



CertyIQ

Premium exam material

Get certification quickly with the CertyIQ Premium exam material.
Everything you need to prepare, learn & pass your certification exam easily. Lifetime free updates
First attempt guaranteed success.

<https://www.CertyIQ.com>



CompTIA

About CertyIQ

We here at CertyIQ eventually got enough of the industry's greedy exam paid for. Our team of IT professionals comes with years of experience in the IT industry Prior to training CertyIQ we worked in test areas where we observed the horrors of the paywall exam preparation system.

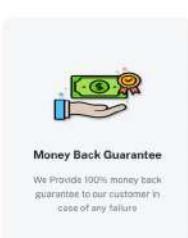
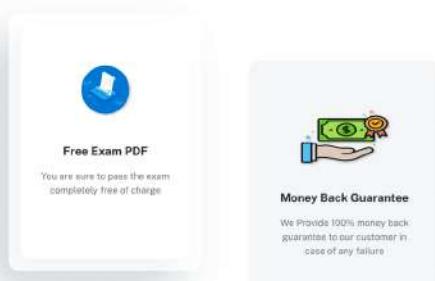
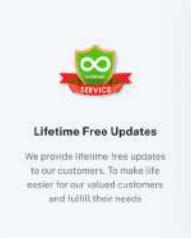
The misuse of the preparation system has left our team disillusioned. And for that reason, we decided it was time to make a difference. We had to make In this way, CertyIQ was created to provide quality materials without stealing from everyday people who are trying to make a living.

Doubt Support

We have developed a very scalable solution using which we are able to solve 400+ doubts every single day with an average rating of 4.8 out of 5.

<https://www.certyiq.com>

Mail us on - certyiqofficial@gmail.com



John

October 19, 2022



Thanks you so much for your help. I scored 972 in my exam today. More than 90% were from your PDFs!

October 22, 2022



Passed my exam today with 891 marks. Out of 52 questions, 51 were from certyiq PDFs including Contoso case study. Thank You certyiq team!

Dana

September 04, 2022



Thanks a lot for this updated AZ-900 Q&A. I just passed my exam and got 974, I followed both of your Az-900 videos and the 6 PDF, the PDFs are very much valid, all answers are correct. Could you please create a similar video/PDF for DP900, your content/PDF's is really awesome. The team did a really good job. Thank You 😊.

Henry Rome

2 months ago



These questions are real and 100 % valid. Thank you so much for your efforts, also your 4 PDFs are awesome, I passed the DP900 exam on 1 Sept. With 968 marks. Thanks a lot, buddy!

Esmaria

2 months ago



Simple easy to understand explanations. To anyone out there wanting to write AZ900, I highly recommend 6 PDF's. Thank you so much, appreciate all your hard work in having such great content. Passed my exam Today - 3 September with 942 score.

Ahamed Shibly

2 months ago



Customer support is realy fast and helpful, I just finished my exam and this video along with the 6 PDF helped me pass! Definitely recommend getting the PDFs. Thank you!



(AZ-104)

Microsoft Azure Administrator

Total: **608 Questions**

Link: <https://certiq.com/papers/microsoft/az-104>

Question: 1

CertyIQ

Your company has several departments. Each department has a number of virtual machines (VMs).

The company has an Azure subscription that contains a resource group named RG1.

All VMs are located in RG1.

You want to associate each VM with its respective department.

What should you do?

- A. Create Azure Management Groups for each department.
- B. Create a resource group for each department.
- C. Assign tags to the virtual machines.
- D. Modify the settings of the virtual machines.

Answer: C**Explanation:**

C. Assign tags to the virtual machines.

By assigning tags, you can organize resources in a way that makes sense for your organization, which will allow you to easily filter and view resources based on criteria such as department, environment, or cost center. In this case, you can create a tag called "Department" and assign the appropriate value to each VM.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags>

Question: 2

CertyIQ

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company has an Azure Active Directory (Azure AD) subscription.

You want to implement an Azure AD conditional access policy.

The policy must be configured to require members of the Global Administrators group to use Multi-Factor Authentication and an Azure AD-joined device when they connect to Azure AD from untrusted locations.

Solution: You access the multi-factor authentication page to alter the user settings.

Does the solution meet the goal?

- A. Yes
- B. No

Answer: B**Explanation:**

B. The solution does not meet the goal. While accessing the multi-factor authentication page allows you to configure multi-factor authentication for users, it does not specifically target the members of the Global Administrators group. To meet the goal of requiring Global Administrators to use Multi-Factor Authentication and an Azure AD-joined device when connecting from untrusted locations, you need to set up an Azure AD conditional access policy.

Question: 3

CertyIQ

Note: The question is included in a number of questions that depicts the identical set-up. However, every question

has a distinctive result. Establish if the solution satisfies the requirements.

Your company has an Azure Active Directory (Azure AD) subscription.

You want to implement an Azure AD conditional access policy.

The policy must be configured to require members of the Global Administrators group to use Multi-Factor Authentication and an Azure AD-joined device when they connect to Azure AD from untrusted locations.

Solution: You access the Azure portal to alter the session control of the Azure AD conditional access policy.

Does the solution meet the goal?

A. Yes

B. No

Answer: B

Explanation:

B. No.

Azure AD Conditional Access policies allow you to control how users access resources based on conditions like location, device compliance, and risk level.

Session controls in Conditional Access define how long sessions remain valid or restrict access based on security signals.

However, altering session control does not directly enforce or change authentication behavior for specific applications or services beyond session duration and restrictions.

Question: 4

CertyIQ

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company has an Azure Active Directory (Azure AD) subscription.

You want to implement an Azure AD conditional access policy.

The policy must be configured to require members of the Global Administrators group to use Multi-Factor Authentication and an Azure AD-joined device when they connect to Azure AD from untrusted locations.

Solution: You access the Azure portal to alter the grant control of the Azure AD conditional access policy.

Does the solution meet the goal?

A. Yes

B. No

Answer: A

Explanation:

A .YES.

Within a Conditional Access policy:

Access Control GRANT: an administrator can use access controls to grant or block access to resources.

Access Control SESSION: an administrator can make use of session controls to enable limited experiences within specific cloud applications.

Reference:

<https://docs.google.com/document/d/1LFqUi7YcKI2d8cs8LnHLGjyHtuXUnz0xik4bpAvZ5fg/edit?usp=sharing>

<https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-grant>

Question: 5

CertyIQ

You are planning to deploy an Ubuntu Server virtual machine to your company's Azure subscription. You are required to implement a custom deployment that includes adding a particular trusted root certification authority (CA).

Which of the following should you use to create the virtual machine?

- A. The New-AzureRmVm cmdlet.
- B. The New-AzVM cmdlet.
- C. The Create-AzVM cmdlet.
- D. The az vm create command.

Answer: D

Explanation:

The az vm create command. you need to create an Ubuntu Linux VM using a cloud-init script for configuration.

For example, az vm create -g MyResourceGroup -n MyVm --image debian --custom-data MyCloudInitScript.yml

Reference:

<https://docs.microsoft.com/en-us/cli/azure/vm?view=azure-cli-latest>

<https://cloudinit.readthedocs.io/en/latest/topics/examples.html>

Question: 6

CertyIQ

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company makes use of Multi-Factor Authentication for when users are not in the office. The Per Authentication option has been configured as the usage model.

After the acquisition of a smaller business and the addition of the new staff to Azure Active Directory (Azure AD) obtains a different company and adding the new employees to Azure Active Directory (Azure AD), you are informed that these employees should also make use of Multi-Factor Authentication.

To achieve this, the Per Enabled User setting must be set for the usage model.

Solution: You reconfigure the existing usage model via the Azure portal.

Does the solution meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Since it is not possible to change the usage model of an existing provider as it is right now, you have to create a new one and reactivate your existing server with activation credentials from the new provider.

Reference:

Question: 7

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company's Azure solution makes use of Multi-Factor Authentication for when users are not in the office. The Per Authentication option has been configured as the usage model.

After the acquisition of a smaller business and the addition of the new staff to Azure Active Directory (Azure AD) obtains a different company and adding the new employees to Azure Active Directory (Azure AD), you are informed that these employees should also make use of Multi-Factor Authentication.

To achieve this, the Per Enabled User setting must be set for the usage model.

Solution: You reconfigure the existing usage model via the Azure CLI.

Does the solution meet the goal?

A. Yes

B. No

Answer: B

Explanation:

The solution provided does not meet the goal of configuring the Per Enabled User setting for the new employees to use Multi-Factor Authentication. To achieve the desired outcome, the Per Enabled User setting should be configured directly for the new employees, not by reconfiguring the existing usage model via the Azure CLI.

Since it is not possible to change the usage model of an existing provider as it is right now, you have to create a new one and reactivate your existing server with activation credentials from the new provider.

Reference:

Question: 8

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company's Azure solution makes use of Multi-Factor Authentication for when users are not in the office. The Per Authentication option has been configured as the usage model.

After the acquisition of a smaller business and the addition of the new staff to Azure Active Directory (Azure AD) obtains a different company and adding the new employees to Azure Active Directory (Azure AD), you are informed that these employees should also make use of Multi-Factor Authentication.

To achieve this, the Per Enabled User setting must be set for the usage model.

Solution: You create a new Multi-Factor Authentication provider with a backup from the existing Multi-Factor Authentication provider data.

Does the solution meet the goal?

A. Yes

B. No

Answer: B

Explanation:

continue to be used and updated, but migration is no longer possible. Multi-factor authentication will continue to be available as a feature in Azure AD Premium licenses.

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-authprovider>

Question: 9

CertyIQ

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company has an Azure Active Directory (Azure AD) tenant named `weyland.com` that is configured for hybrid coexistence with the on-premises Active Directory domain.

You have a server named `DirSync1` that is configured as a DirSync server.

You create a new user account in the on-premise Active Directory. You now need to replicate the user information to Azure AD immediately.

Solution: You run the `Start-ADSyncSyncCycle -PolicyType Initial` PowerShell cmdlet.

Does the solution meet the goal?

A. Yes

B. No

Answer: B

Explanation:

NO Initial will perform a full sync and add the user account created but it will take time,

Delta, will kick off a delta sync and bring only the last change, so it will be "immediately" and will fulfill the requirements.

Question: 10

CertyIQ

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company has an Azure Active Directory (Azure AD) tenant named `weyland.com` that is configured for hybrid coexistence with the on-premises Active Directory domain.

You have a server named `DirSync1` that is configured as a DirSync server.

You create a new user account in the on-premise Active Directory. You now need to replicate the user information to Azure AD immediately.

Solution: You use Active Directory Sites and Services to force replication of the Global Catalog on a domain controller.

Does the solution meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Using Active Directory Sites and Services to force replication of the Global Catalog on a domain controller does not directly impact the synchronization process between the on-premises Active Directory and Azure AD.

To replicate the new user information to Azure AD immediately, you should use Azure AD Connect, the synchronization tool for integrating on-premises Active Directory with Azure AD. Azure AD Connect is

responsible for synchronizing changes between the on-premises environment and Azure AD.

Question: 11

CertyIQ

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company has an Azure Active Directory (Azure AD) tenant named `weyland.com` that is configured for hybrid coexistence with the on-premises Active Directory domain.

You have a server named `DirSync1` that is configured as a DirSync server.

You create a new user account in the on-premise Active Directory. You now need to replicate the user information to Azure AD immediately.

Solution: You restart the `NetLogon` service on a domain controller.

Does the solution meet the goal?

A. Yes

B. No

Answer: B

Explanation:

If you need to manually run a sync cycle, then from PowerShell run `Start-ADSyncSyncCycle -PolicyType Delta`.

To initiate a full sync cycle, run `Start-ADSyncSyncCycle -PolicyType Initial` from a PowerShell prompt.

Running a full sync cycle can be very time consuming, so if you need to replicate the user information to Azure AD immediately then run `Start-ADSyncSyncCycle -PolicyType Delta`.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-feature-scheduler>

Question: 12

CertyIQ

Your company has a Microsoft Azure subscription.

The company has datacenters in Los Angeles and New York.

You are configuring the two datacenters as geo-clustered sites for site resiliency.

You need to recommend an Azure storage redundancy option.

You have the following data storage requirements:

- ⇒ Data must be stored on multiple nodes.
- ⇒ Data must be stored on nodes in separate geographic locations.
- ⇒ Data can be read from the secondary location as well as from the primary location.

Which of the following Azure stored redundancy options should you recommend?

A. Geo-redundant storage

B. Read-only geo-redundant storage

C. Zone-redundant storage

D. Locally redundant storage

Answer: B

Explanation:

RA-GRS allows you to have higher read availability for your storage account by providing read only access to

the data replicated to the secondary location. Once you enable this feature, the secondary location may be used to achieve higher availability in the event the data is not available in the primary region. This is an opt-in feature which requires the storage account be geo-replicated.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy>

Question: 13

CertyIQ

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company has an azure subscription that includes a storage account, a resource group, a blob container and a file share.

A colleague named Jon Ross makes use of a solitary Azure Resource Manager (ARM) template to deploy a virtual machine and an additional Azure Storage account.

You want to review the ARM template that was used by Jon Ross.

Solution: You access the Virtual Machine blade.

Does the solution meet the goal?

A. Yes

B. No

Answer: B

Explanation:

No, accessing the Virtual Machine blade does not provide access to the ARM template used by Jon Ross to deploy the virtual machine and an additional Azure Storage account. The Virtual Machine blade only displays information about the virtual machine itself and its related resources, but not the ARM template used to deploy it.

To review the ARM template used by Jon Ross, you need to access the deployment history of the resource group where the virtual machine and additional storage account were deployed. This will show all deployments made to the resource group, including the ARM template used for the deployment.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-export-template>

Question: 14

CertyIQ

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company has an azure subscription that includes a storage account, a resource group, a blob container and a file share.

A colleague named Jon Ross makes use of a solitary Azure Resource Manager (ARM) template to deploy a virtual machine and an additional Azure Storage account.

You want to review the ARM template that was used by Jon Ross.

Solution: You access the Resource Group blade.

Does the solution meet the goal?

A. Yes

B. No

Answer: A

Explanation:

To view a template from deployment history:

1. Go to the resource group for your new resource group. Notice that the portal shows the result of the last deployment. Select this link.

The screenshot shows the 'Overview' tab selected in the left navigation bar of the Azure Resource Group portal. The main content area displays deployment information. A red box highlights the 'Deployments' section, which shows '1 Succeeded'. Below this, it lists the subscription name as 'Microsoft Azure Consumption' and the subscription ID.

2. You see a history of deployments for the group. In your case, the portal probably lists only one deployment. Select this deployment.

The screenshot shows the deployment history details page. At the top, there are buttons for 'Delete', 'Cancel', 'Redeploy', and 'View template'. Below is a search bar with placeholder text 'Search for deployments by name...'. The main table has columns 'DEPLOYMENT NAME' and 'STATUS'. One deployment is listed: 'Microsoft.WebSiteSQLDatabased1...' with a status of 'Succeeded' indicated by a green checkmark icon. A red box highlights the deployment name.

DEPLOYMENT NAME	STATUS
Microsoft.WebSiteSQLDatabased1...	Succeeded

3. The portal displays a summary of the deployment. The summary includes the status of the deployment and its operations and the values that you provided for parameters. To see the template that you used for the deployment, select View template.

Microsoft.WebSiteSQLDatabase13386b0-9908
Deployment

Actions: Delete Cancel Refresh Redeploy View template

Summary	DEPLOYMENT DATE 7/5/2017 4:01:15 PM
STATUS Succeeded	DURATION 1 minute 30 seconds
RESOURCE GROUP exportsite	RELATED Events

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-export-template>

Question: 15

CertyIQ

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company has an azure subscription that includes a storage account, a resource group, a blob container and a file share.

A colleague named Jon Ross makes use of a solitary Azure Resource Manager (ARM) template to deploy a virtual machine and an additional Azure Storage account.

You want to review the ARM template that was used by Jon Ross.

Solution: You access the Container blade.

Does the solution meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

You should use the Resource Group blade.

No, accessing the Container blade does not provide access to the ARM template used by Jon Ross to deploy the virtual machine and an additional Azure Storage account. The Container blade displays information about the blob container within the storage account, but it does not provide access to the deployment history or ARM templates.

To review the ARM template used by Jon Ross, you need to access the deployment history of the resource

group where the virtual machine and additional storage account were deployed. This will show all deployments made to the resource group, including the ARM template used for the deployment.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-export-template>

Question: 16

CertyIQ

Your company has three virtual machines (VMs) that are included in an availability set.

You try to resize one of the VMs, which returns an allocation failure message.

It is imperative that the VM is resized.

Which of the following actions should you take?

- A. You should only stop one of the VMs.
- B. You should stop two of the VMs.
- C. You should stop all three VMs.
- D. You should remove the necessary VM from the availability set.

Answer: C

Explanation:

If the VM you wish to resize is part of an availability set, then you must stop all VMs in the availability set before changing the size of any VM in the availability set.

The reason all VMs in the availability set must be stopped before performing the resize operation to a size that requires different hardware is that all running VMs in the availability set must be using the same physical hardware cluster. Therefore, if a change of physical hardware cluster is required to change the VM size then all VMs must be first stopped and then restarted one-by-one to a different physical hardware clusters.

Reference:

<https://azure.microsoft.com/es-es/blog/resize-virtual-machines/>

Question: 17

CertyIQ

You have an Azure virtual machine (VM) that has a single data disk. You have been tasked with attaching this data disk to another Azure VM.

You need to make sure that your strategy allows for the virtual machines to be offline for the least amount of time possible.

Which of the following is the action you should take FIRST?

- A. Stop the VM that includes the data disk.
- B. Stop the VM that the data disk must be attached to.
- C. Detach the data disk.
- D. Delete the VM that includes the data disk.

Answer: C

Explanation:

You can simply detach a data disk from one VM and attach it to the other VM without stopping either of the VMs.

Detaching the data disk first ensures that the current VM (Virtual Machine) that includes the data disk can

quickly be brought back online, minimizing its downtime. This action allows you to then attach the disk to the new VM with minimal interruption.

Detaching a disk does not require you to stop or delete the VM, ensuring that the VM itself remains operational for other tasks or configurations that do not involve the detached disk.

Question: 18

CertyIQ

Your company has an Azure subscription.

You need to deploy a number of Azure virtual machines (VMs) using Azure Resource Manager (ARM) templates.

You have been informed that the VMs will be included in a single availability set.

You are required to make sure that the ARM template you configure allows for as many VMs as possible to remain accessible in the event of fabric failure or maintenance.

Which of the following is the value that you should configure for the platformFaultDomainCount property?

- A. 10
- B. 30
- C. Min Value
- D. Max Value

Answer: D

Explanation:

The number of fault domains for managed availability sets varies by region - either two or three per region.

The platformFaultDomainCount property specifies the number of fault domains to be used by the availability set. A fault domain is a group of underlying hardware resources in a data center that share a common power source and network switch, but are physically separated from each other. By distributing virtual machines across fault domains, you can ensure that no single point of failure can take down all of the virtual machines at once.

In Azure, the maximum value for platformFaultDomainCount is 3. This means that an availability set can have up to 3 fault domains. The minimum value for platformFaultDomainCount is 1.

To make sure that the ARM template allows for as many VMs as possible to remain accessible in the event of fabric failure or maintenance, you should set the platformFaultDomainCount property to its maximum value of 3.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/manage-availability>

Question: 19

CertyIQ

Your company has an Azure subscription.

You need to deploy a number of Azure virtual machines (VMs) using Azure Resource Manager (ARM) templates.

You have been informed that the VMs will be included in a single availability set.

You are required to make sure that the ARM template you configure allows for as many VMs as possible to remain accessible in the event of fabric failure or maintenance.

Which of the following is the value that you should configure for the platformUpdateDomainCount property?

