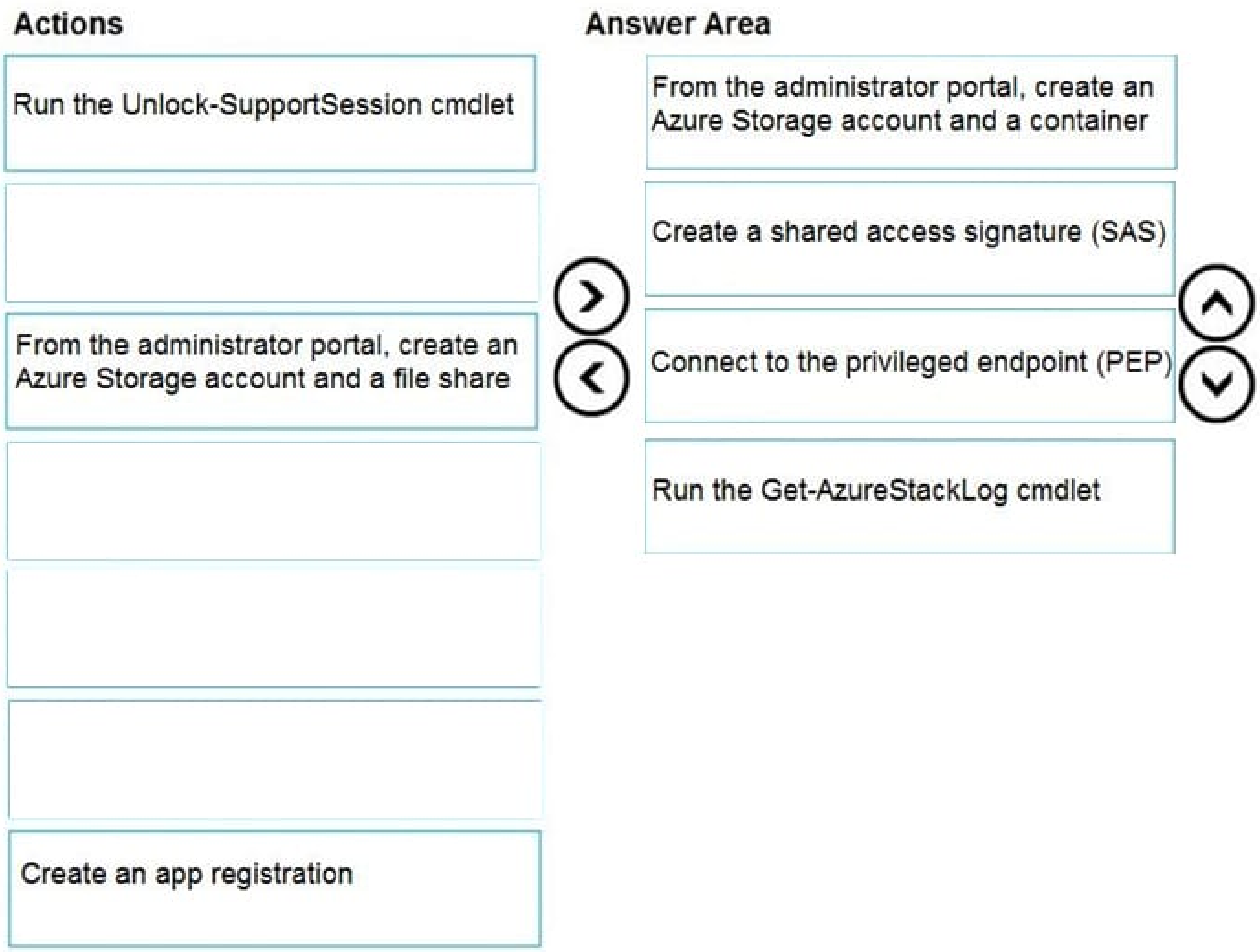
Run the Get-AzureStackLog cmdlet

From the administrator portal, create an Azure Storage account and a container

Create an app registration

Answer Area

Correct Answer:



Actions

Run the Unlock-SupportSession cmdlet

From the administrator portal, create an Azure Storage account and a file share

Create an app registration

Answer Area

From the administrator portal, create an Azure Storage account and a container

Create a shared access signature (SAS)

Connect to the privileged endpoint (PEP)

Run the Get-AzureStackLog cmdlet

Reference: https://docs.microsoft.com/en-us/azure-stack/operator/azure-stack-get-azurestacklog?view=azs-2008

QUESTION 2

You have a connected Azure Stack Hub integrated system that contains a user named User1.

You need to ensure that User1 can onboard a new guest tenant directory. The solution must use the principle of least privilege.

Which role should you assign to User1?