- A. 10
- B. 20

- C. 30
- D. 40

Answer: B

Explanation:

Each virtual machine in your availability set is assigned an update domain and a fault domain by the underlying Azure platform. For a given availability set, five non-user-configurable update domains are assigned by default (Resource Manager deployments can then be increased to provide up to 20 update domains) to indicate groups of virtual machines and underlying physical hardware that can be rebooted at the same time.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/availability-set-overview>

Question: 20

CertyIQ

DRAG DROP -

You have downloaded an Azure Resource Manager (ARM) template to deploy numerous virtual machines (VMs).

The ARM template is based on a current VM, but must be adapted to reference an administrative password.

You need to make sure that the password cannot be stored in plain text.

You are preparing to create the necessary components to achieve your goal.

Which of the following should you create to achieve your goal? Answer by dragging the correct option from the list to the answer area.

Select and Place:

Options

Answer

An Azure Key Vault

An Azure Storage account

Azure Active Directory (AD)
Identity Protection

An access policy

An Azure policy

A backup policy

Answer:

Options

Answer

An Azure Key Vault

An Azure Storage account

Azure Active Directory (AD)
Identity Protection

An access policy

An Azure policy

A backup policy

An Azure Key Vault

An access policy

Explanation:

1. An Azure Key Vault: you can store the administrative password in an Azure Key Vault, which provides secure storage and management of cryptographic keys, certificates, and secrets. Storing the password in a Key Vault ensures that it is not stored in plain text and provides an additional layer of security to protect the password.

2. An access policy: You should create an access policy to control access to the Key Vault secrets. An access policy specifies who can perform operations on the secrets stored in the Key Vault. You can grant permissions to users, applications, and services to access the Key Vault and its secrets, and you can specify the level of access that they have. By creating an access policy, you can control who has access to the administrative password and ensure that it is used only by authorized entities.

Therefore, to achieve your goal, you should create an Azure Key Vault to store the administrative password, and an access policy to control access to the Key Vault secrets.

Question: 21

CertyIQ

Your company has an Azure Active Directory (Azure AD) tenant that is configured for hybrid coexistence with the on-premises Active Directory domain.

The on-premise virtual environment consists of virtual machines (VMs) running on Windows Server 2012 R2 Hyper-

V host servers.

You have created some PowerShell scripts to automate the configuration of newly created VMs. You plan to create several new VMs.

You need a solution that ensures the scripts are run on the new VMs.

Which of the following is the best solution?

- A. Configure a SetupComplete.cmd batch file in the %windir%\setup\scripts directory.
- B. Configure a Group Policy Object (GPO) to run the scripts as logon scripts.
- C. Configure a Group Policy Object (GPO) to run the scripts as startup scripts.
- D. Place the scripts in a new virtual hard disk (VHD).

Answer: A

Explanation:

After you deploy a Virtual Machine you typically need to make some changes before it's ready to use. This is something you can do manually or you could use

Remote PowerShell to automate the configuration of your VM after deployment for example.

But now there's a third alternative available allowing you customize your VM: the CustomScriptextension.

This CustomScript extension is executed by the VM Agent and it's very straightforward: you specify which files it needs to download from your storage account and which file it needs to execute. You can even specify arguments that need to be passed to the script. The only requirement is that you execute a .ps1 file.

Reference:

<https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-a-custom-script-to-windows-setup> <https://azure.microsoft.com/en-us/blog/automating-vm-customization-tasks-using-custom-script-extension/>

Question: 22

CertyIQ

Your company has an Azure Active Directory (Azure AD) tenant that is configured for hybrid coexistence with the on-premises Active Directory domain.

You plan to deploy several new virtual machines (VMs) in Azure. The VMs will have the same operating system and custom software requirements.

You configure a reference VM in the on-premise virtual environment. You then generalize the VM to create an image.

You need to upload the image to Azure to ensure that it is available for selection when you create the new Azure VMs.

Which PowerShell cmdlets should you use?

- A. Add-AzVM
- B. Add-AzVhd
- C. Add-AzImage
- D. Add-AzImageDataDisk

Answer: B

Explanation:

The Add-AzVhd cmdlet uploads on-premises virtual hard disks, in .vhd file format, to a blob storage account as fixed virtual hard disks.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/upload-generalized-managed>

DRAG DROP -

Your company has an Azure subscription that includes a number of Azure virtual machines (VMs), which are all part of the same virtual network.

Your company also has an on-premises Hyper-V server that hosts a VM, named VM1, which must be replicated to Azure.

Which of the following objects that must be created to achieve this goal? Answer by dragging the correct option from the list to the answer area.

Select and Place:

Options

Answer

Hyper-V site

Storage account

Azure Recovery
Services Vault

Azure Traffic
Manager instance

Replication policy

Endpoint

Answer:

Options

Hyper-V site

Storage account

Azure Recovery Services Vault

Azure Traffic Manager instance

Replication policy

Endpoint

Answer

Hyper-V site

Azure Recovery Services Vault

Replication policy

Explanation:

Hyper-V site: Represents the on-premises Hyper-V servers that will be protected.

Azure Recovery Services Vault: A key component in ASR that stores recovery points and orchestrates replication, failover, and failback.

Replication policy :Defines the replication settings, including frequency and retention.

Question: 24

CertyIQ

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company's Azure subscription includes two Azure networks named VirtualNetworkA and VirtualNetworkB. VirtualNetworkA includes a VPN gateway that is configured to make use of static routing. Also, a site-to-site VPN connection exists between your company's on-premises network and VirtualNetworkA.

You have configured a point-to-site VPN connection to VirtualNetworkA from a workstation running Windows 10. After configuring virtual network peering between

VirtualNetworkA and VirtualNetworkB, you confirm that you are able to access VirtualNetworkB from the company's on-premises network. However, you find that you cannot establish a connection to VirtualNetworkB from the Windows 10 workstation.

You have to make sure that a connection to VirtualNetworkB can be established from the Windows 10 workstation.

Solution: You choose the Allow gateway transit setting on VirtualNetworkA.

Does the solution meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

After configuring virtual network peering between

VirtualNetworkA and VirtualNetworkB, you confirm that you are able to access VirtualNetworkB from the company's on-premises network." This indicates the Allow/Use gateway transit is set up working. The next step will be restart/reinstall the VPN-Client config at the windows 10 WS.

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-point-to-site-routing>

Question: 25

CertyIQ

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company's Azure subscription includes two Azure networks named VirtualNetworkA and VirtualNetworkB. VirtualNetworkA includes a VPN gateway that is configured to make use of static routing. Also, a site-to-site VPN connection exists between your company's on-premises network and VirtualNetworkA.

You have configured a point-to-site VPN connection to VirtualNetworkA from a workstation running Windows 10.

After configuring virtual network peering between

VirtualNetworkA and VirtualNetworkB, you confirm that you are able to access VirtualNetworkB from the company's on-premises network. However, you find that you cannot establish a connection to VirtualNetworkB from the Windows 10 workstation.

You have to make sure that a connection to VirtualNetworkB can be established from the Windows 10 workstation.

Solution: You choose the Allow gateway transit setting on VirtualNetworkB.

Does the solution meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

If you make a change to the topology of your network and have Windows VPN clients, the VPN client package for Windows clients must be downloaded and installed again in order for the changes to be applied to the client.

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-point-to-site-routing>

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-point-to-site-routing>

Question: 26

CertyIQ

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company's Azure subscription includes two Azure networks named VirtualNetworkA and VirtualNetworkB. VirtualNetworkA includes a VPN gateway that is configured to make use of static routing. Also, a site-to-site VPN connection exists between your company's on-premises network and VirtualNetworkA.

You have configured a point-to-site VPN connection to VirtualNetworkA from a workstation running Windows 10.

After configuring virtual network peering between

VirtualNetworkA and VirtualNetworkB, you confirm that you are able to access VirtualNetworkB from the company's on-premises network. However, you find that you cannot establish a connection to VirtualNetworkB from the Windows 10 workstation.

You have to make sure that a connection to VirtualNetworkB can be established from the Windows 10 workstation.

Solution: You download and re-install the VPN client configuration package on the Windows 10 workstation.

Does the solution meet the goal?

A. Yes

B. No

Answer: A

Explanation:

"If you make a change to the topology of your network and have Windows VPN clients, the VPN client package for Windows clients must be downloaded and installed again in order for the changes to be applied to the client."

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-point-to-site-routing>

Question: 27

CertyIQ

Your company has virtual machines (VMs) hosted in Microsoft Azure. The VMs are located in a single Azure virtual network named VNet1.

The company has users that work remotely. The remote workers require access to the VMs on VNet1.

You need to provide access for the remote workers.

What should you do?

- A. Configure a Site-to-Site (S2S) VPN.
- B. Configure a VNet-toVNet VPN.
- C. Configure a Point-to-Site (P2S) VPN.
- D. Configure DirectAccess on a Windows Server 2012 server VM.
- E. Configure a Multi-Site VPN

Answer: C

Explanation:

A Point-to-Site (P2S) VPN gateway connection lets you create a secure connection to your virtual network from an individual client computer.

To provide access for remote workers to virtual machines (VMs) hosted in Microsoft Azure, you can use a Point-to-Site (P2S) VPN connection. This type of connection enables individual remote clients to securely connect to an Azure virtual network (VNet) over the Internet.

A Site-to-Site (S2S) VPN connection is used to connect two or more on-premises networks to an Azure virtual network (VNet), while a VNet-to-VNet VPN connection is used to connect two or more Azure virtual networks (VNets) together.

Reference:

Question: 28

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company has a Microsoft SQL Server Always On availability group configured on their Azure virtual machines (VMs).

You need to configure an Azure internal load balancer as a listener for the availability group.

Solution: You create an HTTP health probe on port 1433.

Does the solution meet the goal?

A. Yes

B. No

Answer: B

Explanation:

No, creating an HTTP health probe on port 1433 does not meet the goal of configuring an Azure internal load balancer as a listener for the SQL Server Always On availability group.

In order to configure an Azure internal load balancer as a listener for the availability group, you need to create a TCP health probe on port 1433. SQL Server uses TCP to communicate on port 1433, so a TCP health probe is the appropriate choice to ensure the availability and health of the SQL Server instances in the availability group.

Question: 29

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company has a Microsoft SQL Server Always On availability group configured on their Azure virtual machines (VMs).

You need to configure an Azure internal load balancer as a listener for the availability group.

Solution: You set Session persistence to Client IP.

Does the solution meet the goal?

A. Yes

B. No

Answer: B

Explanation:

FYI: Session persistence ensures that a client will remain connected to the same server throughout a session or period of time. Because load balancing may, by default, send users to unique servers each time they connect, this can mean that complicated or repeated requests are slowed down.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sql/virtual-machines-windows-portal-sql-alwayson-int-listener>

Question: 30

CertyIQ

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company has a Microsoft SQL Server Always On availability group configured on their Azure virtual machines (VMs).

You need to configure an Azure internal load balancer as a listener for the availability group.

Solution: You enable Floating IP.

Does the solution meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Yes, enabling Floating IP on the Azure internal load balancer as a listener for the availability group can meet the goal. By enabling Floating IP, the load balancer will use a floating IP address as the source IP address for outbound flows from the backend pool. This will ensure that the IP address used by the backend pool remains the same even if a VM is restarted or replaced, which is important for maintaining the listener for the availability group.

Question: 31

CertyIQ

Your company has two on-premises servers named SRV01 and SRV02. Developers have created an application that runs on SRV01. The application calls a service on SRV02 by IP address.

You plan to migrate the application on Azure virtual machines (VMs). You have configured two VMs on a single subnet in an Azure virtual network.

You need to configure the two VMs with static internal IP addresses.

What should you do?

- A. Run the New-AzureRMVMConfig PowerShell cmdlet.
- B. Run the Set-AzureSubnet PowerShell cmdlet.
- C. Modify the VM properties in the Azure Management Portal.
- D. Modify the IP properties in Windows Network and Sharing Center.
- E. Run the Set-AzureStaticVNetIP PowerShell cmdlet.

Answer: E

Explanation:

Specify a static internal IP for a previously created VM

If you want to set a static IP address for a VM that you previously created, you can do so by using the following cmdlets. If you already set an IP address for the

VM and you want to change it to a different IP address, you'll need to remove the existing static IP address before running these cmdlets. See the instructions below to remove a static IP.

For this procedure, you'll use the Update-AzureVM cmdlet. The Update-AzureVM cmdlet restarts the VM as part of the update process. The DIP that you specify will be assigned after the VM restarts. In this example, we set the IP address for VM2, which is located in cloud service StaticDemo.

```
Get-AzureVM -ServiceName StaticDemo -Name VM2 | Set-AzureStaticVNetIP -IPAddress 192.168.4.7 |  
Update-AzureVM
```

Question: 32

Your company has an Azure Active Directory (Azure AD) subscription.

You need to deploy five virtual machines (VMs) to your company's virtual network subnet.

The VMs will each have both a public and private IP address. Inbound and outbound security rules for all of these virtual machines must be identical.

Which of the following is the least amount of network interfaces needed for this configuration?

- A. 5
- B. 10
- C. 20
- D. 40

Answer: A**Explanation:**

To deploy five VMs with both public and private IP addresses, you would need at least five network interfaces (one for each VM). Each VM requires a network interface to connect to the virtual network, and since each VM will have both a public and a private IP address, you would typically assign one network interface per VM.

5 VM so 5 NIC Cards .we have public and private ip address set to them .however they needs same inbound and outbound rule so create NSG and attach to NIC and this req can be fulfilled 5 NIC hence 5 is right answer.

Question: 33

Your company has an Azure Active Directory (Azure AD) subscription.

You need to deploy five virtual machines (VMs) to your company's virtual network subnet.

The VMs will each have both a public and private IP address. Inbound and outbound security rules for all of these virtual machines must be identical.

Which of the following is the least amount of security groups needed for this configuration?

- A. 4
- B. 3
- C. 2
- D. 1

Answer: D**Explanation:**

D. 1 In Azure, Network Security Groups (NSGs) are used to control inbound and outbound traffic to network interfaces (NICs), subnets, or both.

For the given scenario:

There are five virtual machines (VMs).

Each VM has both a public and private IP address.

All VMs must have identical inbound and outbound security rules.

Since all VMs require the same security rules, you can assign a single NSG at the subnet level. This ensures that the security rules apply uniformly to all VMs within that subnet.

all identical security groups so you will only require 1 security group as all the settings are the same

Question: 34**CertyIQ**

Your company's Azure subscription includes Azure virtual machines (VMs) that run Windows Server 2016. One of the VMs is backed up every day using Azure Backup Instant Restore. When the VM becomes infected with data encrypting ransomware, you decide to recover the VM's files. Which of the following is TRUE in this scenario?

- A. You can only recover the files to the infected VM.
- B. You can recover the files to any VM within the company's subscription.
- C. You can only recover the files to a new VM.
- D. You will not be able to recover the files.

Answer: B**Explanation:**

1. You can restore files by mounting the backup to your own local machine if you like, just like you could on any of the VMs in Azure as they are all 2016. It just uses an iSCSI connection to the backup image.
2. The answer is B. Recovery of files, you cannot restore files to an older or newer version of the OS, It must be a compatible client OS. Therefore, restoring files back to the same subscription is the best option but it has to be the same OS version. Although answer A is possible but restoring files back to an infected VM doesn't sound right to me.

Question: 35**CertyIQ**

Your company's Azure subscription includes Azure virtual machines (VMs) that run Windows Server 2016. One of the VMs is backed up every day using Azure Backup Instant Restore. When the VM becomes infected with data encrypting ransomware, you are required to restore the VM. Which of the following actions should you take?

- A. You should restore the VM after deleting the infected VM.
- B. You should restore the VM to any VM within the company's subscription.
- C. You should restore the VM to a new Azure VM.
- D. You should restore the VM to an on-premise Windows device.

Answer: C**Explanation:**

- C. You should restore the VM to a new Azure VM.

Azure Backup provides Instant Restore for virtual machines, which allows you to quickly recover your VM in case of issues such as ransomware attacks.

For a ransomware infection, the best approach is to restore the VM to a new Azure VM rather than overwriting or restoring to an existing VM. This ensures that the infected VM does not affect the restored system.

Question: 36**CertyIQ**

You administer a solution in Azure that is currently having performance issues. You need to find the cause of the performance issues pertaining to metrics on the Azure infrastructure. Which of the following is the tool you should use?

- A. Azure Traffic Analytics
- B. Azure Monitor
- C. Azure Activity Log
- D. Azure Advisor

Answer: B

Explanation:

Metrics in Azure Monitor are stored in a time-series database which is optimized for analyzing time-stamped data. This makes metrics particularly suited for alerting and fast detection of issues.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-platform>

CertyIQ

Question: 37

Your company has an Azure subscription that includes a Recovery Services vault. You want to use Azure Backup to schedule a backup of your company's virtual machines (VMs) to the Recovery Services vault. Which of the following VMs can you back up? Choose all that apply.

- A. VMs that run Windows 10.
- B. VMs that run Windows Server 2012 or higher.
- C. VMs that have NOT been shut down.
- D. VMs that run Debian 8.2+.
- E. VMs that have been shut down.

Answer: ABCDE

Explanation:

Azure Backup supports backup of 64-bit Windows server operating system from Windows Server 2008.

Azure Backup supports backup of 64-bit Windows 10 operating system.

Azure Backup supports backup of 64-bit Debian operating system from Debian 7.9+.

Azure Backup supports backup of VM that are shutdown or offline.

Reference:

<https://docs.microsoft.com/en-us/azure/backup/backup-support-matrix-iaas> <https://docs.microsoft.com/en-us/azure/virtual-machines/linux/endorsed-distros>

CertyIQ

Question: 38

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 Active Directory (Azure AD) tenant named contoso.com.

You have a CSV file that contains the names and email addresses of 500 external users.
You need to create a guest user account in contoso.com for each of the 500 external users.
Solution: You create a PowerShell script that runs the New-AzureADUser cmdlet for each user.
Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

The New-AzureADUser cmdlet creates a user in Azure Active Directory (Azure AD).

Instead use the New-AzureADMSInvitation cmdlet which is used to invite a new external user to your directory.

Reference:

<https://docs.microsoft.com/en-us/powershell/module/azuread/new-azureadmsinvitation>

Question: 39

CertyIQ

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 Active Directory (Azure AD) tenant named contoso.com.

You have a CSV file that contains the names and email addresses of 500 external users.

You need to create a guest user account in contoso.com for each of the 500 external users.

Solution: From Azure AD in the Azure portal, you use the Bulk create user operation.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

"Bulk Create" is for new Azure AD Users.

For Guests:

- Use "Bulk invite users" to prepare a comma-separated value (.csv) file with the user information and invitation preferences
- Upload the .csv file to Azure AD
- Verify the users were added to the directory

Instead use the New-AzureADMSInvitation cmdlet which is used to invite a new external user to your directory.

Reference:

<https://docs.microsoft.com/en-us/powershell/module/azuread/new-azureadmsinvitation>

Question: 40

CertyIQ

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 Active Directory (Azure AD) tenant named contoso.com.

You have a CSV file that contains the names and email addresses of 500 external users.

You need to create a guest user account in contoso.com for each of the 500 external users.

Solution: You create a PowerShell script that runs the New-AzureADMSInvitation cmdlet for each external user.

Does this meet the goal?

A. Yes

B. No

Answer: A**Explanation:**

Use the New-AzureADMSInvitation cmdlet which is used to invite a new external user to your directory.

Yes, this solution should meet the goal. The New-AzureADMSInvitation cmdlet can be used to send invitations to external users to become guest users in an Azure AD tenant. By running the cmdlet for each external user listed in the CSV file, a guest user account can be created in the contoso.com Azure AD tenant for each of the 500 external users.

Reference:

<https://docs.microsoft.com/en-us/powershell/module/azuread/new-azureadmsinvitation>

Question: 41

CertyIQ

You have the Azure virtual machines shown in the following table:

Name	Azure region
VM1	West Europe
VM2	West Europe
VM3	North Europe
VM4	North Europe

You have a Recovery Services vault that protects VM1 and VM2.

You need to protect VM3 and VM4 by using Recovery Services.

What should you do first?

A. Create a new Recovery Services vault

B. Create a storage account

C. Configure the extensions for VM3 and VM4

D. Create a new backup policy

Answer: A

Explanation:

A Recovery Services vault is a storage entity in Azure that houses data. The data is typically copies of data, or configuration information for virtual machines

(VMs), workloads, servers, or workstations. You can use Recovery Services vaults to hold backup data for various Azure services

Reference:

<https://docs.microsoft.com/en-us/azure/site-recovery/azure-to-azure-tutorial-enable-replicatio>

Question: 42**CertyIQ****HOTSPOT -**

You have an Azure subscription named Subscription1 that contains a resource group named RG1.

In RG1, you create an internal load balancer named LB1 and a public load balancer named LB2.

You need to ensure that an administrator named Admin1 can manage LB1 and LB2. The solution must follow the principle of least privilege.

Which role should you assign to Admin1 for each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To add a backend pool to LB1:

Contributor on LB1
Network Contributor on LB1
Network Contributor on RG1
Owner on LB1

To add a health probe to LB2:

Contributor on LB2
Network Contributor on LB2
Network Contributor on RG1
Owner on LB2

Answer:

Answer Area

To add a backend pool to LB1:

Contributor on LB1
Network Contributor on LB1
Network Contributor on RG1
Owner on LB1

To add a health probe to LB2:

Contributor on LB2
Network Contributor on LB2
Network Contributor on RG1
Owner on LB2

Explanation:

Network Contributor on LB1

Network Contributor on LB2

Network Contributor role on LB1 and LB2 is the correct answer. With this role user can add create a backend address without actually adding the actual IP addresses. Network contributor can also create and modify health probe.

If the user wants to add address to backend pools (eg: IPs from a VNet or entire subnet) then a Network Contributor role is required at the resource group level (or atleast on VNet)

Question: 43

CertyIQ

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com and an Azure Kubernetes Service (AKS) cluster named AKS1.

An administrator reports that she is unable to grant access to AKS1 to the users in contoso.com.

You need to ensure that access to AKS1 can be granted to the contoso.com users.

What should you do first?

- A. From contoso.com, modify the Organization relationships settings.
- B. From contoso.com, create an OAuth 2.0 authorization endpoint.
- C. Recreate AKS1.
- D. From AKS1, create a namespace.

Answer: B

Explanation:

Cluster administrators can configure Kubernetes role-based access control (Kubernetes RBAC) based on a user's identity or directory group membership. Azure AD authentication is provided to AKS clusters with OpenID Connect. OpenID Connect is an identity layer built on top of the OAuth 2.0 protocol

<https://docs.microsoft.com/en-us/azure/aks/managed-aad>

Question: 44

CertyIQ

You have a Microsoft 365 tenant and an Azure Active Directory (Azure AD) tenant named contoso.com. You plan to grant three users named User1, User2, and User3 access to a temporary Microsoft SharePoint document library named Library1. You need to create groups for the users. The solution must ensure that the groups are deleted automatically after 180 days. Which two groups should you create? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. a Microsoft 365 group that uses the Assigned membership type
- B. a Security group that uses the Assigned membership type
- C. a Microsoft 365 group that uses the Dynamic User membership type
- D. a Security group that uses the Dynamic User membership type
- E. a Security group that uses the Dynamic Device membership type

Answer: AC**Explanation:**

You can set expiration policy only for Office 365 groups in Azure Active Directory (Azure AD).

Note: With the increase in usage of Office 365 Groups, administrators and users need a way to clean up unused groups. Expiration policies can help remove inactive groups from the system and make things cleaner.

When a group expires, all of its associated services (the mailbox, Planner, SharePoint site, etc.) are also deleted.

You can set up a rule for dynamic membership on security groups or Office 365 groups.

Incorrect Answers:

B, D, E: You can set expiration policy only for Office 365 groups in Azure Active Directory (Azure AD).

Reference:

<https://docs.microsoft.com/en-us/office365/admin/create-groups/office-365-groups-expiration-policy?view=o365-worldwide>

Question: 45

CertyIQ

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table:

Name	Type	Member of
User1	Member	Group1
User2	Guest	Group1
User3	Member	None
UserA	Member	Group2
UserB	Guest	Group2

User3 is the owner of Group1.

Group2 is a member of Group1.

You configure an access review named Review1 as shown in the following exhibit:

Create an access review

Access reviews enable reviewers to attest user's membership in a group or access to an application.

* Review name: Review1

Description: (empty)

* Start date: 2018-11-22

Frequency: One time

Duration (in days): 1

End: Never

* Number of times: 0

* End date: 2018-12-22

Users

Users to review: Members of a group

Scope: Guest users only

* Group: Group1

Reviewers

Reviewers: Group owners

Programs

Link to program

Default program

Upon completion settings

Advanced settings

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User3 can perform an access review of User1	<input type="radio"/>	<input type="radio"/>
User3 can perform an access review of UserA	<input type="radio"/>	<input type="radio"/>
User3 can perform an access review of UserB	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User3 can perform an access review of User1	<input type="radio"/>	<input checked="" type="radio"/>
User3 can perform an access review of UserA	<input type="radio"/>	<input checked="" type="radio"/>
User3 can perform an access review of UserB	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

User3 can perform an access review of User1 = **No**

User1 is a Member and not a Guest Account, Access Review specified Guests only.

User3 can perform an access review of UserA = **No**

User1 is a Member and not a Guest Account, Access Review specified Guests only.

User3 can perform an access review of UserB = **No**

Created Group 1 and Group 2, added Group 2 as a member in Group 1,

Added guest Accounts to Group 1 and Group 2,

In the Access Review results only the Guest Accounts in Group 1 appeared for review and "Not" the Guest accounts in Group 2.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

You have the Azure management groups shown in the following table:

Name	In management group
Tenant Root Group	<i>Not applicable</i>
ManagementGroup11	Tenant Root Group
ManagementGroup12	Tenant Root Group
ManagementGroup21	ManagementGroup11

You add Azure subscriptions to the management groups as shown in the following table:

Name	Management group
Subscription1	ManagementGroup21
Subscription2	ManagementGroup12

You create the Azure policies shown in the following table:

Name	Parameter	Scope
Not allowed resource types	virtualNetworks	Tenant Root Group
Allowed resource types	virtualNetworks	ManagementGroup12

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
You can create a virtual network in Subscription1.	<input type="radio"/>	<input type="radio"/>
You can create a virtual machine in Subscription2.	<input type="radio"/>	<input type="radio"/>
You can add Subscription1 to ManagementGroup11.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
You can create a virtual network in Subscription1.	<input checked="" type="radio"/>	<input type="radio"/>
You can create a virtual machine in Subscription2.	<input type="radio"/>	<input checked="" type="radio"/>
You can add Subscription1 to ManagementGroup11.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Box 1: No -

Virtual networks are not allowed at the root and is inherited. Deny overrides allowed.

Box 2: No-

Subscription 2: Allowed to create a VNET which restricts anything else.

Box 3: No -

Already in one Management group called 21, so cannot add into another. A Subscription can be assigned to 1 Management Group

Reference:

<https://docs.microsoft.com/en-us/azure/governance/management-groups/overview>

<https://docs.microsoft.com/en-us/azure/governance/management-groups/manage#moving-management-groups-and-subscriptions>

Question: 47

CertyIQ

You have an Azure policy as shown in the following exhibit:

SCOPE

- * Scope ([Learn more about setting the scope](#))

Subscription 1

Exclusions

Subscription 1/ContosoRG1

BASICS

- * Policy definition

Not allowed resource types

- * Assignment name 

Not allowed resource types

Assignment ID

/subscriptions/5eb8d0b6-ce3b-4ce0-a631-9f5321bedabb/providers/Microsoft.Authorization/policyAssignments/0e6fb866bf854f54accae2a9

Description

Assigned by

admin1@contoso.com

PARAMETERS

- * Not allowed resource types 

Microsoft.Sql/servers

What is the effect of the policy?

- A. You are prevented from creating Azure SQL servers anywhere in Subscription 1.
- B. You can create Azure SQL servers in ContosoRG1 only.
- C. You are prevented from creating Azure SQL Servers in ContosoRG1 only.
- D. You can create Azure SQL servers in any resource group within Subscription 1.

Answer: B

Explanation:

You are prevented from creating Azure SQL servers anywhere in Subscription 1 with the exception of ContosoRG1

B is correct option , as current policy prevents creation of sql servers in sub1 , but due to exclusion , only inside ContosoRG1 , you can create sql servers.

Question: 48

CertyIQ

HOTSPOT -

You have an Azure subscription that contains the resources shown in the following table:

Name	Type	Resource group	Tag
RG6	Resource group	<i>Not applicable</i>	<i>None</i>
VNET1	Virtual network	RG6	Department: D1

You assign a policy to RG6 as shown in the following table:

Section	Setting	Value
Scope	Scope	Subscription1/RG6
	Exclusions	<i>None</i>
Basics	Policy definition	Apply tag and its default value
	Assignment name	Apply tag and its default value
Parameters	Tag name	Label
	Tag value	Value1

To RG6, you apply the tag: RGroup: RG6.

You deploy a virtual network named VNET2 to RG6.

Which tags apply to VNET1 and VNET2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

VNET1:

- None
- Department: D1 only
- Department: D1, and RGroup: RG6 only
- Department: D1, and Label: Value1 only
- Department: D1, RGroup: RG6, and Label: Value1

VNET2:

- None
- RGroup: RG6 only
- Label: Value1 only
- RGroup: RG6, and Label: Value1

Answer:

Answer Area

VNET1:

None
Department: D1 only
Department: D1, and RGroup: RG6 only
Department: D1, and Label: Value1 only
Department: D1, RGroup: RG6, and Label: Value1

VNET2:

None
RGroup: RG6 only
Label: Value1 only
RGroup: RG6, and Label: Value1

Explanation:

VNET1: Department: D1 only.

RG tags are not inherited to resources

VNET2: Label:Value1 only.

Incorrect Answers:

Tags are not inherited. The tag was only applied to the resource group, the VNET2 resource won't inherit it

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-policies>

Question: 49

CertyIQ

You have an Azure subscription named AZPT1 that contains the resources shown in the following table:

Name	Type
storage1	Azure Storage account
VNET1	Virtual network
VM1	Azure virtual machine
VM1Managed	Managed disk for VM1
RVAULT1	Recovery Services vault for the site recovery of VM1

You create a new Azure subscription named AZPT2.

You need to identify which resources can be moved to AZPT2.

Which resources should you identify?

- A. VM1, storage1, VNET1, and VM1Managed only
- B. VM1 and VM1Managed only
- C. VM1, storage1, VNET1, VM1Managed, and RVAULT1
- D. RVAULT1 only

Answer: C**Explanation:**

You can move a VM and its associated resources to a different subscription by using the Azure portal.

You can now move an Azure Recovery Service (ASR) Vault to either a new resource group within the current subscription or to a new subscription.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/move-resource-group-and-subscription>

CertyIQ**Question: 50**

You recently created a new Azure subscription that contains a user named Admin1.

Admin1 attempts to deploy an Azure Marketplace resource by using an Azure Resource Manager template. Admin1 deploys the template by using Azure

PowerShell and receives the following error message: 'User failed validation to purchase resources. Error message: 'Legal terms have not been accepted for this item on this subscription. To accept legal terms, please go to the Azure portal (<http://go.microsoft.com/fwlink/?LinkId=534873>) and configure programmatic deployment for the Marketplace item or create it there for the first time.'

You need to ensure that Admin1 can deploy the Marketplace resource successfully.

What should you do?

- A. From Azure PowerShell, run the Set-AzApiManagementSubscription cmdlet
- B. From the Azure portal, register the Microsoft.Marketplace resource provider
- C. From Azure PowerShell, run the Set-AzMarketplaceTerms cmdlet
- D. From the Azure portal, assign the Billing administrator role to Admin1

Answer: C**Explanation:**

```
Set-AzMarketplaceTerms -Publisher <String> -Product <String> -Name <String> [-Accept] [-Terms <PSAgreementTerms>] [-DefaultProfile <IAzureContextContainer>] [-WhatIf] [-Confirm] [<CommonParameters>]
```

Reference:

<https://docs.microsoft.com/en-us/powershell/module/Az.MarketplaceOrdering/Set-AzMarketplaceTerms?view=azps-4.6.0>

Reference:

<https://docs.microsoft.com/en-us/powershell/module/az.marketplaceordering/set-azmarketplaceterms?view=azps-4.1.0>

CertyIQ**Question: 51**

You have an Azure Active Directory (Azure AD) tenant that contains 5,000 user accounts.

You create a new user account named AdminUser1.

You need to assign the User administrator administrative role to AdminUser1.

What should you do from the user account properties?

- A. From the Licenses blade, assign a new license
- B. From the Directory role blade, modify the directory role
- C. From the Groups blade, invite the user account to a new group

Answer: B

Explanation:

Assign a role to a user -

1. Sign in to the Azure portal with an account that's a global admin or privileged role admin for the directory.
2. Select Azure Active Directory, select Users, and then select a specific user from the list.
3. For the selected user, select Directory role, select Add role, and then pick the appropriate admin roles from the Directory roles list, such as Conditional access administrator.
4. Press Select to save.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-assign-role-azure-portal>

Question: 52

CertyIQ

You have an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com that contains 100 user accounts.

You purchase 10 Azure AD Premium P2 licenses for the tenant.

You need to ensure that 10 users can use all the Azure AD Premium features.

What should you do?

- A. From the Licenses blade of Azure AD, assign a license
- B. From the Groups blade of each user, invite the users to a group
- C. From the Azure AD domain, add an enterprise application
- D. From the Directory role blade of each user, modify the directory role

Answer: A

Explanation:

- A. From the Licenses blade of Azure AD, assign a license.

To ensure that the 10 users can use all the Azure AD Premium P2 features, you need to assign each of these users a Premium P2 license. This is done from the Licenses blade in the Azure Active Directory section of the Azure portal. Here, you can manage and assign licenses directly to individual users or to a group that these users are part of. Assigning the license enables the users to access Premium features such as Identity Protection, Privileged Identity Management, and more.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/license-users-groups>

Question: 53

CertyIQ

You have an Azure subscription named Subscription1 and an on-premises deployment of Microsoft System Center Service Manager.

Subscription1 contains a virtual machine named VM1.

You need to ensure that an alert is set in Service Manager when the amount of available memory on VM1 is below

10 percent.

What should you do first?

- A. Create an automation runbook
- B. Deploy a function app
- C. Deploy the IT Service Management Connector (ITSM)
- D. Create a notification

Answer: C

Explanation:

The IT Service Management Connector (ITSMC) allows you to connect Azure and a supported IT Service Management (ITSM) product/service, such as the Microsoft System Center Service Manager.

With ITSMC, you can create work items in ITSM tool, based on your Azure alerts (metric alerts, Activity Log alerts and Log Analytics alerts).

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/itsmc-overview>

CertyIQ

Question: 54

You sign up for Azure Active Directory (Azure AD) Premium P2.

You need to add a user named as an administrator on all the computers that will be joined to the Azure AD domain.

What should you configure in Azure AD?

- A. Device settings from the Devices blade
- B. Providers from the MFA Server blade
- C. User settings from the Users blade
- D. General settings from the Groups blade

Answer: A

Explanation:

When you connect a Windows device with Azure AD using an Azure AD join, Azure AD adds the following security principles to the local administrators group on the device:

- ⇒ The Azure AD global administrator role
- ⇒ The Azure AD device administrator role
- ⇒ The user performing the Azure AD join

In the Azure portal, you can manage the device administrator role on the Devices page. To open the Devices page:

1. Sign in to your Azure portal as a global administrator or device administrator.
2. On the left navbar, click Azure Active Directory.
3. In the Manage section, click Devices.
4. On the Devices page, click Device settings.
5. To modify the device administrator role, configure Additional local administrators on Azure AD joined devices.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/devices/assign-local-admin>

HOTSPOT -

You have Azure Active Directory tenant named Contoso.com that includes following users:

Name	Role
User1	Cloud device administrator
User2	User administrator

Contoso.com includes following Windows 10 devices:

Name	Join type
Device1	Azure AD registered
Device2	Azure AD joined

You create following security groups in Contoso.com:

Name	Membership Type	Owner
Group1	Assigned	User2
Group2	Dynamic Device	User2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 can add Device2 to Group1	<input type="radio"/>	<input type="radio"/>
User2 can add Device1 to Group1	<input type="radio"/>	<input type="radio"/>
User2 can add Device2 to Group2	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 can add Device2 to Group1	<input type="radio"/>	<input checked="" type="radio"/>
User2 can add Device1 to Group1	<input checked="" type="radio"/>	<input type="radio"/>
User2 can add Device2 to Group2	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

User1 can add Device2 to Group1: No

User2 can add Device1 to Group1: Yes

User2 can add Device2 to Group2: No

Groups can contain both registered and joined devices as members.

As a global administrator or cloud device administrator, you can manage the registered or joined devices. Intune Service administrators can update and delete devices. User administrator can manage users but not devices.

User1 is a cloud device administrator. Users in this role can enable, disable, and delete devices in Azure AD and read Windows 10 BitLocker keys (if present) in the Azure portal. The role does not grant permissions to manage any other properties on the device.

User2 is the owner of Group1. He can add Device1 to Group1.

Group2 is configured for dynamic membership. The properties on which the membership of a device in a group of the type dynamic device are defined cannot be changed by either an end user or an user administrator. User2 cannot add any device to Group2.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal>

Question: 56

CertyIQ

You have an Azure subscription that contains a resource group named RG26.

RG26 is set to the West Europe location and is used to create temporary resources for a project. RG26 contains the resources shown in the following table.

Name	Type	Location
VM1	Virtual machine	North Europe
RGV1	Recovery Services vault	North Europe
SQLD01	SQL server in Azure VM	North Europe
sa001	Storage account	West Europe

SQLDB01 is backed up to RGV1.

When the project is complete, you attempt to delete RG26 from the Azure portal. The deletion fails.

You need to delete RG26.

What should you do first?

- A. Delete VM1
- B. Stop VM1
- C. Stop the backup of SQLDB01
- D. Delete sa001

Answer: C

Explanation:

Stop the backup of SQLDB01"

VM's running or not would not block the deletion of a Resource Group.

Storage Accounts also don't block the deletion of a Resource Group.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/delete-resource-group?tabs=azure-powershell#required-access-and-deletion-failures>

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-delete-vault?tabs=portal#before-you-start>

Question: 57

CertyIQ

You have an Azure subscription named Subscription1 that contains a virtual network named VNet1. VNet1 is in a resource group named RG1.

Subscription1 has a user named User1. User1 has the following roles:

- ⇒ Reader
- ⇒ Security Admin
- ⇒ Security Reader

You need to ensure that User1 can assign the Reader role for VNet1 to other users.

What should you do?

- A. Remove User1 from the Security Reader and Reader roles for Subscription1.
- B. Assign User1 the User Access Administrator role for VNet1.
- C. Assign User1 the Network Contributor role for VNet1.
- D. Assign User1 the Network Contributor role for RG1.

Answer: B

Explanation:

Has full access to all resources including the right to delegate access to others.

Note:

There are several versions of this question in the exam. The question has two possible correct answers:

- ⇒ Assign User1 the User Access Administrator role for VNet1.
- ⇒ Assign User1 the Owner role for VNet1.

Other incorrect answer options you may see on the exam include the following:

- ⇒ Assign User1 the Contributor role for VNet1.
- ⇒ Remove User1 from the Security Reader and Reader roles for Subscription1. Assign User1 the Contributor

role for Subscription1.