A. Owner

B. Global administrator

C. Hybrid identity administrator

D. Domain name administrator

Correct Answer: C

Hybrid Identity Administrator role is now available with Cloud Provisioning Type: New feature Service category: Azure AD Cloud Provisioning Product capability: Identity Lifecycle Management

IT Admins can start using the new "Hybrid Admin" role as the least privileged role for setting up Azure AD Connect Cloud Provisioning. With this new role, you no longer have to use the Global Admin role to set up and configure Cloud Provisioning.

Note: Hybrid Identity Administrator Users in this role can create, manage and deploy provisioning configuration setup from AD to Azure AD using Cloud Provisioning as well as manage Azure AD Connect, Pass-through Authentication (PTA), Password hash synchronization (PHS), Seamless Single Sign-On (Seamless SSO), and federation settings. Users can also troubleshoot and monitor logs using this role.

Reference: https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/whats- new-archive

https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions- reference#hybrid-identity-administrator

QUESTION 3

HOTSPOT

You have an Azure Stack Hub Integrated system.

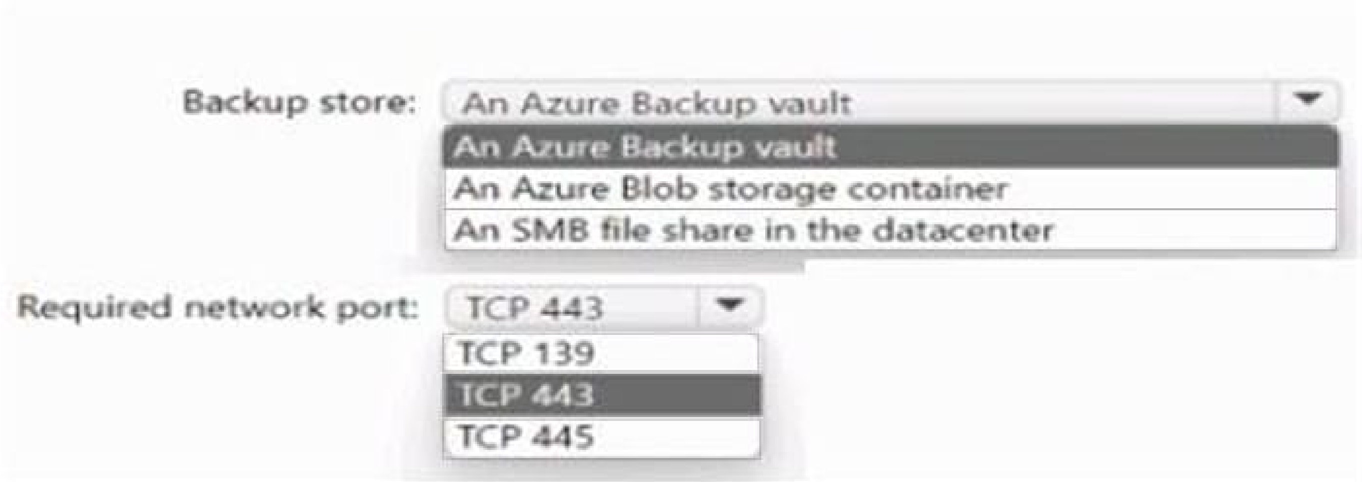
Outbound traffic from the Azure Stack Hub integrated system is controlled by a third-party firewall.

You need to implement the Infrastructure Backup Service.

Which storage location should you use for the backup, and which network port is required to perform the backup? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