⇒ Remove User1 from the Security Reader role for Subscription1. Assign User1 the Contributor role for RG1.

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/overview>

Question: 58

CertyIQ

You have an Azure Active Directory (Azure AD) tenant named contosocloud.onmicrosoft.com.

Your company has a public DNS zone for contoso.com.

You add contoso.com as a custom domain name to Azure AD.

You need to ensure that Azure can verify the domain name.

Which type of DNS record should you create?

- A. MX
- B. NSEC
- C. PTR
- D. RRSIG

Answer: A

Explanation:

To verify your custom domain name (example)

1. Sign in to the Azure portal using a Global administrator account for the directory.
2. Select Azure Active Directory, and then select Custom domain names.
3. On the Fabrikam - Custom domain names page, select the custom domain name, Contoso.
4. On the Contoso page, select Verify to make sure your custom domain is properly registered and is valid for Azure AD. Use either the TXT or the MX record type.

Note:

There are several versions of this question in the exam. The question can have two correct answers:

1. MX
2. TXT

The question can also have other incorrect answer options, including the following:

1. SRV
2. NSEC3

Reference:

<https://docs.microsoft.com/en-us/azure/dns/dns-web-sites-custom-domain>

Question: 59

CertyIQ

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 Directory (Azure AD) tenant named Adatum and an Azure Subscription named Subscription1. Adatum contains a group named Developers.

Subscription1 contains a resource group named Dev.

You need to provide the Developers group with the ability to create Azure logic apps in the Dev resource group.

Solution: On Subscription1, you assign the DevTest Labs User role to the Developers group.

Does this meet the goal?

- A. Yes

B. No

Answer: B

Explanation:

DevTest Labs User role only lets you connect, start, restart, and shutdown virtual machines in your Azure DevTest Labs.

The Logic App Contributor role lets you manage logic app, but not access to them. It provides access to view, edit, and update a logic app.

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles> <https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-securing-a-logic-app>

CertyIQ

Question: 60

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 Directory (Azure AD) tenant named Adatum and an Azure Subscription named Subscription1. Adatum contains a group named Developers.

Subscription1 contains a resource group named Dev.

You need to provide the Developers group with the ability to create Azure logic apps in the Dev resource group.

Solution: On Subscription1, you assign the Logic App Operator role to the Developers group.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

B. No

The Logic App Operator role only allows users to view and manage logic apps. It does not allow them to create new ones. Therefore, assigning the Logic App Operator role to the Developers group will not meet the goal of providing them with the ability to create Azure logic apps in the Dev resource group.

You would need the Logic App Contributor role.

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>
<https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-securing-a-logic-app>

CertyIQ

Question: 61

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 Directory (Azure AD) tenant named Adatum and an Azure Subscription named Subscription1.

Adatum contains a group named Developers.

Subscription1 contains a resource group named Dev.

You need to provide the Developers group with the ability to create Azure logic apps in the Dev resource group.

Solution: On Dev, you assign the Contributor role to the Developers group.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Yes, assigning the Contributor role to the Developers group on the Dev resource group would meet the goal of providing the group with the ability to create Azure logic apps in the Dev resource group.

The Contributor role grants full access to manage all resources in the resource group, including the ability to create and manage logic apps. By assigning the Contributor role to the Developers group, you are giving them the necessary permissions to create and manage logic apps in the Dev resource group.

The Contributor role can manage all resources (and add resources) in a Resource Group.

Question: 62

CertyIQ

DRAG DROP -

You have an Azure subscription that is used by four departments in your company. The subscription contains 10 resource groups. Each department uses resources in several resource groups.

You need to send a report to the finance department. The report must detail the costs for each department.

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

Assign a tag to each resource group.

Assign a tag to each resource.

Download the usage report.

From the Cost analysis blade, filter the view by tag.

Open the **Resource costs** blade of each resource group.

Answer Area



Answer:

Actions

Answer Area

Assign a tag to each resource group.

Assign a tag to each resource.

Assign a tag to each resource.

From the Cost analysis blade, filter the view by tag.

Download the usage report.



Download the usage report.



From the Cost analysis blade, filter the view by tag.

Open the **Resource costs** blade of each resource group.

Explanation:

Box 1: Assign a tag to each resource.

You apply tags to your Azure resources giving metadata to logically organize them into a taxonomy. After you apply tags, you can retrieve all the resources in your subscription with that tag name and value. Each resource or resource group can have a maximum of 15 tag name/value pairs. Tags applied to the resource group are not inherited by the resources in that resource group.

Box 2: From the Cost analysis blade, filter the view by tag

After you get your services running, regularly check how much they're costing you. You can see the current spend and burn rate in Azure portal.

1. Visit the Subscriptions blade in Azure portal and select a subscription.

You should see the cost breakdown and burn rate in the popup blade.

2. Click Cost analysis in the list to the left to see the cost breakdown by resource. Wait 24 hours after you add a service for the data to populate.

3. You can filter by different properties like tags, resource group, and timespan. Click Apply to confirm the filters and Download if you want to export the view to a Comma-Separated Values (.csv) file.

Box 3: Download the usage report

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags> <https://docs.microsoft.com/en-us/azure/billing/billing-getting-started>

Question: 63

CertyIQ

You have an Azure subscription named Subscription1 that contains an Azure Log Analytics workspace named Workspace1.

You need to view the error events from a table named Event.

Which query should you run in Workspace1?

- A. Get-Event Event | where \$_.EventType == "error"
- B. search in (Event) "error"
- C. select * from Event where EventType == "error"
- D. search in (Event) * | where EventType -eq "error"

Answer: B

Explanation:

To search a term in a specific table, add the table-name just after the search operator

Note:

There are several versions of this question in the exam. The question has two possible correct answers:

1. Event | search "error"
2. Event | where EventType == "error"
3. search in (Event) "error"

Other incorrect answer options you may see on the exam include the following:

1. Get-Event Event | where \$_.EventTye "eq "error"
2. Event | where EventType is "error"
3. search in (Event) * | where EventType "eq "error"
4. select * from Event where EventType is "error"

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/search-queries> <https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/get-started-portal> <https://docs.microsoft.com/en-us/azure/data-explorer/kusto/query/searchoperator?pivots=azuredatadexplorer>

Question: 64

CertyIQ

HOTSPOT -

You have an Azure subscription that contains a virtual network named VNET1 in the East US 2 region. A network interface named VM1-NI is connected to

VNET1.

You successfully deploy the following Azure Resource Manager template.

```
{  
    "apiVersion": "2017-03-30",  
    "type": "Microsoft.Compute/virtualMachines",  
    "name": "VM1",  
    "zones": "1",  
    "location": "EastUS2",  
    "dependsOn": [  
        "[resourceId('Microsoft.Network/networkInterfaces', 'VM1-NI')]"  
    ],  
    "properties": {  
        "hardwareProfile": {  
            "vmSize": "Standard_A2_v2"  
        },  
        "osProfile": {  
            "computerName": "VM1",  
            "adminUsername": "AzureAdmin",  
            "adminPassword": "[parameters('adminPassword')]"  
        },  
        "storageProfile": {  
            "imageReference": "[variables('image')]",  
            "osDisk": {  
                "createOption": "FromImage"  
            }  
        },  
        "networkProfile": {  
            "networkInterfaces": [  
                {  
                    "id": "[resourceId('Microsoft.Network/networkInterfaces', 'VM1-NI')]"  
                }  
            ]  
        }  
    },  
    {  
        "apiVersion": "2017-03-30",  
        "type": "Microsoft.Compute/virtualMachines",  
        "name": "VM1",  
        "zones": "1",  
        "location": "EastUS2",  
        "dependsOn": [  
            "[resourceId('Microsoft.Network/networkInterfaces', 'VM1-NI')]"  
        ],  
        "properties": {  
            "hardwareProfile": {  
                "vmSize": "Standard_A2_v2"  
            },  
            "osProfile": {  
                "computerName": "VM1",  
                "adminUsername": "AzureAdmin",  
                "adminPassword": "[parameters('adminPassword')]"  
            },  
            "storageProfile": {  
                "imageReference": "[variables('image')]",  
                "osDisk": {  
                    "createOption": "FromImage"  
                }  
            },  
            "networkProfile": {  
                "networkInterfaces": [  
                    {  
                        "id": "[resourceId('Microsoft.Network/networkInterfaces', 'VM1-NI')]"  
                    }  
                ]  
            }  
        }  
    }  
}
```

```

"name": "VM2",
"zones": "2",
"location: "EastUS2",
"dependsOn": [
    "[resourceId('Microsoft.Network/networkInterfaces', 'VM2-NI')]"
],
"properties": {
    "hardwareProfile": {
        "vmSize": "Standard_A2_v2"
    },
    "osProfile": {
        "computerName": "VM2",
        "adminUsername": "AzureAdmin",
        "adminPassword": "[parameters('adminPassword')]"
    },
    "storageProfile": {
        "imageReference": "[variables('image')]",
        "osDisk": {
            "createOption": "FromImage"
        }
    },
    "networkProfile": {
        "networkInterfaces": [
            {
                "id": "[resourceId('Microsoft.Network/networkInterfaces', 'VM2-NI')]"
            }
        ]
    }
}
}

```

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
VM1 and VM2 can connect to VNET1	<input type="radio"/>	<input type="radio"/>
If an Azure datacenter becomes unavailable, VM1 or VM2 will be available.	<input type="radio"/>	<input type="radio"/>
If the East US 2 region becomes unavailable, VM1 or VM2 will be available.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
VM1 and VM2 can connect to VNET1	<input checked="" type="radio"/>	<input type="radio"/>
If an Azure datacenter becomes unavailable, VM1 or VM2 will be available.	<input checked="" type="radio"/>	<input type="radio"/>
If the East US 2 region becomes unavailable, VM1 or VM2 will be available.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Box 1: Yes -

Box 2: Yes -

VM1 is in Zone1, while VM2 is on Zone2.

Box 3: No -

Reference:

<https://docs.microsoft.com/en-us/azure/architecture/resiliency/recovery-loss-azure-region>

Question: 65

CertyIQ

You have an Azure subscription named Subscription1. Subscription1 contains the resource groups in the following table.

Name	Azure region	Policy
RG1	West Europe	Policy1
RG2	North Europe	Policy2
RG3	France Central	Policy3

RG1 has a web app named WebApp1. WebApp1 is located in West Europe.

You move WebApp1 to RG2.

What is the effect of the move?

- A. The App Service plan for WebApp1 remains in West Europe. Policy2 applies to WebApp1.
- B. The App Service plan for WebApp1 moves to North Europe. Policy2 applies to WebApp1.
- C. The App Service plan for WebApp1 remains in West Europe. Policy1 applies to WebApp1.
- D. The App Service plan for WebApp1 moves to North Europe. Policy1 applies to WebApp1.

Answer: A

Explanation:

You can move an app to another App Service plan, as long as the source plan and the target plan are in the same resource group and geographical region.

The region in which your app runs is the region of the App Service plan it's in. However, you cannot change an App Service plan's region.

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/app-service-plan-manage>

Question: 66

CertyIQ

HOTSPOT -

You have an Azure subscription named Subscription1 that has a subscription ID of c276fc76-9cd4-44c9-99a7-4fd71546436e.

You need to create a custom RBAC role named CR1 that meets the following requirements:

- ⇒ Can be assigned only to the resource groups in Subscription1
- ⇒ Prevents the management of the access permissions for the resource groups
- ⇒ Allows the viewing, creating, modifying, and deleting of resources within the resource groups

What should you specify in the assignable scopes and the permission elements of the definition of CR1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

"assignableScopes": [

"/"
"/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e"
"/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e/resourceGroups"

],

"permissions": [

{

 "actions": [

 "*

],

 "additionalProperties": {},

 "dataActions": [],

 "notActions": [

"Microsoft.Authorization/*"
"Microsoft.Resources/*"
"Microsoft.Security/*"

],

 "notDataActions": []

}

],

Answer:

Answer Area

```
"assignableScopes": [
    "/",
    "/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e",
    "/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e/resourceGroups"
],
"permissions": [
{
    "actions": [
        "*"
    ],
    "additionalProperties": {},
    "dataActions": [],
    "notActions": [
        "Microsoft.Authorization/*",
        "Microsoft.Resources/*",
        "Microsoft.Security/*"
    ]
},
{
    "notDataActions": []
}
]
```

Explanation:

1) "/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e"

2) "Microsoft.Authorization/*"

"assignableScopes" must be the Subscription, so that this Custom Role can be only assignable to Resources Groups under the same Subscription.

"notActions" must deny only the actions that interact with the Authorization API Endpoints. Everything else must\can be allowed.

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles>
<https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftresources>

Question: 67

CertyIQ

You have an Azure subscription.

Users access the resources in the subscription from either home or from customer sites. From home, users must establish a point-to-site VPN to access the Azure resources. The users on the customer sites access the Azure resources by using site-to-site VPNs.

You have a line-of-business-app named App1 that runs on several Azure virtual machine. The virtual machines run Windows Server 2016.

You need to ensure that the connections to App1 are spread across all the virtual machines.

What are two possible Azure services that you can use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. an internal load balancer
- B. a public load balancer
- C. an Azure Content Delivery Network (CDN)
- D. Traffic Manager
- E. an Azure Application Gateway

Answer: AE

Explanation:

A. an internal load balancer: An internal load balancer can be used to distribute traffic among the virtual machines running App1. It can distribute traffic based on various algorithms such as round-robin, least connections, and IP hash. The internal load balancer is a layer 4 (Transport Layer) load balancer that can distribute traffic within a virtual network.

E. an Azure Application Gateway: An Azure Application Gateway is a layer 7 (Application Layer) load balancer that can distribute traffic based on various criteria such as URL path, host headers, and cookie. It can also perform SSL offloading, session affinity, and URL-based routing. It is typically used to route traffic to different backend services based on the incoming request's contents. It is a more advanced option than the internal load balancer but requires a public IP address.

Reference:

<https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/vpn>

<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview> <https://docs.microsoft.com/en-us/azure/application-gateway/overview>

Question: 68

CertyIQ

You have an Azure subscription.

You have 100 Azure virtual machines.

You need to quickly identify underutilized virtual machines that can have their service tier changed to a less expensive offering.

Which blade should you use?

- A. Monitor
- B. Advisor
- C. Metrics
- D. Customer insights

Answer: B

Explanation:

Advisor helps you optimize and reduce your overall Azure spend by identifying idle and underutilized resources. You can get cost recommendations from the Cost tab on the Advisor dashboard.

Reference:

Question: 69

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant.

You need to create a conditional access policy that requires all users to use multi-factor authentication when they access the Azure portal.

Which three settings should you configure? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

* Name

Policy1



Assignments

Users and groups



0 users and groups selected

Cloud apps



0 cloud apps selected

Conditions



0 conditions selected

Access controls

Grant



0 controls selected

Session



Answer:

Answer Area

* Name

Policy1



Assignments

Users and groups



0 users and groups selected

Cloud apps



0 cloud apps selected

Conditions



0 conditions selected

Access controls

Grant



0 controls selected

Session



Explanation:

Select Users & Groups : Where you have to choose all users.

- Select Cloud apps or actions: to specify the Azure portal

- Grant: to grant the MFA.

Those are the minimum requirements to create MFA policy. No conditions are required in the question.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/app-based-mfa>

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-policies>

Question: 70

CertyIQ

You have an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

The User administrator role is assigned to a user named Admin1.

An external partner has a Microsoft account that uses the sign in.

Admin1 attempts to invite the external partner to sign in to the Azure AD tenant and receives the following error message: 'Unable to invite user ' " Generic authorization exception.'

You need to ensure that Admin1 can invite the external partner to sign in to the Azure AD tenant.

What should you do?

- A. From the Users settings blade, modify the External collaboration settings.
- B. From the Custom domain names blade, add a custom domain.
- C. From the Organizational relationships blade, add an identity provider.
- D. From the Roles and administrators blade, assign the Security administrator role to Admin1.

Answer: A

Explanation:

- A. From the Users settings blade, modify the External collaboration settings.

The error message indicates that there's an issue with the external collaboration settings in your Azure Active Directory. These settings dictate who can invite external users and under what circumstances.

To address this issue, you need to adjust the external collaboration settings to allow Admin1 to invite external partners. These settings can be found in the "Users settings" blade in Azure Active Directory.

Reference:

<https://techcommunity.microsoft.com/t5/Azure-Active-Directory/Generic-authorization-exception-inviting-Azure-AD-gests/td-p/274742>

Question: 71

CertyIQ

You have an Azure subscription linked to an Azure Active Directory tenant. The tenant includes a user account named User1.

You need to ensure that User1 can assign a policy to the tenant root management group.

What should you do?

- A. Assign the Owner role for the Azure Subscription to User1, and then modify the default conditional access policies.
- B. Assign the Owner role for the Azure subscription to User1, and then instruct User1 to configure access management for Azure resources.
- C. Assign the Global administrator role to User1, and then instruct User1 to configure access management for

Azure resources.

D. Create a new management group and delegate User1 as the owner of the new management group.

Answer: C

Explanation:

No one is given default access to the root management group. Azure AD Global Administrators are the only users that can elevate themselves to gain access. Once they have access to the root management group, the global administrators can assign any Azure role to other users to manage it.

Reference:

<https://docs.microsoft.com/en-us/azure/governance/management-groups/overview#important-facts-about-the-root-management-group>

<https://docs.microsoft.com/en-us/azure/governance/management-groups/overview>

Question: 72

CertyIQ

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant named adatum.com. Adatum.com contains the groups in the following table.

Name	Group type	Membership type	Membership rule
Group1	Security	Dynamic user	(user.city -startsWith "m")
Group2	Microsoft 365	Dynamic user	(user.department -notIn ["human resources"])
Group3	Microsoft 365	Assigned	<i>Not applicable</i>

You create two user accounts that are configured as shown in the following table.

Name	City	Department	Office 365 license assigned
User1	Montreal	Human resources	Yes
User2	Melbourne	Marketing	No

Of which groups are User1 and User2 members? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User1:

- Group1 only
- Group2 only
- Group3 only
- Group1 and Group2 only
- Group1 and Group3 only
- Group2 and Group3 only
- Group1, Group2, and Group3

User2:

- Group1 only
- Group2 only
- Group3 only
- Group1 and Group2 only
- Group1 and Group3 only
- Group2 and Group3 only
- Group1, Group2, and Group3

Answer:

Answer Area

User1:								
<table border="1"><tr><td>Group1 only</td></tr><tr><td>Group2 only</td></tr><tr><td>Group3 only</td></tr><tr><td>Group1 and Group2 only</td></tr><tr><td>Group1 and Group3 only</td></tr><tr><td>Group2 and Group3 only</td></tr><tr><td>Group1, Group2, and Group3</td></tr></table>		Group1 only	Group2 only	Group3 only	Group1 and Group2 only	Group1 and Group3 only	Group2 and Group3 only	Group1, Group2, and Group3
Group1 only								
Group2 only								
Group3 only								
Group1 and Group2 only								
Group1 and Group3 only								
Group2 and Group3 only								
Group1, Group2, and Group3								
User2:								
<table border="1"><tr><td>Group1 only</td></tr><tr><td>Group2 only</td></tr><tr><td>Group3 only</td></tr><tr><td>Group1 and Group2 only</td></tr><tr><td>Group1 and Group3 only</td></tr><tr><td>Group2 and Group3 only</td></tr><tr><td>Group1, Group2, and Group3</td></tr></table>		Group1 only	Group2 only	Group3 only	Group1 and Group2 only	Group1 and Group3 only	Group2 and Group3 only	Group1, Group2, and Group3
Group1 only								
Group2 only								
Group3 only								
Group1 and Group2 only								
Group1 and Group3 only								
Group2 and Group3 only								
Group1, Group2, and Group3								

Explanation:

Box 1: Group 1 only .

First rule applies -

Box 2: Group1 and Group2 only .

Both membership rules apply.

Reference:

<https://docs.microsoft.com/en-us/sccm/core/clients/manage/collections/create-collections>

Question: 73

CertyIQ

HOTSPOT -

You have a hybrid deployment of Azure Active Directory (Azure AD) that contains the users shown in the following table.

Name	Type	Source
User1	Member	Azure AD
User2	Member	Windows Server Active Directory
User3	Guest	Microsoft account

You need to modify the JobTitle and UsageLocation attributes for the users.

For which users can you modify the attributes from Azure AD? To answer, select the appropriate options in the

answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

JobTitle:

User1 only
User1 and User2 only
User1 and User3 only
User1, User2, and User3

UsageLocation:

User1 only
User1 and User2 only
User1 and User3 only
User1, User2, and User3

Answer:

Answer Area

JobTitle:

User1 only
User1 and User2 only
User1 and User3 only
User1, User2, and User3

UsageLocation:

User1 only
User1 and User2 only
User1 and User3 only
User1, User2, and User3

Explanation:

Box 1:User1 and User3 only

You must use Windows Server Active Directory to update the identity, contact info, or job info for users whose

source of authority is Windows Server Active Directory.

Box 2: User1, User2, and User3

Usage location is an Azure property that can only be modified from Azure AD (for all users including Windows Server AD users synced via Azure AD Connect).

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-profile-azure-portal>

Question: 74

CertyIQ

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 need to ensure that an Azure Active Directory (Azure AD) user named Admin1 is assigned the required role to enable Traffic Analytics for an Azure subscription.

Solution: You assign the Network Contributor role at the subscription level to Admin1.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Your account must meet one of the following to enable traffic analytics:

Your account must have any one of the following Azure roles at the subscription scope: owner, contributor, reader, or network contributor.

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics-faq>

Question: 75

CertyIQ

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 need to ensure that an Azure Active Directory (Azure AD) user named Admin1 is assigned the required role to enable Traffic Analytics for an Azure subscription.

Solution: You assign the Owner role at the subscription level to Admin1.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Your account must meet one of the following to enable traffic analytics:

Your account must have any one of the following Azure roles at the subscription scope: owner, contributor, reader, or network contributor.

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics-faq>

CertyIQ**Question: 76**

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 need to ensure that an Azure Active Directory (Azure AD) user named Admin1 is assigned the required role to enable Traffic Analytics for an Azure subscription.

Solution: You assign the Reader role at the subscription level to Admin1.

Does this meet the goal?

- A. Yes
- B. No

Answer: B**Explanation:**

B. No

Assigning the Reader role at the subscription level to Admin1 does not meet the goal of enabling Traffic Analytics for an Azure subscription. The Reader role has permissions to view resources but does not allow for any write operations, which are required to enable Traffic Analytics. To enable Traffic Analytics, Admin1 would need to be assigned a role that has write permissions, such as the Owner, Contributor, or a custom role with specific permissions for Traffic Analytics.

CertyIQ**Question: 77**

You have an Azure subscription that contains a user named User1.

You need to ensure that User1 can deploy virtual machines and manage virtual networks. The solution must use the principle of least privilege.

Which role-based access control (RBAC) role should you assign to User1?

- A. Owner
- B. Virtual Machine Contributor
- C. Contributor
- D. Virtual Machine Administrator Login

Answer: C**Explanation:**

Contributor: Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC

Incorrect Answers:

- A: Owner: Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.
B: Virtual Machine Contributor: Lets you manage virtual machines, but not access to them, and not the virtual network or storage account they're connected to.
D: Virtual Machine Administrator Login: View Virtual Machines in the portal and login as administrator.

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

Question: 78

CertyIQ

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant that contains three global administrators named Admin1, Admin2, and Admin3.

The tenant is associated to an Azure subscription. Access control for the subscription is configured as shown in the Access control exhibit. (Click the Access Control tab.)

[+ Add](#) [Edit columns](#) [Refresh](#) | [Remove](#) | [Got feedback?](#)

[Check access](#) [Role assignments](#) [Deny assignments](#) [Classic administrators](#) [Roles](#)

Manage access to Azure resources for users, groups, service principals and managed identities at this scope by creating role assignments. [Learn more](#)

Name	Type	Role
<input type="text"/> Search by name or email	All	Owner
Scope	Group by	<input type="text"/> Search for a role
All scopes	Role	<input checked="" type="checkbox"/> Select all <input checked="" type="checkbox"/> Owner

1 items (1 Users)

<input type="checkbox"/> NAME	TYPE	ROLE	SCOPE
OWNER			
Admin3 Admin3@Cont...	User	Owner	This resource

You sign in to the Azure portal as Admin1 and configure the tenant as shown in the Tenant exhibit. (Click the Tenant tab.)

Save Discard

Directory properties

* Name

Cont190525outlook

Country or region

Slovenia

Location

EU Model Clause compliant datacenters

Notification language

English



Directory ID

a93d91a6-faca-4fa6-a749-f6c25469152e



Technical contact



Global privacy contact



Privacy statement URL



Access management for Azure resources

Admin1@Cont190525outlook.onmicrosoft.com (Admin1@Cont190525outlook.onmicrosoft.com) can manage access to all Azure subscriptions and management groups in this directory. [Learn more](#)

Yes

No

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Admin1 can add Admin 2 as an owner of the subscription.	<input type="radio"/>	<input type="radio"/>
Admin3 can add Admin 2 as an owner of the subscription.	<input type="radio"/>	<input type="radio"/>
Admin2 can create a resource group in the subscription.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Admin1 can add Admin 2 as an owner of the subscription.	<input checked="" type="radio"/>	<input type="radio"/>
Admin3 can add Admin 2 as an owner of the subscription.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can create a resource group in the subscription.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Azure (RBAC) and Azure AD roles are independent. AD roles do not grant access to resources and Azure roles do not grant access to Azure AD. However, a Global Administrator in AD can elevate access to all subscriptions and will be User Access Administrator in Azure root scope.

All 3 users are GA (AD) and Admin3 is owner of the subscription (RBAC).

Admin1 has elevated access, so he is also User Access Admin (RBAC).

To assign a user the owner role at the Subscription scope, you require permissions, such as User Access Admin or Owner.

Box 1: Yes

Admin1 has elevated access, so he is User Access Admin. This is valid.

Box 2: Yes

Admi3 is Owner of the Subscription. This is valid.

Box 3: No

Admin2 is just a GA in Azure AD scope. He doesn't have permission in the Subscription.

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/elevate-access-global-admin>

<https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal-subscription-admin>

Question: 79

CertyIQ

You have an Azure subscription named Subscription1 that contains an Azure virtual machine named VM1. VM1 is in a resource group named RG1.

VM1 runs services that will be used to deploy resources to RG1.

You need to ensure that a service running on VM1 can manage the resources in RG1 by using the identity of VM1. What should you do first?

- A. From the Azure portal, modify the Managed Identity settings of VM1
- B. From the Azure portal, modify the Access control (IAM) settings of RG1
- C. From the Azure portal, modify the Access control (IAM) settings of VM1

D. From the Azure portal, modify the Policies settings of RG1

Answer: A

Explanation:

Managed identities for Azure resources provides Azure services with an automatically managed identity in Azure Active Directory. You can use this identity to authenticate to any service that supports Azure AD authentication, without having credentials in your code.

You can enable and disable the system-assigned managed identity for VM using the Azure portal.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/qs-configure-portal-windows-vm>

Question: 80

CertyIQ

You have an Azure subscription that contains a resource group named TestRG.

You use TestRG to validate an Azure deployment.

TestRG contains the following resources:

Name	Type	Description
VM1	Virtual Machine	VM1 is running and configured to back up to Vault1 daily
Vault1	Recovery Services Vault	Vault1 includes all backups of VM1
VNET1	Virtual Network	VNET1 has a resource lock of type Delete

You need to delete TestRG.

What should you do first?

- A. Modify the backup configurations of VM1 and modify the resource lock type of VNET1
- B. Remove the resource lock from VNET1 and delete all data in Vault1
- C. Turn off VM1 and remove the resource lock from VNET1
- D. Turn off VM1 and delete all data in Vault1

Answer: B

Explanation:

When you delete a resource group, all of its resources are also deleted. Deleting a resource group deletes all of its template deployments and currently stored operations.

As an administrator, you can lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. The lock overrides any permissions the user might have.

You can't delete a vault that contains backup data. Once backup data is deleted, it will go into the soft deleted state.

So you have to remove the lock on order to delete the VNET and delete the backups in order to delete the vault.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/delete-resource-group?tabs=azure-powershell>

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources>

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-delete-vault#before-you-start>

Question: 81

CertyIQ

You have an Azure DNS zone named adatum.com.

You need to delegate a subdomain named research.adatum.com to a different DNS server in Azure.

What should you do?

- A. Create an NS record named research in the adatum.com zone.
- B. Create a PTR record named research in the adatum.com zone.
- C. Modify the SOA record of adatum.com.
- D. Create an A record named *.research in the adatum.com zone.

Answer: A

Explanation:

A. Create an NS record named research in the adatum.com zone.

To delegate a subdomain named research.adatum.com to a different DNS server in Azure, you should create an NS (Name Server) record named "research" in the adatum.com zone.

The NS record is used to delegate authority for a subdomain to a different set of name servers. By creating an NS record named "research" in the adatum.com zone and specifying the name server(s) for the subdomain, you can delegate the management of the research.adatum.com subdomain to the specified DNS server(s) in Azure.

You need to create a name server (NS) record for the zone.

Reference:

<https://docs.microsoft.com/en-us/azure/dns/delegate-subdomain>

Question: 82

CertyIQ

DRAG DROP -

You have an Azure Active Directory (Azure AD) tenant that has the contoso.onmicrosoft.com domain name.

You have a domain name of contoso.com registered at a third-party registrar.

You need to ensure that you can create Azure AD users that have names containing a suffix of @contoso.com.

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

Add a record to the public contoso.com DNS zone

Add an Azure AD tenant

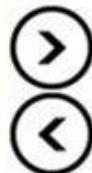
Configure company branding

Create an Azure DNS zone

Add a custom name

Verify the domain

Answer Area



Answer:

Actions

Add an Azure AD tenant

Configure company branding

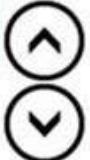
Create an Azure DNS zone

Answer Area

Add a custom name

Add a record to the public contoso.com DNS zone

Verify the domain



Explanation:

Add a custom name: Register the contoso.com domain in your Azure AD tenant.

Add a record to the public contoso.com DNS zone: Add the necessary DNS records at the domain registrar to verify the domain.

Verify the domain: Complete the verification process in Azure AD to confirm ownership of the contoso.com domain.

Reference:

<https://docs.microsoft.com/en-us/azure/dns/dns-web-sites-custom-domain>

You have an Azure subscription named Subscription1 that contains an Azure Log Analytics workspace named Workspace1.

You need to view the error events from a table named Event.

Which query should you run in Workspace1?

- A. Get-Event Event | where \$_.EventType == "error"
- B. Event | search "error"
- C. select * from Event where EventType == "error"
- D. search in (Event) * | where EventType "eq error"

Answer: B

Explanation:

The search operator provides a multi-table/multi-column search experience.

The syntax is:

Table_name | search "search term"

Note:

There are several versions of this question in the exam. The question has three possible correct answers:

- 1. search in (Event) "error"
 - 2. Event | search "error"
 - 3. Event | where EventType == "error"
- Other incorrect answer options you may see on the exam include the following:
- 1. Get-Event Event | where \$_.EventTye "eq "error"
 - 2. Event | where EventType is "error"
 - 3. select * from Event where EventType is "error"
 - 4. search in (Event) * | where EventType "eq "error"

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/search-queries> <https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/get-started-portal> <https://docs.microsoft.com/en-us/azure/data-explorer/kusto/query/searchoperator?pivots=azuredatexplorer>

Question: 84

CertyIQ

You have a registered DNS domain named contoso.com.

You create a public Azure DNS zone named contoso.com.

You need to ensure that records created in the contoso.com zone are resolvable from the internet.

What should you do?

- A. Create NS records in contoso.com.
- B. Modify the SOA record in the DNS domain registrar.
- C. Create the SOA record in contoso.com.
- D. Modify the NS records in the DNS domain registrar.

Answer: D

Explanation:

- D. Modify the NS records in the DNS domain registrar.

To ensure that records created in the contoso.com zone are resolvable from the internet, you need to modify the NS (Name Server) records in the DNS domain registrar.

When you create a public Azure DNS zone named contoso.com, Azure assigns a set of NS records for that zone. These NS records specify the name servers responsible for handling DNS queries for the contoso.com

domain. To make the records in the Azure DNS zone resolvable from the internet, you need to update the NS records at the DNS domain registrar to point to the name servers provided by Azure.

Registrar “owns” the tld and will have their NS registered against the domain by default. By changing the registrar NS records to point to your Azure DNS NS records you take ownership into your Azure DNS.

Reference:

<https://docs.microsoft.com/en-us/azure/dns/dns-delegate-domain-azure-dns>

Question: 85

CertyIQ

HOTSPOT -

You have an Azure subscription that contains a storage account named storage1. The subscription is linked to an Azure Active Directory (Azure AD) tenant named contoso.com that syncs to an on-premises Active Directory domain.

The domain contains the security principals shown in the following table.

Name	Type
User1	User
Computer1	Computer

In Azure AD, you create a user named User2.

The storage1 account contains a file share named share1 and has the following configurations.

```
"kind": "StorageV2",
"properties": {
    "azureFilesIdentityBasedAuthentication": {
        "directoryServiceOptions": "AD",
        "activeDirectoryProperties": {
            "domainName": "Contoso.com",
            "netBiosDomainName": "Contoso.com",
            "forestName": "Contoso.com",
        }
    }
}
```

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
You can assign the Storage File Data SMB Share Contributor role to User1 for share1.	<input type="radio"/>	<input type="radio"/>
You can assign the Storage File Data SMB Share Reader role to Computer1 for share1.	<input type="radio"/>	<input type="radio"/>
You can assign the Storage File Data SMB Share Elevated Contributor role to User2 for share1.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area**Statements****Yes No**You can assign the Storage File Data SMB Share Contributor role to User1 for share1. You can assign the Storage File Data SMB Share Reader role to Computer1 for share1. You can assign the Storage File Data SMB Share Elevated Contributor role to User2 for share1. **Explanation:**

1. You can assign the Storage File Data SMB Share Contributor role to User1 for share1.

Yes. The Storage File Data SMB Share Contributor role allows a user to read, write, and delete files and directories in an Azure file share over SMB (Server Message Block). This role can be assigned to individual users.

2. You can assign the Storage File Data SMB Share Reader role to Computer1 for share1.

NO. Azure RBAC roles apply to Azure AD users, groups, or managed identities, but not directly to computers (e.g., Computer1). Azure does not support assigning roles directly to devices.

3. You can assign the Storage File Data SMB Share Elevated Contributor role to User2 for share1.

Yes. The Storage File Data SMB Share Elevated Contributor role is similar to Contributor but allows assigning NTFS permissions on the file share. It can be assigned to users.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-ad-ds-assign-permissions?tabs=azure-portal>

Question: 86**CertyIQ****HOTSPOT -**

You have an Azure subscription named Subscription1 that contains a virtual network VNet1.

You add the users in the following table.

User	Role
User1	Owner
User2	Security Admin
User3	Network Contributor

Which user can perform each configuration? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Add a subnet to VNet1:

User1 only
User3 only
User1 and User3 only
User2 and User3 only
User1, User2, and User3

Assign a user the Reader role to VNet1:

User1 only
User2 only
User3 only
User1 and User2 only
User2 and User3 only
User1, User2, and User3

Answer:

Answer Area

Add a subnet to VNet1:

User1 only
User3 only
User1 and User3 only
User2 and User3 only
User1, User2, and User3

Assign a user the Reader role to VNet1:

User1 only
User2 only
User3 only
User1 and User2 only
User2 and User3 only
User1, User2, and User3

Explanation:

Box 1: User1 and User3 only.

User1: The Owner Role lets you manage everything, including access to resources.

User3: The Network Contributor role lets you manage networks, including creating subnets.

Box 2: User1 only.

The Security Admin role: In Security Center only: Can view security policies, view security states, edit security policies, view alerts and recommendations, dismiss alerts and recommendations.

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

<https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftnetwork>

HOTSPOT -

You have the Azure resources shown on the following exhibit.



Tenant Root Group



MG1



Sub1



RG1



VM1

You plan to track resource usage and prevent the deletion of resources.

To which resources can you apply locks and tags? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Locks:

- RG1 and VM1 only
- Sub1 and RG1 only
- Sub1, RG1, and VM1 only
- MG1, Sub1, RG1, and VM1 only
- Tenant Root Group, MG1, Sub1, RG1, and VM1

Tags:

- RG1 and VM1 only
- Sub1 and RG1 only
- Sub1, RG1, and VM1 only
- MG1, Sub1, RG1, and VM1 only
- Tenant Root Group, MG1, Sub1, RG1, and VM1

Answer:

Answer Area

Locks:

- RG1 and VM1 only
- Sub1 and RG1 only
- Sub1, RG1, and VM1 only
- MG1, Sub1, RG1, and VM1 only
- Tenant Root Group, MG1, Sub1, RG1, and VM1

Tags:

- RG1 and VM1 only
- Sub1 and RG1 only
- Sub1, RG1, and VM1 only
- MG1, Sub1, RG1, and VM1 only
- Tenant Root Group, MG1, Sub1, RG1, and VM1

Explanation:

Box 1: Sub1, RG1, and VM1 only -

You can lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources.

Box 2: Sub1, RG1, and VM1 only -

You apply tags to your Azure resources, resource groups, and subscriptions.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json> <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources?tabs=json>

Question: 88

CertyIQ

You have an Azure Active Directory (Azure AD) tenant.

You plan to delete multiple users by using Bulk delete in the Azure Active Directory admin center.

You need to create and upload a file for the bulk delete.

Which user attributes should you include in the file?

- A. The user principal name and usage location of each user only
- B. The user principal name of each user only
- C. The display name of each user only
- D. The display name and usage location of each user only
- E. The display name and user principal name of each user only

Answer: B

Explanation:

B. The user principal name of each user only.

The user principal name (UPN) uniquely identifies each user in Azure AD. It is commonly used as the primary identifier for user-related operations, including deletion. When performing a bulk delete, including the UPN of each user is essential for accurately identifying and deleting the intended users.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/users-bulk-delete>

Question: 89**CertyIQ**

HOTSPOT -

You have an Azure subscription named Sub1 that contains the Azure resources shown in the following table.

Name	Type
RG1	Resource group
storage1	Storage account
VNET1	Virtual network

You assign an Azure policy that has the following settings:

- ⇒ Scope: Sub1
- ⇒ Exclusions: Sub1/RG1/VNET1
- ⇒ Policy definition: Append a tag and its value to resources
- ⇒ Policy enforcement: Enabled
- ⇒ Tag name: Tag4
- ⇒ Tag value: value4

You assign tags to the resources as shown in the following table.

Resource	Tag
Sub1	Tag1:subscription
RG1	Tag2:IT
storage1	Tag3:value1
VNET1	Tag3:value2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
RG1 has the Tag2:IT tag assigned only	<input type="radio"/>	<input type="radio"/>
Storage1 has the Tag1:subscription, Tag2:IT, Tag3:value1, and Tag4:value4 tags assigned.	<input type="radio"/>	<input type="radio"/>
VNET1 has the Tag2:IT and Tag3:value2 tags assigned only	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
RG1 has the Tag2:IT tag assigned only	<input type="radio"/>	<input checked="" type="radio"/>
Storage1 has the Tag1:subscription, Tag2:IT, Tag3:value1, and Tag4:value4 tags assigned.	<input type="radio"/>	<input checked="" type="radio"/>
VNET1 has the Tag2:IT and Tag3:value2 tags assigned only	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Box 1: No -

The Azure Policy will add Tag4 to RG1.