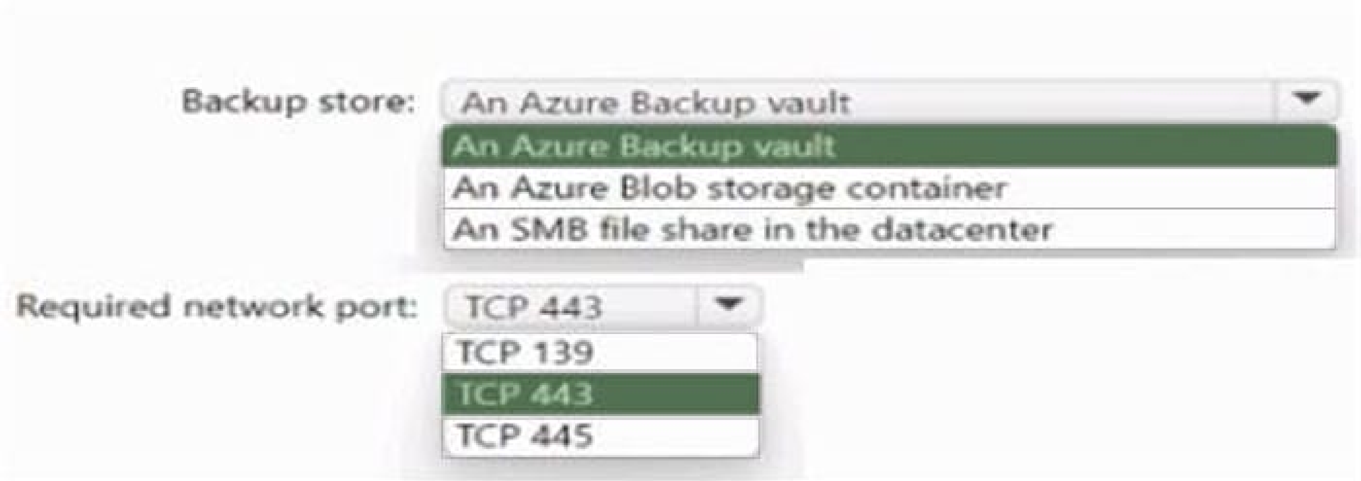
Backup store: An Azure Backup vault

- An Azure Backup vault
- An Azure Blob storage container
- An SMB file share in the datacenter

Required network port: TCP 443

- TCP 139
- TCP 443
- TCP 445

Correct Answer:



Backup store: An Azure Backup vault

- An Azure Backup vault
- An Azure Blob storage container
- An SMB file share in the datacenter

Required network port: TCP 443

- TCP 139
- TCP 443
- TCP 445

QUESTION 4

You need to configure the log forwarding. The solution must meet the Azure Stack Hub requirements. What should you do?

A. Connect to 192.168.101.101 and run the Set-EventLogLevel and Add-AzLogProfile cmdlets.

B. Connect to 192.168.100.224 and run the Set-SyslogServer and Set-SyslogClient cmdlets.

C. Connect to 192.168.100.224 and run the Set-EventLogLevel and Add-AzLogProfile cmdlets.

D. Connect to 192.168.101.101 and run the Set-SyslogServer and Set-SyslogClient cmdlets.

Correct Answer: D

Integrate Azure Stack Hub with monitoring solutions using syslog forwarding The syslog channel exposes audits, alerts, and security logs from all the components of the Azure Stack Hub infrastructure. Use syslog forwarding to integrate with security monitoring solutions and to retrieve all audits, alerts, and security logs to store them for retention. Cmdlets to configure syslog forwarding Configuring syslog forwarding requires access to the privileged endpoint (PEP). Two PowerShell cmdlets have been added to the PEP to configure the syslog forwarding: ### cmdlet to pass the syslog server information to the client and to configure the transport protocol, the encryption and the authentication between the client and the server Set-SyslogServer [-ServerName] [-ServerPort] [-NoEncryption] [-SkipCertificateCheck] [-SkipCNCheck] [-UseUDP] [-Remove]### cmdlet to configure the certificate for the syslog client to authenticate with the server Set-SyslogClient [-pfxBinary] [-CertPassword]

Reference: https://learn.microsoft.com/en-us/azure-stack/operator/azure-stack-integrate-security

QUESTION 5

DRAG DROP

You have an Azure Stack Hub integrated system.

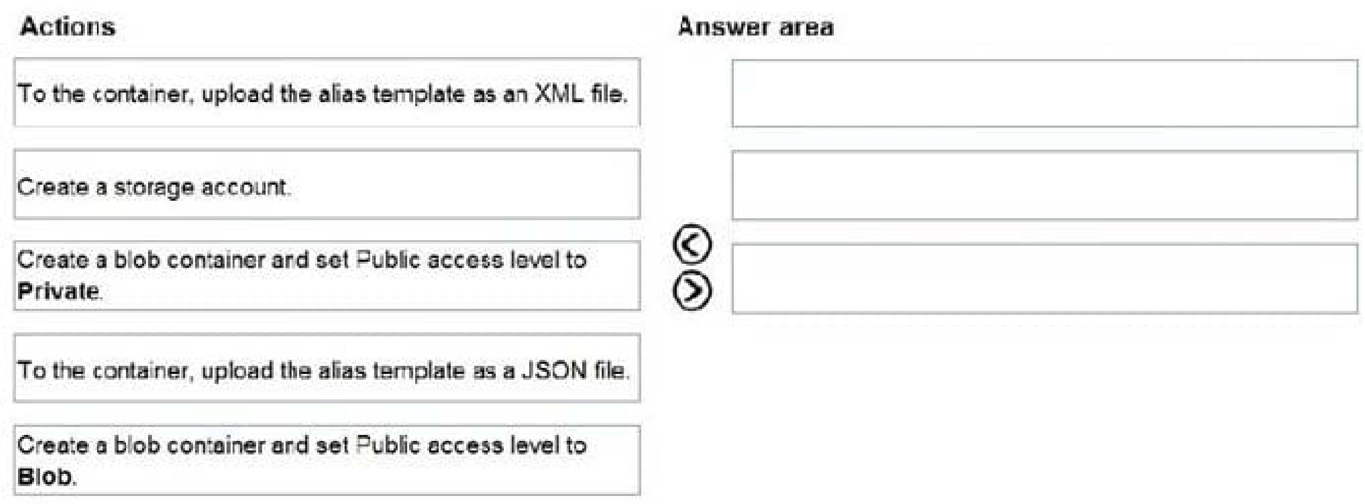
You plan to enable Azure Command-Line Interface (CLI) for Azure Stack Hub users.