Box 2: No -

Tags applied to the resource group or subscription aren't inherited by the resources although you can enable inheritance with Azure Policy. Storage1 has Tag3:

Value1 and the Azure Policy will add Tag4.

Box 3: No -

Tags applied to the resource group or subscription aren't inherited by the resources so VNET1 does not have Tag2.

VNET1 has Tag3:value2. VNET1 is excluded from the Azure Policy so Tag4 will not be added to VNET1.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources?tabs=json>

Question: 90

CertyIQ

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 need to ensure that an Azure Active Directory (Azure AD) user named Admin1 is assigned the required role to

enable Traffic Analytics for an Azure subscription.

Solution: You assign the Traffic Manager Contributor role at the subscription level to Admin1.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

One of the following Azure built-in roles needs to be assigned to your account:

- Owner
- Contributor
- Reader
- Network Contributor

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics#user-access-requirements>

Question: 91

CertyIQ

You have three offices and an Azure subscription that contains an Azure Active Directory (Azure AD) tenant.

You need to grant user management permissions to a local administrator in each office.

What should you use?

- A. Azure AD roles
- B. administrative units
- C. access packages in Azure AD entitlement management
- D. Azure roles

Answer: B

Explanation:

Administrative units restrict permissions in a role to any portion of your organization that you define. You could, for example, use administrative units to delegate the Helpdesk Administrator role to regional support specialists, so they can manage users only in the region that they support.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/roles/administrative-units>

Question: 92

CertyIQ

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 Directory (Azure AD) tenant named Adatum and an Azure Subscription named Subscription1. Adatum contains a group named Developers. Subscription1 contains a resource group named Dev. You need to provide the Developers group with the ability to create Azure logic apps in the Dev resource group. Solution: On Dev, you assign the Logic App Contributor role to the Developers group. Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

"Yes" is correct. Logic App Contributor role will allow you to create Logic Apps.

Your Azure subscription requires Contributor permissions for the resource group that contains that logic app resource. If you create a logic app resource, you automatically have Contributor access."

Reference:

<https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-securing-a-logic-app?tabs=azure-portal>

Question: 93

CertyIQ

HOTSPOT -

You have an Azure Load Balancer named LB1.

You assign a user named User1 the roles shown in the following exhibit.

User1 assignments – LB1

Assignments for the selected user, group, service principal, or managed identity at this scope or inherited to this scope.

Search by assignment name or description

Role assignments (2) ⓘ

Role	D..	Scope	Group assignment
User Access Administrator	L...	This resource	--
Virtual Machine Contributor	L...	Resource group (inherited)	--

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User1 can [answer choice] LB1.

delete
create a NAT rule for
assign access to other users for

User1 can [answer choice] the resource group.

delete a virtual machine from
modify the load balancing rules in
deploy an Azure Kubernetes Service (AKS) cluster to

Answer:

Answer Area

User1 can [answer choice] LB1.

delete
create a NAT rule for
assign access to other users for

User1 can [answer choice] the resource group.

delete a virtual machine from
modify the load balancing rules in
deploy an Azure Kubernetes Service (AKS) cluster to

Explanation:

1. assign access to other users for.

2. delete a Virtual machine from.

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#user-access-administrator>

Lets you manage user access to Azure resources.

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-contributor>

Create and manage virtual machines, manage disks, install and run software, reset password of the root user of the virtual machine using VM extensions, and manage local user accounts using VM extensions. This role does not grant you management access to the virtual network or storage account the virtual machines are connected to. This role does not allow you to assign roles in Azure RBAC.

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-contributor>
<https://docs.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles>

Question: 94

You have an Azure subscription named Subscription1 that contains a virtual network named VNet1. VNet1 is in a resource group named RG1.

Subscription1 has a user named User1. User1 has the following roles:

- ⇒ Reader
- ⇒ Security Admin
- ⇒ Security Reader

You need to ensure that User1 can assign the Reader role for VNet1 to other users.

What should you do?

- A. Remove User1 from the Security Reader role for Subscription1. Assign User1 the Contributor role for RG1.
- B. Assign User1 the Owner role for VNet1.
- C. Assign User1 the Contributor role for VNet1.
- D. Assign User1 the Network Contributor role for VNet1.

Answer: B

Explanation:

Has full access to all resources including the right to delegate access to others.

Note:

There are several versions of this question in the exam. The question has two possible correct answers:

- ⇒ Assign User1 the User Access Administrator role for VNet1.
- ⇒ Assign User1 the Owner role for VNet1.

Other incorrect answer options you may see on the exam include the following:

- ⇒ Remove User1 from the Security Reader and Reader roles for Subscription1. Assign User1 the Contributor role for Subscription1.
- ⇒ Remove User1 from the Security Reader and Reader roles for Subscription1.
- ⇒ Assign User1 the Network Contributor role for RG1.

References:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles>

<https://docs.microsoft.com/en-us/azure/role-based-access-control/overview>

Question: 95

CertyIQ

HOTSPOT -

You configure the custom role shown in the following exhibit.

```
{  
    "properties": {  
        "roleName": "role1",  
        "description": "",  
        "roletype": "true",  
        "assignableScopes": [  
            "/subscriptions/3d6209d5-c714-4440-9556e-d6342086c2d7/"  
        ],  
        "permissions": [  
            {  
                "actions": [  
                    "Microsoft.Authorization/*/read",  
                    "Microsoft.Compute/availabilitySets/*",  
                    "Microsoft.Compute/locations/*",  
                    "Microsoft.Compute/virtualMachines/*",  
                    "Microsoft.Compute/virtualMachineScaleSets/*",  
                    "Microsoft.Compute/disks/write",  
                    "Microsoft.Compute/disks/read",  
                    "Microsoft.Compute/disks/delete",  
                    "Microsoft.Network/locations/*",  
                    "Microsoft.Network/networkInterfaces/*",  
                    "Microsoft.Network/networkSecurityGroups/join/action",  
                    "Microsoft.Network/networkSecurityGroups/read",  
                    "Microsoft.Network/publicIPAddresses/join/action",  
                    "Microsoft.Network/publicIPAddresses/read",  
                    "Microsoft.Network/virtualNetworks/read",  
                    "Microsoft.Network/virtualNetworks/subnets/join/action",  
                    "Microsoft.Resources/deployments/*",  
                    "Microsoft.Resources/subscriptions/resourceGroups/read",  
                    "Microsoft.Support/*"  
                ],  
                "notActions": [],  
                "dataActions": [],  
                "notDataActions": []  
            }  
        ]  
    }  
}
```

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To ensure that users can sign in to virtual machines that are assigned role1, modify the [answer choice] section

▼
actions
roletype
notActions
dataActions
notDataActions
assignableScopes

To ensure that role1 can be assigned only to a resource group named RG1, modify the [answer choice] section

▼
actions
roletype
notActions
dataActions
notDataActions
assignableScopes

Answer:

Answer Area

To ensure that users can sign in to virtual machines that are assigned role1, modify the [answer choice] section

▼	
actions	
roletype	
notActions	
dataActions	
notDataActions	
assignableScopes	

To ensure that role1 can be assigned only to a resource group named RG1, modify the [answer choice] section

▼	
actions	
roletype	
notActions	
dataActions	
notDataActions	
assignableScopes	

Explanation:

Box 1: dataActions -

An array of strings that specifies the data plane actions that the role allows to be performed to your data within that object.

assignableScopes: An array of strings that specifies the scopes that the role is available for assignment.

<https://learn.microsoft.com/en-us/azure/role-based-access-control/role-definitions>.

Box 2: assignableScopes -

Azure role-based access control (Azure RBAC) is the authorization system you use to manage access to Azure resources. To grant access, you assign roles to users, groups, service principals, or managed identities at a particular scope.

When you assign roles, you must specify a scope. Scope is the set of resources the access applies to. In Azure, you can specify a scope at four levels from broad to narrow: management group, subscription, resource group, and resource.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/devices/howto-vm-sign-in-azure-ad-windows>

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

<https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal>

Question: 96

CertyIQ

You have an Azure subscription that contains a storage account named storage1. The storage1 account contains a file share named share1.

The subscription is linked to a hybrid Azure Active Directory (Azure AD) tenant that contains a security group named Group1.

You need to grant Group1 the Storage File Data SMB Share Elevated Contributor role for share1.

What should you do first?

- A. Enable Active Directory Domain Service (AD DS) authentication for storage1.
- B. Grant share-level permissions by using File Explorer.
- C. Mount share1 by using File Explorer.
- D. Create a private endpoint.

Answer: A

Explanation:

Before you enable Azure AD over SMB for Azure file shares, make sure you have completed the following prerequisites:

1. Select or create an Azure AD tenant.
 2. To support authentication with Azure AD credentials, you must enable Azure AD Domain Services for your Azure AD tenant.
- Etc.

Note: The Storage File Data SMB Share Elevated Contributor allows read, write, delete and modify NTFS permissions in Azure Storage file shares over SMB.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-active-directory-domain-service-enable>

Question: 97

CertyIQ

You have 15 Azure subscriptions.

You have an Azure Active Directory (Azure AD) tenant that contains a security group named Group1.

You plan to purchase additional Azure subscription.

You need to ensure that Group1 can manage role assignments for the existing subscriptions and the planned

subscriptions. The solution must meet the following requirements:

- ⇒ Use the principle of least privilege.
- ⇒ Minimize administrative effort.

What should you do?

- A. Assign Group1 the Owner role for the root management group.
- B. Assign Group1 the User Access Administrator role for the root management group.
- C. Create a new management group and assign Group1 the User Access Administrator role for the group.
- D. Create a new management group and assign Group1 the Owner role for the group.

Answer: B

Explanation:

The User Access Administrator role is the required role to manage role assignments using the least privileged model. The Owner role provides more elevated privileges than required and does not follow the least privileged model making answers A and D incorrect. Per requirements ⇒ Use the principle of least privilege and ⇒ Minimize administrative effort, assigning Group1 the User Access Administrator role for the root management group satisfies both requirements. It allows for all subscriptions (current and planned) to inherit the permissions granted to Group1. C is incorrect because in addition to creating a new management group and assigning Group1 the User Access Administrator role for the group you will have to move the current subscriptions and newly planned subscriptions to the new management group that you created. This does not satisfy the ⇒ Minimize administrative effort requirement.

Question: 98

CertyIQ

HOTSPOT -

You have an Azure subscription that contains the hierarchy shown in the following exhibit.



You create an Azure Policy definition named Policy1.

To which Azure resources can you assign Policy1 and which Azure resources can you specify as exclusions from Policy1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

You can assign Policy1 to:

Subscription1 and RG1 only
ManagementGroup1 and Subscription1 only
Tenant Root Group, ManagementGroup1, and Subscription1 only
Tenant Root Group, ManagementGroup1, Subscription1, and RG1 only
Tenant Root Group, ManagementGroup1, Subscription1, RG1, and VM1

You can exclude Policy1 from:

VM1 only
RG1 and VM1 only
Subscription1, RG1, and VM1 only
ManagementGroup1, Subscription1, RG1, and VM1 only
Tenant Root Group, ManagementGroup1, Subscription1, RG1, and VM1

Answer:

Answer Area

You can assign Policy1 to:

Subscription1 and RG1 only
ManagementGroup1 and Subscription1 only
Tenant Root Group, ManagementGroup1, and Subscription1 only
Tenant Root Group, ManagementGroup1, Subscription1, and RG1 only
Tenant Root Group, ManagementGroup1, Subscription1, RG1, and VM1

You can exclude Policy1 from:

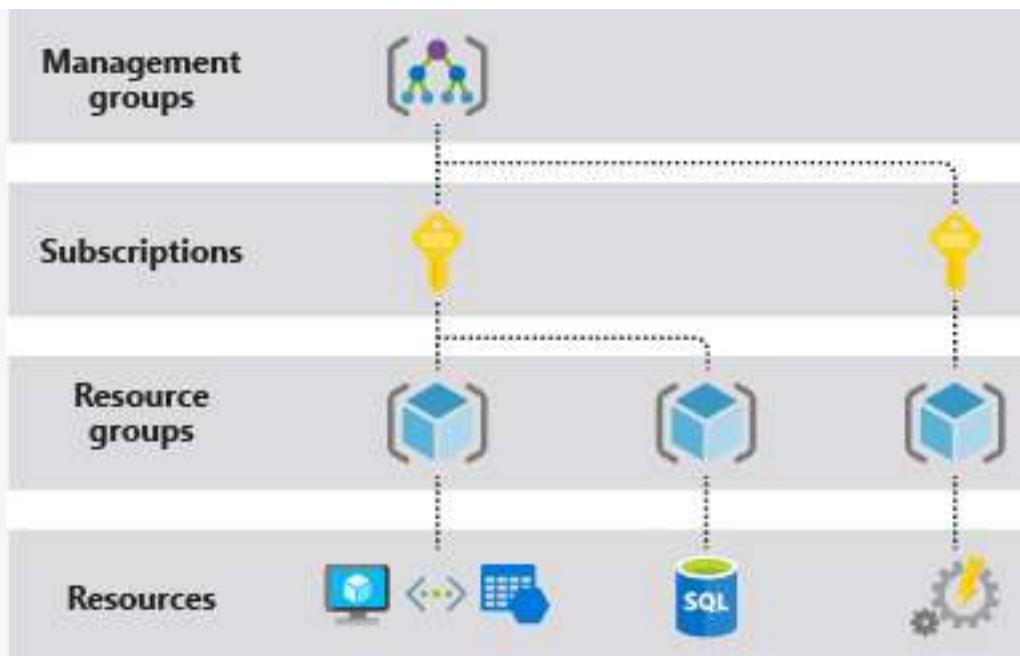
VM1 only
RG1 and VM1 only
Subscription1, RG1, and VM1 only
ManagementGroup1, Subscription1, RG1, and VM1 only
Tenant Root Group, ManagementGroup1, Subscription1, RG1, and VM1

Explanation:

Box 1: Tenant Root Group, ManagementGroup1, Subscription1, RG1, and VM1

Once your business rules have been formed, the policy definition or initiative is assigned to any scope of resources that Azure supports, such as management groups, subscriptions, resource groups, or individual resources.

Note: Azure provides four levels of scope: management groups, subscriptions, resource groups, and resources. The following image shows an example of these layers.



Box 2: ManagementGroup1, Subscription1, RG1, and VM1

You can exclude a subscope from the assignment.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/overview>

Question: 99

CertyIQ

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 subscription that contains the following users in an Azure Active Directory tenant named contoso.onmicrosoft.com:

Name	Role	Scope
User1	Global administrator	Azure Active Directory
User2	Global administrator	Azure Active Directory
User3	User administrator	Azure Active Directory
User4	Owner	Azure Subscription

User1 creates a new Azure Active Directory tenant named external.contoso.onmicrosoft.com.

You need to create new user accounts in external.contoso.onmicrosoft.com.

Solution: You instruct User2 to create the user accounts.

Does that meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

After User1 creates a new Azure Active Directory tenant named external.contoso.onmicrosoft.com, User-1

becomes owner and Global Administrator of external.contoso.onmicrosoft.com.

BUT User-2 doesn't have any authorization in new tenant. User-2's Global Administrator Role applies to contoso.onmicrosoft.com NOT for external.contoso.onmicrosoft.com.

SO User-1 can not instruct User2 to create the user accounts.

MAYBE that can be done after User-1 assigns Global Administrator or User Access Administrator Role to User-2.

Question: 100

CertyIQ

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 subscription that contains the following users in an Azure Active Directory tenant named contoso.onmicrosoft.com:

Name	Role	Scope
User1	Global administrator	Azure Active Directory
User2	Global administrator	Azure Active Directory
User3	User administrator	Azure Active Directory
User4	Owner	Azure Subscription

User1 creates a new Azure Active Directory tenant named external.contoso.onmicrosoft.com.

You need to create new user accounts in external.contoso.onmicrosoft.com.

Solution: You instruct User4 to create the user accounts.

Does that meet the goal?

A. Yes

B. No

Answer: B

Explanation:

when you create a new tenant, the creator is the only global admin and owner, he must first give access to others to allow anything.

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-access-create-new-tenant#your-user-account-in-the-new-tenant>

Question: 101

CertyIQ

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 subscription that contains the following users in an Azure Active Directory tenant named contoso.onmicrosoft.com:

Name	Role	Scope
User1	Global administrator	Azure Active Directory
User2	Global administrator	Azure Active Directory
User3	User administrator	Azure Active Directory
User4	Owner	Azure Subscription

User1 creates a new Azure Active Directory tenant named external.contoso.onmicrosoft.com.

You need to create new user accounts in external.contoso.onmicrosoft.com.

Solution: You instruct User3 to create the user accounts.

Does that meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Only a global administrator can add users to this tenant.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/organizations/accounts/add-users-to-azure-ad>

Question: 102

CertyIQ

You have two Azure subscriptions named Sub1 and Sub2.

An administrator creates a custom role that has an assignable scope to a resource group named RG1 in Sub1.

You need to ensure that you can apply the custom role to any resource group in Sub1 and Sub2. The solution must minimize administrative effort.

What should you do?

- A. Select the custom role and add Sub1 and Sub2 to the assignable scopes. Remove RG1 from the assignable scopes.
- B. Create a new custom role for Sub1. Create a new custom role for Sub2. Remove the role from RG1.
- C. Create a new custom role for Sub1 and add Sub2 to the assignable scopes. Remove the role from RG1.
- D. Select the custom role and add Sub1 to the assignable scopes. Remove RG1 from the assignable scopes. Create a new custom role for Sub2.

Answer: A

Explanation:

Can be used as:

```
"AssignableScopes": [
  "/subscriptions/ Sub1 ",
  "/subscriptions/ Sub2 "]
```

Note: Custom role example:

The following shows what a custom role looks like as displayed using Azure PowerShell in JSON format. This custom role can be used for monitoring and restarting virtual machines.

```
"Name": "Virtual Machine Operator",
"Id": "88888888-8888-8888-8888-888888888888",
"IsCustom": true,
```

```

"Description": "Can monitor and restart virtual machines.",
"Actions": [
    "Microsoft.Storage/*/read",
    "Microsoft.Network/*/read",
    "Microsoft.Compute/*/read",
    "Microsoft.Compute/virtualMachines/start/action",
    "Microsoft.Compute/virtualMachines/restart/action",
    "Microsoft.Authorization/*/read",
    "Microsoft.ResourceHealth/availabilityStatuses/read",
    "Microsoft.Resources/subscriptions/resourceGroups/read",
    "Microsoft.Insights/alertRules/*",
    "Microsoft.Insights/diagnosticSettings/*",
    "Microsoft.Support/*"
],
"NotActions": [],
"DataActions": [],
"NotDataActions": [],
"AssignableScopes": [
    "/subscriptions/ subscriptionId1 ",
    "/subscriptions/ subscriptionId2 ",
    "/providers/Microsoft.Management/managementGroups/ groupId1 "
]

```

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles>

Question: 103

CertyIQ

You have an Azure Subscription that contains a storage account named storageacct1234 and two users named User1 and User2.

You assign User1 the roles shown in the following exhibit.

User1 assignments – storageacct1234

Assignments for the selected user, group, service principal, or managed identity at this scope or inherited to this scope.

Search by assignment name or description

Role assignments (2) <small>(i)</small>			
Role	Scope	Group assignment	Condition
Reader	Resource group (inherited)	--	None
Storage Blob Data Contributor	This resource	--	Add

Deny assignments (0) (i)

Classic administrators (0) (i)

Which two actions can User1 perform? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Assign roles to User2 for storageacct1234.

- B. Upload blob data to storageacct1234.
- C. Modify the firewall of storageacct1234.
- D. View blob data in storageacct1234.
- E. View file shares in storageacct1234.

Answer: BD

Explanation:

Upload blob data to storageacct1234: User1 has been assigned the “Storage Blob Data Contributor” role for the storage account named storageacct1234. This role allows them to upload data to blob containers within that storage account.

View blob data in storageacct1234: Additionally, User1 has the “Reader” role at the Resource group (inherited) scope. While this role doesn’t provide read permissions to data in Azure Storage, it does allow User1 to view storage account resources, including blob containers. Therefore, User1 can view blob data within the storageacct1234 storage account.

Question: 104

CertyIQ

You have an Azure subscription named Subscription1 that contains an Azure Log Analytics workspace named Workspace1.

You need to view the error events from a table named Event.

Which query should you run in Workspace1?

- A. select * from Event where EventType == "error"
- B. Event | search "error"
- C. Event | where EventType is "error"
- D. Get-Event Event | where \$_.EventType == "error"

Answer: B

Explanation:

Both B & C are OK, other possibilities are:

- 1) Event | search "Error"
- 2) Event | where eventType = "Error"
- 3) Search in (Event) "Error"

Question: 105

CertyIQ

You have an Azure App Services web app named App1.

You plan to deploy App1 by using Web Deploy.

You need to ensure that the developers of App1 can use their Azure AD credentials to deploy content to App1. The solution must use the principle of least privilege.

What should you do?

- A. Assign the Owner role to the developers
- B. Configure app-level credentials for FTPS
- C. Assign the Website Contributor role to the developers
- D. Configure user-level credentials for FTPS

Answer: C

Explanation:

C. Assign the Website Contributor role to the developers.

Assigning the Website Contributor role to the developers would grant them the necessary permissions to deploy content to the Azure App Services web app (App1) without giving them excessive privileges. This role provides the necessary permissions for managing the website, including deployment, without granting ownership or administrative rights, thus adhering to the principle of least privilege.

Question: 106

CertyIQ

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 Active Directory (Azure AD) tenant named contoso.com.

You have a CSV file that contains the names and email addresses of 500 external users.

You need to create a guest user account in contoso.com for each of the 500 external users.

Solution: From Azure AD in the Azure portal, you use the Bulk invite users operation.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

The question states "You have a CSV file that contains the names and email addresses of 500 external users."

This implies that the required fields (Email and Redirection URL) are missing from the .csv file.

Here are the csv field pre-requisites that are needed for bulk upload of external users:

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/tutorial-bulk-invite#prerequisites>

Question: 107

CertyIQ

HOTSPOT

You have an Azure subscription that is linked to an Azure AD tenant. The tenant contains the custom role-based access control (RBAC) roles shown in the following table.

Name	Description
Role1	Azure subscription role
Role2	Azure AD role

From the Azure portal, you need to create two custom roles named Role3 and Role4. Role3 will be an Azure subscription role. Role4 will be an Azure AD role.

Which roles can you clone to create the new roles? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Role3:

- Role1 only
- Built-in Azure subscription roles only
- Role1 and built-in Azure subscription roles only
- Built-in Azure subscription roles and built-in Azure AD roles only
- Role1, Role2, built-in Azure subscription roles, and built-in Azure AD roles**

Role4:

- Role2 only
- Built-in Azure AD roles only
- Role2 and built-in Azure AD roles only
- Built-in Azure AD roles and built-in Azure subscription roles only
- Role1, Role2, built-in Azure AD, and built-in Azure subscription roles**

Answer:

Answer Area

Role3:

- Role1 only
- Built-in Azure AD roles only
- Role1 and built-in Azure AD roles only**
- Role1, built-in Azure AD roles, and built-in Azure subscription roles

Role4:

- Role2 only**
- Built-in Azure AD roles only
- Role2 and built-in Azure subscription roles only
- Role2, built-in Azure subscription roles, and built-in Azure AD roles

Explanation:

Role3: Role1 and built-in Azure AD roles only.

Role4: Role2 only

There's a difference between Built-in AD roles and Built-in Subscription roles.

Built-in AD roles can't be cloned, but built-in subscription roles can be. Custom roles of either type can be cloned.

To clone the Bulit-in subscription Role, you open the subscription or the Resource group where you want to create the custom role and assign the permissions --> Go to Access Control (IAM) --> Roles tab --> Search for the subscription Role then clone it from the three dots in the right of the role.

Reference: <https://learn.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal>

Question: 108

CertyIQ

DRAG DROP

You have an Azure subscription named Sub1 that contains two users named User1 and User2.

You need to assign role-based access control (RBAC) roles to User1 and User2. The users must be able to perform the following tasks in Sub1:

- User1 must view the data in any storage account.
- User2 must assign users the Contributor role for storage accounts.

The solution must use the principle of least privilege.

Which RBAC role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

RBAC roles

Owner

Contributor

Reader and Data Access

Storage Account Contributor

Answer Area

User1:

User2:

Answer:

Answer Area

User1: Reader and Data Access

User2: Owner

Explanation:

"Reader and Data Access":

"Lets you view everything but will not let you delete or create a storage account or contained resource. It will also allow read/write access to all data contained in a storage account via access to storage account keys."

"Owner" is needed to manage permissions, as "User Access Administrator" is not offered as an option.

CertyIQ

Question: 109

You have an Azure subscription that contains 10 virtual machines, a key vault named Vault1, and a network security group (NSG) named NSG1. All the resources are deployed to the East US Azure region.

The virtual machines are protected by using NSG1. NSG1 is configured to block all outbound traffic to the internet.

You need to ensure that the virtual machines can access Vault1. The solution must use the principle of least privilege and minimize administrative effort

What should you configure as the destination of the outbound security rule for NSG1?

- A. an application security group
- B. a service tag
- C. an IP address range

Answer: B

Explanation:

B. a service tag.

In order to ensure that the virtual machines can access Vault1 while also using the principle of least privilege and minimizing administrative effort, you should configure a service tag as the destination of the outbound security rule for NSG1. Service tags represent a group of IP addresses associated with Azure PaaS and SaaS services. By specifying a service tag as the destination of the outbound security rule, you can allow the virtual machines to access Vault1 without having to manually specify the IP addresses of Vault1. This reduces administrative effort and ensures that the virtual machines are only able to access Vault1, rather than any other internet destination.

CertyIQ

Question: 110

You have an Azure AD tenant named adatum.com that contains the groups shown in the following table.

Name	Member of
Group1	None
Group2	Group1
Group3	Group2

Adatum.com contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3
User4	None

You assign the Azure Active Directory Premium Plan 2 license to Group1 and User4.

Which users are assigned the Azure Active Directory Premium Plan 2 license?

- A. User4 only
- B. User1 and User4 only
- C. User1, User2, and User4 only
- D. User1, User2, User3, and User4

Answer: B

Explanation:

User1 and User4 only.

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced>

"Group-based licensing currently doesn't support groups that contain other groups (nested groups). If you apply a license to a nested group, only the immediate first-level user members of the group have the licenses applied."

Question: 111

CertyIQ

HOTSPOT

You have an Azure AD tenant named contoso.com.

You have two external partner organizations named fabrikam.com and litwareinc.com. Fabrikam.com is configured as a connected organization.

You create an access package as shown in the Access package exhibit. (Click the Access package tab.)

New access package

[* Basics](#) [Resource roles](#) [* Requests](#) [Requestor information](#) [* Lifecycle](#) [Review + Create](#)

Summary of access package configuration

Basics

Name	package1
Description	Guest users
Catalog name	General

Resource roles

Resource	Type	Sub Type	Role
Group1	Group and Team	Security Group	Member

Requests

Users who can request access	All configured connected organizations
Require approval	No
Enabled	Yes

Requestor information

Questions

Question	Answer format	Multiple choice options	Required

Attributes (Preview)

Attribute type	Attribute	Default display string	Answer format	Multi

Lifecycle

Access package assignments expire	After 365 days
Require access reviews	No

You configure the external user lifecycle settings as shown in the Lifecycle exhibit. (Click the Lifecycle tab.)

Manage the lifecycle of external users

Select what happens when an external user, who was added to your directory through an access package request, loses their last assignment to any access package.

Block external user from signing in to this directory

Yes No

Remove external user

Yes No

Number of days before removing external user from this directory

30

Delegate entitlement management

By default, only Global Administrators and User Administrators can create and manage catalogs, and can manage all catalogs. Users added to entitlement management as Catalog creators can also create catalogs and will become the owner of any catalogs they create.

Catalog creators (1) 0 selected

Add catalog creators

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Litwareinc.com users can be assigned to package1.	<input type="radio"/>	<input type="radio"/>
After 365 days, fabrikam.com users will be removed from Group1.	<input type="radio"/>	<input type="radio"/>
After 395 days, fabrikam.com users will be removed from the contoso.com tenant.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
Litwareinc.com users can be assigned to package1.	<input type="radio"/>	<input checked="" type="radio"/>
After 365 days, fabrikam.com users will be removed from Group1.	<input type="radio"/>	<input checked="" type="radio"/>
After 395 days, fabrikam.com users will be removed from the contoso.com tenant.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

N Litware is not a connected organization

N expired, not remove

Y $365 + 30 = 395$ removed

<https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-external-users>

You can select what happens when an external user, who was invited to your directory through making an access package request, no longer has any access package assignments. This can happen if the user

relinquishes all their access package assignments, or their last access package assignment expires. By default, when an external user no longer has any access package assignments, they're blocked from signing in to your directory. After 30 days, their guest user account is removed from your directory.

If you want to remove the guest user account in this directory, you can set the number of days before it's removed. If you want to remove the guest user account as soon as they lose their last assignment to any access packages, set Number of days before removing external user from this directory to 0.

<https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-external-users>

Question: 112

CertyIQ

You have an Azure subscription named Subscription1 that contains a virtual network named VNet1. VNet1 is in a resource group named RG1.

Subscription1 has a user named User1. User1 has the following roles:

- Reader
- Security Admin
- Security Reader

You need to ensure that User1 can assign the Reader role for VNet1 to other users.

What should you do?

- A. Assign User1 the Network Contributor role for VNet1.
- B. Remove User1 from the Security Reader role for Subscription1. Assign User1 the Contributor role for RG1.
- C. Assign User1 the Owner role for VNet1.
- D. Assign User1 the Network Contributor role for RG1.

Answer: C

Explanation:

C. Assign User1 the Owner role for VNet1.

User1 currently has the following roles:

Reader: Can view resources but cannot modify or assign roles.

Security Admin: Can manage security policies but cannot assign roles.

Security Reader: Can view security-related information but cannot assign roles.

To allow User1 to assign the Reader role for VNet1 to other users, User1 must have RBAC permissions to grant roles. This requires the Owner or User Access Administrator role.

Question: 113

CertyIQ

HOTSPOT

-

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

Name	Member of
User1	Group1
User2	Group2
User3	Group3

The groups are configured as shown in the following table.

Name	Type	Azure AD roles can be assigned to the group
Group1	Security	Yes
Group2	Security	Yes
Group3	Microsoft 365	Yes

You have a resource group named RG1 as shown in the following exhibit.

RG1 | Access control (IAM)

Resource group

Search (Ctrl+ /)

Add Download role assignments Edit columns Refresh Remove

Overview Activity log Access control (IAM) Tags Resource visualizer Events

Check access Role assignments Roles Deny assignments Classic administrator

Number of role assignments for this subscription 2 2000

Search by name or email Type : All Role : All Scope : All sc

2 items (1 Users, 1 Groups)

Name	Type	Role	Scope	Condition
GR	Group	Owner	This resource	None
prvi...	User	Owner	Subscription (Inherited)	None

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
You can assign User2 the Owner role for RG1 by adding Group2 as a member of Group1.	<input type="radio"/>	<input type="radio"/>
You can assign User3 the Owner role for RG1 by adding Group3 as a member of Group1.	<input type="radio"/>	<input type="radio"/>
You can assign User3 the Owner role for RG1 by assigning the Owner role to Group3 for	<input type="radio"/>	<input type="radio"/>

Answer:**Answer Area****Statements**

	Yes	No
You can assign User2 the Owner role for RG1 by adding Group2 as a member of Group1.	<input type="radio"/>	<input checked="" type="radio"/>
You can assign User3 the Owner role for RG1 by adding Group3 as a member of Group1.	<input type="radio"/>	<input checked="" type="radio"/>
You can assign User3 the Owner role for RG1 by assigning the Owner role to Group3 for	<input checked="" type="radio"/>	<input type="radio"/>

You can assign User2 the Owner role for RG1 by adding Group2 as a member of Group1.

You can assign User3 the Owner role for RG1 by adding Group3 as a member of Group1.

You can assign User3 the Owner role for RG1 by assigning the Owner role to Group3 for

Explanation:

1. No, role assignments do not automatically propagate to nested groups in Azure. Azure Role-Based Access Control (RBAC) does not support the automatic inheritance of role assignments for nested groups.
2. No, a Microsoft 365 group cannot be a member of a security group in Azure AD. Microsoft 365 groups (formerly known as Office 365 groups) are designed primarily for collaboration purposes and integrate with tools like Outlook, Teams, SharePoint, and others. They are different from security groups, which are used for managing permissions to resources within Azure and other Microsoft services.
3. Yes, a Microsoft 365 group can be assigned as the owner of a resource group in Azure. In Azure Role-Based Access Control (RBAC), you can assign roles, including the "Owner" role, to users, security groups, or Microsoft 365 groups.

CertyIQ**Question: 114**

You have an Azure subscription named Subscription1 that contains a virtual network named VNet1. VNet1 is in a resource group named RG1.

Subscription1 has a user named User1. User1 has the following roles:

- Reader
- Security Admin
- Security Reader

You need to ensure that User1 can assign the Reader role for VNet1 to other users.

What should you do?

- A. Remove User1 from the Security Reader role for Subscription1. Assign User1 the Contributor role for RG1.
- B. Assign User1 the Owner role for VNet1.
- C. Remove User1 from the Security Reader and Reader roles for Subscription1. Assign User1 the Contributor role for Subscription1.
- D. Assign User1 the Contributor role for VNet1.

Answer: B**Explanation:**

B. Assign User1 the Owner role for VNet1.

User1 currently has the following roles:

Reader: Can view resources but cannot modify or assign roles.

Security Admin: Can manage security policies but cannot assign roles.

Security Reader: Can view security-related information but cannot assign roles.

To allow User1 to assign the Reader role for VNet1 to other users, User1 must have permission to manage RBAC (role-based access control) assignments. This requires the Owner or User Access Administrator role.

Question: 115

CertyIQ

Your on-premises network contains a VPN gateway.

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

Name	Type	Description
vgw1	Virtual network gateway	Gateway for Site-to-Site VPN to the on-premises network
storage1	Storage account	Standard performance tier
Vnet1	Virtual network	Enabled forced tunneling
VM1	Virtual machine	Connected to Vnet1

You need to ensure that all the traffic from VM1 to storage1 travels across the Microsoft backbone network.

What should you configure?

- A. Azure Application Gateway
- B. private endpoints
- C. a network security group (NSG)
- D. Azure Virtual WAN

Answer: B

Explanation:

Private endpoints are used to provide secure and private connectivity from a virtual network to Azure storage. When you configure a private endpoint, a private IP address is assigned to the storage account within the virtual network. All traffic to the storage account goes over the Microsoft backbone network, rather than over the public internet, providing increased security and reliability. By configuring a private endpoint for the storage account in this scenario, you can ensure that all the traffic from VM1 to storage1 travels across the Microsoft backbone network.

Question: 116

CertyIQ

HOTSPOT

You have an Azure subscription that contains a user named User1 and the resources shown in the following table.

Name	Type
RG1	Resource group
networkinterface1	Virtual network interface
NSG1	Network security group (NSG)

NSG1 is associated to networkinterface1.

User1 has role assignments for NSG1 as shown in the following table.

Role	Scope
Contributor	This resource
Reader	Subscription (Inherited)
Storage Account Contributor	Resource group (Inherited)

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can create a storage account in RG1.	<input type="radio"/>	<input type="radio"/>
User1 can modify the DNS settings of networkinterface1.	<input type="radio"/>	<input type="radio"/>
User1 can create an inbound security rule to filter inbound traffic to networkinterface1.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 can create a storage account in RG1.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
User1 can modify the DNS settings of networkinterface1.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
User1 can create an inbound security rule to filter inbound traffic to networkinterface1.	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Explanation:

YES, No, Yes

(YES) User1 can create a storage account in RG1, since User1 has Storage Account Contribute Role inherited from Resource Group.

(NO) User1 can modify the DNS settings of networkinterface1, since it requires Network Contribute role referring to the following link.

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface?tabs=network-interface-portal#permissions>

(YES) User1 can create an inbound security rule to filter inbound traffic to networkinterface1, since User1 has

Question: 117

You have an Azure subscription named Subscription1 that contains a virtual network named VNet1. VNet1 is in a resource group named RG1.

Subscription1 has a user named User1. User1 has the following roles:

- Reader
- Security Admin
- Security Reader

You need to ensure that User1 can assign the Reader role for VNet1 to other users.

What should you do?

- A. Remove User1 from the Security Reader role for Subscription1. Assign User1 the Contributor role for RG1.
- B. Assign User1 the Access Administrator role for VNet1.
- C. Remove User1 from the Security Reader and Reader roles for Subscription1. Assign User1 the Contributor role for Subscription1.
- D. Assign User1 the Network Contributor role for RG1.

Answer: B**Explanation:**

B. Assign User1 the Access Administrator role for VNet1.

User1 currently has the following roles:

Reader: Can view resources but cannot modify or assign roles.

Security Admin: Can manage security policies but cannot assign roles.

Security Reader: Can view security-related information but cannot assign roles.

To assign roles to other users, User1 must have permission to manage access control (RBAC). This requires the "User Access Administrator" role, which is often referred to as Access Administrator.

Question: 118

HOTSPOT

-

You have three Azure subscriptions named Sub1, Sub2, and Sub3 that are linked to an Azure AD tenant.

The tenant contains a user named User1, a security group named Group1, and a management group named MG1. User1 is a member of Group1.

Sub1 and Sub2 are members of MG1. Sub1 contains a resource group named RG1. RG1 contains five Azure functions.

You create the following role assignments for MG1:

- Group1: Reader
- User1: User Access Administrator

You assign User the Virtual Machine Contributor role for Sub1 and Sub2.

Answer Area

Statements	Yes	No
The Group1 members can view the configurations of the Azure functions.	<input type="radio"/>	<input type="radio"/>
User1 can assign the Owner role for RG1.	<input type="radio"/>	<input type="radio"/>
User1 can create a new resource group and deploy a virtual machine to the new group.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
The Group1 members can view the configurations of the Azure functions.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can assign the Owner role for RG1.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can create a new resource group and deploy a virtual machine to the new group.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Y/N.

1) GROUP1 Reader access, provides access to view all items, except secrets

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#reader>

2) To Assign OWNER role, you need to either Owner role or User Administrator Access Role

<https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal-subscription-admin#prerequisites>

3) Neither User Access Admin Role nor the Reader Role allows to create new resources.

<https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-steps>

Question: 119

CertyIQ

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

Name	Description
share1	File share in storage1
storage1	Storage account
User1	Azure AD user

You need to assign User1 the Storage File Data SMB Share Contributor role for share1.

What should you do first?

- A. Enable identity-based data access for the file shares in storage1.
- B. Modify the security profile for the file shares in storage1.
- C. Select Default to Azure Active Directory authorization in the Azure portal for storage1.
- D. Configure Access control (IAM) for share1.

Answer: A

Explanation:

A. Enable identity-based data access for the file shares in storage1.

Enabling identity-based data access for file shares is a prerequisite for assigning roles like the Storage File Data SMB Share Contributor role. Without enabling this feature, Azure AD authentication and authorization for accessing file shares would not be possible.