You create an alias template file.

You need to configure the virtual machine aliases endpoint. The solution must use the principle of least privilege.

Which three 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.

Select and Place:



Actions

To the container, upload the alias template as an XML file.

Create a storage account.

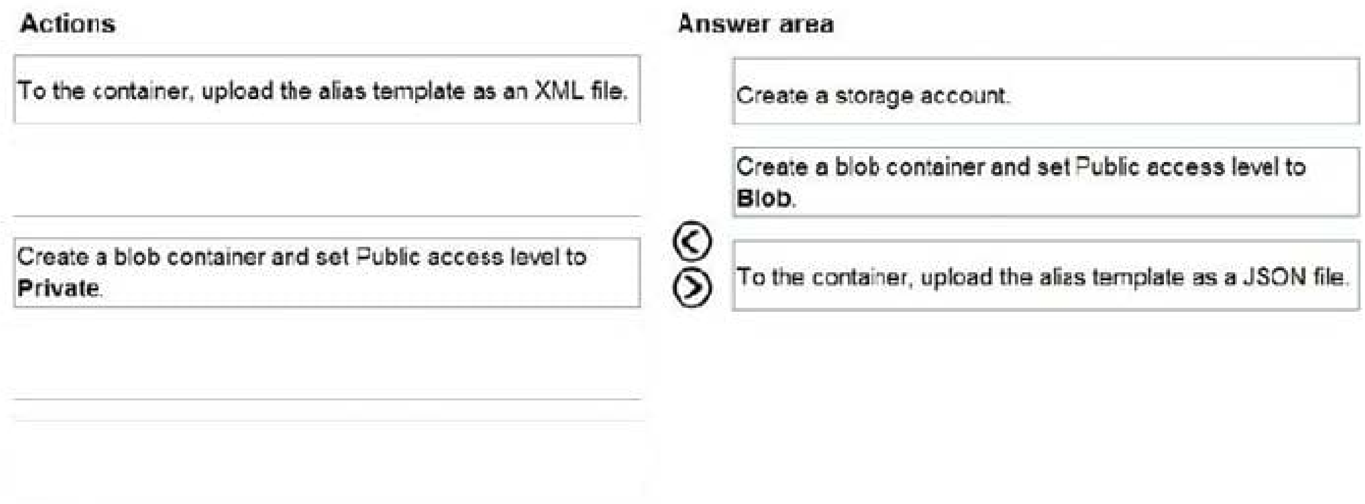
Create a blob container and set Public access level to **Private**.

To the container, upload the alias template as a JSON file.

Create a blob container and set Public access level to **Blob**.

Answer area

Correct Answer:



Actions

To the container, upload the alias template as an XML file.

Create a blob container and set Public access level to **Private**.

Answer area

Create a storage account.

Create a blob container and set Public access level to **Blob**.

To the container, upload the alias template as a JSON file.

Step 1: Create a storage account A sample alias file with many common image aliases is available. You can use that as a starting point. Host this file in a space where your CLI clients can reach it. One way is to host the file in a blob storage account and share the URL with your users:

1.

Download the sample file from GitHub.

2.

Create a storage account in Azure Stack Hub (Step 1). When that\\'s done, create a blob container. Set the access policy to "public." (Step 2)

3.

Upload the JSON file to the new container (Step 3). When that\\'s done, you can view the URL of the blob. Select the blob name and then select the URL from the blob properties.

Step 2: Create a blob container and set the Public access to Blob. Set up the VM aliases endpoint

Azure Stack Hub operators should set up a publicly accessible endpoint that hosts a VM alias file. The VM alias file is a JSON file that provides a common name for an image. You use the name when you deploy a VM as an Azure CLI parameter.

Note: When public access is allowed for a storage account, you can configure a container with the following permissions:

*

Public read access for blobs only: Blobs within the container can be read by anonymous request, but container data is not available anonymously. Anonymous clients cannot enumerate the blobs within the container.

*

Public read access for container and its blobs: Container and blob data can be read by anonymous request, except for container permission settings and container metadata. Clients can enumerate blobs within the container by anonymous request, but cannot enumerate containers within the storage account.

*

No public read access: The container and its blobs can be accessed only with an authorized request. This option is the default for all new containers. Step 3: To the container, upload the alias template as a JSON file.

AZ-600 VCE Dumps AZ-600 Exam Questions AZ-600 Braindumps