Question: 120

CertyIQ

You have an Azure subscription named Subscription1 that contains a virtual network named VNet1. VNet1 is in a resource group named RG1.

Subscription1 has a user named User1. User1 has the following roles:

- Reader
- Security Admin
- Security Reader

You need to ensure that User1 can assign the Reader role for VNet1 to other users.

What should you do?

- A. Remove User1 from the Security Reader role for Subscription1. Assign User1 the Contributor role for RG1.
- B. Assign User1 the User Access Administrator role for VNet1.
- C. Remove User1 from the Security Reader and Reader roles for Subscription1.
- D. Assign User1 the Contributor role for VNet1.

Answer: B

Explanation:

B. Assign User1 the User Access Administrator role for VNet1.

User1 currently has the following roles:

Reader → Can view resources but cannot modify or assign roles.

Security Admin → Can manage security policies but cannot assign roles.

Security Reader → Can view security-related information but cannot assign roles.

To assign the Reader role for VNet1 to other users, User1 must have permission to manage role assignments (RBAC).

This requires the "User Access Administrator" role, which allows users to assign roles without granting full ownership permissions.

Question: 121

CertyIQ

HOTSPOT

You have an Azure AD tenant named adatum.com that contains the groups shown in the following table.

Name	Type	Member of
Group1	Security	None
Group2	Security	Group1

Adatum.com contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2

You assign an Azure Active Directory Premium P2 license to Group1 as shown in the following exhibit.

Assign license

...



Got feedback?

Users and groups

Assignment options

Review + assign

Azure Active Directory Premium P2

Azure Active Directory Premium P1

Off

On

Azure Active Directory Premium P2

Off

On

Microsoft Azure Multi-Factor
Authentication

Off

On

Microsoft Defender for Cloud Apps
Discovery

Off

On

Group2 is NOT directly assigned a license.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
You can assign User1 the Microsoft Defender for Cloud Apps Discovery license.	<input type="radio"/>	<input type="radio"/>
You can remove the Azure Active Directory Premium P2 license from User1.	<input type="radio"/>	<input type="radio"/>
User2 is assigned the Azure Active Directory Premium P2.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
You can assign User1 the Microsoft Defender for Cloud Apps Discovery license.	<input checked="" type="radio"/>	<input type="radio"/>
You can remove the Azure Active Directory Premium P2 license from User1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 is assigned the Azure Active Directory Premium P2.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

YNN

- 1) Y, You can assign users MS Defender for Cloud Apps on a per user basis.
- 2) N, You cannot remove the P2 license as User1 is in Group1.
- 3) N, nested group assignments don't work

Question: 122

CertyIQ

HOTSPOT

-

You have a hybrid deployment of Azure Active Directory (Azure AD) that contains the users shown in the following table.

Name	User type	On-premises sync enabled
User1	Member	No
User2	Member	Yes
User3	Guest	No

You need to modify the JobTitle and UsageLocation attributes for the users.

For which users can you modify the attributes from Azure AD? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

JobTitle:

- User1 only
- User1 and User2 only
- User1 and User3 only
- User1, User2, and User3

UsageLocation:

- User1 only
- User1 and User2 only
- User1 and User3 only
- User1, User2, and User3

Answer:

Answer Area

JobTitle:

- User1 only
- User1 and User2 only
- User1 and User3 only**
- User1, User2, and User3

UsageLocation:

- User1 only
- User1 and User2 only
- User1 and User3 only**
- User1, User2, and User3**

Explanation:

JobTitle :**User1 and User3 only.**

This means only User1 and User3 are associated with the job title, excluding User2.

UsageLocation :**User1, User2, and User3.**

This means all three users (User1, User2, and User3) are associated with the UsageLocation field.

Question: 123

CertyIQ

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 Active Directory (Azure AD) tenant named contoso.com.

You have a CSV file that contains the names and email addresses of 500 external users.

You need to create a guest user account in contoso.com for each of the 500 external users.

Solution: You create a PowerShell script that runs the New-MgUser cmdlet for each external user.

Does this meet the goal?

A.Yes

B.No

Answer: B

Explanation:

New-AzureADMSInvitation or New-MgInvitation can be used to invite users, Not New-MgUser

<https://learn.microsoft.com/en-us/powershell/microsoftgraph/azuread-msoline-cmdlet-map?view=graph-powershell-1.0#users>

Question: 124

CertyIQ

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 Active Directory (Azure AD) tenant named contoso.com.

You have a CSV file that contains the names and email addresses of 500 external users.

You need to create a guest user account in contoso.com for each of the 500 external users.

Solution: You create a PowerShell script that runs the New-MgInvitation cmdlet for each external user.

Does this meet the goal?

A.Yes

B.No

Answer: A

Explanation:

New-AzureADMSInvitation or New-MgInvitation can be used to invite users, Not New-MgUser

<https://learn.microsoft.com/en-us/powershell/microsoftgraph/azuread-msoline-cmdlet-map?view=graph-powershell-1.0#users>

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/bulk-invite-powershell#send-bulk-invitations> describes exactly the same task required by this question, and the proposed script uses New-AzureADMSInvitation cmdlet. But page <https://learn.microsoft.com/en-us/powershell/microsoftgraph/overview?view=graph-powershell-1.0> says: "Microsoft Graph PowerShell is the replacement for the Azure AD PowerShell and MSOnline modules and is recommended for interacting with Azure AD.". By searching the Microsoft Graph PowerShell command equivalent of New-AzureADMSInvitation in this page <https://learn.microsoft.com/en-us/powershell/microsoftgraph/azuread-msoline-cmdlet-map?view=graph-powershell-1.0#users> I find the command New-MgInvitation. So my reply to this question is "A": yes.

CertyIQ**Question: 125**

You have an Azure subscription named Subscription1 that contains virtual network named VNet1. VNet1 is in a resource group named RG1.

A user named User1 has the following roles for Subscription1:

- Reader
- Security Admin
- Security Reader

You need to ensure that User1 can assign the Reader role for VNet1 to other users.

What should you do?

- A. Assign User1 the Contributor role for VNet1.
- B. Assign User1 the Network Contributor role for VNet1.
- C. Assign User1 the User Access Administrator role for VNet1.
- D. Remove User1 from the Security Reader and Reader roles for Subscription1. Assign User1 the Contributor role for Subscription1.

Answer: C**Explanation:**

Network Contributor - Lets you manage networks, but not access to them.<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#network-contributor>
User Access Administrator - Lets you manage user access to Azure resources.<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#user-access-administrator>
Contributor - Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image galleries.
T2Q71 - similar question with another possible solution - Assign User1 the Owner role for VNet1.

CertyIQ**Question: 126**

You have an Azure subscription named Subscription1 that contains virtual network named VNet1. VNet1 is in a resource group named RG1.

User named User1 has the following roles for Subscription1:

- Reader
- Security Admin
- Security Reader

You need to ensure that User1 can assign the Reader role for VNet1 to other users.

What should you do?

- A.Remove User1 from the Security Reader and Reader roles for Subscription1. Assign User1 the Contributor role for Subscription1.
- B.Remove User1 from the Security Reader role for Subscription1. Assign User1 the Contributor role for RG1.
- C.Assign User1 the Network Contributor role for VNet1.
- D.Assign User1 the User Access Administrator role for VNet1.

Answer: D

Explanation:

Network Contributor - Lets you manage networks, but not access to them.<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#network-contributor>
User Access Administrator - Lets you manage user access to Azure resources.<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#user-access-administrator>
Only User Access Administrator or Owner could assign roles to other users.

Question: 127

CertyIQ

HOTSPOT

You have an Azure Storage account named storage1 that uses Azure Blob storage and Azure File storage.

You need to use AzCopy to copy data to the blob storage and file storage in storage1.

Which authentication method should you use for each type of storage? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Blob storage:

- Azure AD only
- Shared access signatures (SAS) only
- Azure AD and shared access signatures (SAS)

File storage:

- Azure AD only
- Shared access signatures (SAS) only
- Azure AD and shared access signatures (SAS)

Answer:

Answer Area

Blob storage:

- Azure AD only
- Shared access signatures (SAS) only
- Azure AD and shared access signatures (SAS)

File storage:

- Azure AD only
- Shared access signatures (SAS) only
- Azure AD and shared access signatures (SAS)

Explanation:

Blob Storage Selection:

The selected option is "Azure AD and shared access signatures (SAS)".

This means both Azure Active Directory (Azure AD) authentication and SAS tokens can be used to access the blob storage.

Azure AD provides identity-based authentication, while SAS tokens provide temporary, delegated access.

File Storage Selection:

The selected option is "Shared access signatures (SAS) only".

This indicates that only SAS tokens can be used to access the file storage, and Azure AD authentication is not enabled for this resource.

Question: 128

CertyIQ

HOTSPOT

You have an Azure AD tenant that contains a user named External User.

External User authenticates to the tenant by using .

You need to ensure that External User authenticates to the tenant by using .

Which two settings should you configure from the Overview blade? To answer, select the appropriate settings in the answer area.

NOTE: Each correct answer is worth one point.

Answer Area

The screenshot shows the Azure portal's 'External User' overview page for a user named 'External User'. The user's principal name is listed as 'external195_gmail.com#EXT#@sk230415outlook.onmicrosoft.com' and they are categorized as a 'Guest'. Key details shown include the user principal name, object ID, creation date/time (Apr 30, 2023, 11:58 AM), user type (Guest), and identities (mail). The 'Manage' sidebar on the left lists various options like custom security attributes, assigned roles, and administrative units. The 'Overview' tab is selected at the top. Below the main details, there are three cards in a grid: 'Account status' (Enabled), 'Sign-ins' (Last sign-in: -- --, See all sign-ins), and 'B2B collaboration' (Invitation state: Accepted, Reset redemption status).

Answer:

Answer Area

The screenshot shows the Azure portal's 'External User' blade. At the top, there's a search bar and several action buttons: 'Edit properties', 'Delete', 'Refresh', 'Reset password', 'Revoke sessions', 'Manage view', and 'Get feedback?'. Below these are tabs for 'Overview', 'Monitoring', and 'Properties', with 'Overview' being the active tab. Under 'Basic info', there's a purple circular profile picture with 'EU' in white, followed by the user name 'External User' and the email address 'external195@gmail.com#EXT#@d270415outlook.onmicrosoft.com'. The 'User principal name' is 'external195@gmail.com#EXT#', 'Object ID' is '2b151249-fa9d-4cfe-b0fd-f6cfc0f0fa1c', 'Created date time' is 'Apr 10, 2023, 11:38 AM', and 'Last sign-in' is 'Never'. To the right of these details are sections for 'Group members', 'Applications', 'Assigned roles', and 'Assigned license'. Below this is a 'My Feed' section with three cards: 'Account status' (Enabled), 'Sign-ins' (Last sign-in: Never, See all sign-ins), and 'B2B collaboration' (highlighted with a red box). On the left side, there's a sidebar with 'Overview', 'Audit logs', 'Sign-in logs', 'Diagnose and solve problems', 'Manage' (with options like 'Custom security attributes (preview)', 'Assigned roles', 'Administrative units', 'Groups', 'Applications', 'Licenses', 'Devices', 'Azure role assignments', and 'Authentication methods'), and 'Troubleshooting + Support'.

Explanation:

Identities Section (Mail)

The Identities field shows "mail", indicating that the user is authenticated using their email identity.

This means the external user is using their email-based authentication (possibly via Microsoft, Google, or another identity provider) to access the organization's resources.

B2B Collaboration

In the bottom right, the tag "B2B collaboration" is visible.

B2B collaboration is a feature in Azure AD that allows organizations to securely share applications and services with users from other organizations.

External users are typically added via guest invitations and can use their existing credentials from their home organization to sign in.

Question: 129

CertyIQ

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

Name	Description
RG1	Resource group
RG2	Resource group
storage1	Storage account in RG1
Workspace1	Azure Synapse Analytics workspace in RG2

You need to assign Workspace1 a role to allow read, write, and delete operations for the data stored in the containers of storage1.

Which role should you assign?

- A.Storage Account Contributor
- B.Contributor
- C.Storage Blob Data Contributor
- D.Reader and Data Access

Answer: C

Explanation:

Storage Blob Data Contributor.

This role specifically grants permissions to read, write, and delete blobs in Azure Storage containers.

It does not allow managing the storage account settings but provides full control over the stored data, which is exactly what is required in the question.

Question: 130

CertyIQ

You have an Azure subscription named Subscription1 that contains virtual network named VNet1. VNet1 is in a resource group named RG1.

A user named User1 has the following roles for Subscription1:

- Reader
- Security Admin
- Security Reader

You need to ensure that User1 can assign the Reader role for VNet1 to other users.

What should you do?

- A.Remove User1 from the Security Reader and Reader roles for Subscription1. Assign User1 the Contributor role for Subscription1.
- B.Assign User1 the Contributor role for VNet1.
- C.Assign User1 the Owner role for VNet1.
- D.Assign User1 the Network Contributor role for RG1.

Answer: C

Explanation:

C. Assign User1 the Owner role for VNet1.

To assign roles in Azure, a user needs to have Owner or User Access Administrator permissions. Currently, User1 has the following roles for Subscription1:

Reader → Can only view resources but cannot assign roles.

Security Admin → Manages security policies but cannot assign roles.

Security Reader → Can view security settings but cannot assign roles.

Since none of these roles provide RBAC (Role-Based Access Control) management permissions, User1 cannot currently assign the Reader role to others for VNet1.

CertyIQ

Question: 131

You have an Azure AD tenant that contains the groups shown in the following table.

Name	Type	Security
Group1	Security	Enabled
Group2	Mail-enabled security	Enabled
Group3	Microsoft 365	Enabled
Group4	Microsoft 365	Disabled

You purchase Azure Active Directory Premium P2 licenses.

To which groups can you assign a license?

- A.Group1 only
- B.Group1 and Group3 only
- C.Group3 and Group4 only
- D.Group1, Group2, and Group3 only
- E.Group1, Group2, Group3, and Group4

Answer: B

Explanation:

B. Group1 and Group3 only.

Azure AD licenses can be assigned to user accounts. When you want to assign licenses to a group, the intention is to assign those licenses to the members of the group.

You can assign licenses to Microsoft 365 groups and security groups, but not to mail-enabled security groups.

Furthermore, the group should be security-enabled to get the licenses assigned.

From the given list:

Group1: Security group (Security Enabled) - You can assign licenses.

Group2: Mail-enabled security group (Security Enabled) - You cannot assign licenses to mail-enabled security groups.

Group3: Microsoft 365 group (Security Enabled) - You can assign licenses.

Group4: Microsoft 365 group (Security Disabled) - You cannot assign licenses to security-disabled groups.

Question: 132

CertyIQ

HOTSPOT

-

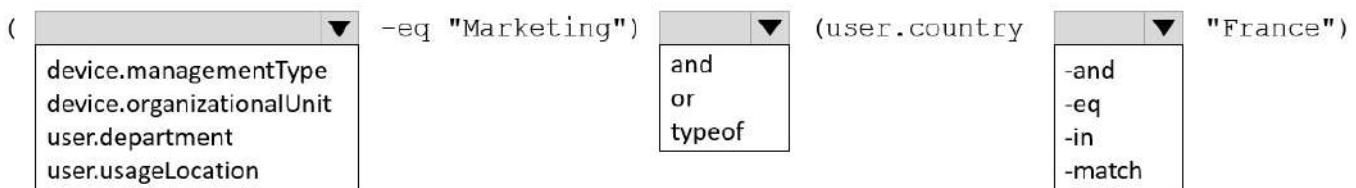
You have an Azure AD tenant.

You need to create a Microsoft 365 group that contains only members of a marketing department in France.

How should you complete the dynamic membership rule? To answer, select the appropriate options in the answer area.

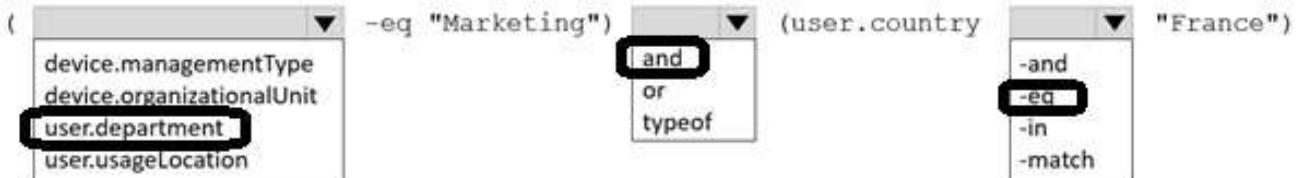
NOTE: Each correct answer is worth one point.

Answer Area



Answer:

Answer Area



Explanation:

First Condition: user.department -

The user.department attribute is checked to see if it equals "Marketing".

This ensures that only users belonging to the Marketing department are considered.

Logical Operator: and

The and operator means both conditions must be true for the rule to apply.

If it were or, only one condition would need to be true.

Second Condition: user.country -eq "France"

The user.country attribute is checked to see if it equals "France".

This ensures that only users located in France are considered.

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership#operator-precedence>

Question: 133

CertyIQ

HOTSPOT

-

You have an Azure AD tenant.

You need to modify the Default user role permissions settings for the tenant. The solution must meet the following requirements:

- Standard users must be prevented from creating new service principals.
- Standard users must only be able to use PowerShell or Microsoft Graph to manage their own Azure resources.

Which two settings should you modify? To answer, select the appropriate settings in the answer area.

NOTE: Each correct answer is worth one point.

Default user role permissions

Learn more 

Users can register applications 	<input checked="" type="checkbox"/> Yes
---	---

Restrict non-admin users from creating tenants 	<input checked="" type="checkbox"/> No
--	--

Users can create security groups 	<input checked="" type="checkbox"/> Yes
--	---

Guest user access

Learn more 

Guest user access restrictions 	<input type="radio"/> Guest users have the same access as members (most inclusive) <input checked="" type="radio"/> Guest users have limited access to properties and memberships of directory objects <input type="radio"/> Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)
--	--

Administration portal

Learn more 

Restrict access to Azure AD administration portal 	<input checked="" type="checkbox"/> No
---	--

LinkedIn account connections

Learn more 

Allow users to connect their work or school account with LinkedIn 	<input checked="" type="radio"/> Yes <input type="radio"/> Selected group <input type="radio"/> No
---	--

Show keep user signed in

Show keep user signed in 	<input checked="" type="checkbox"/> Yes
--	---

Answer:

Default user role permissions

Learn more ⓘ

Users can register applications ⓘ	<input checked="" type="checkbox"/> Yes
Restrict non-admin users from creating tenants ⓘ	<input checked="" type="radio"/> No
Users can create security groups ⓘ	<input checked="" type="checkbox"/> Yes

Guest user access

Learn more ⓘ

Guest user access restrictions ⓘ	<input type="radio"/> Guest users have the same access as members (most inclusive)
	<input checked="" type="radio"/> Guest users have limited access to properties and memberships of directory objects
	<input type="radio"/> Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Administration portal

Learn more ⓘ

Restrict access to Azure AD administration portal ⓘ	<input checked="" type="radio"/> No
---	-------------------------------------

LinkedIn account connections

Learn more ⓘ

Allow users to connect their work or school account with LinkedIn ⓘ *	<input checked="" type="radio"/> Yes
	<input type="radio"/> Selected group
	<input type="radio"/> No

Show keep user signed in

Show keep user signed in ⓘ	<input checked="" type="checkbox"/> Yes
----------------------------	---

Explanation:

1. "Users can register applications" (Enabled - "Yes")

This setting allows regular (non-admin) users to register applications in Azure AD.

If enabled (Yes), users can:

Create and register Azure AD applications.

Generate service principals.

Integrate applications with Azure AD authentication.

Security Concern:

Enabling this could pose security risks if users register applications without oversight.

Organizations may disable this setting (No) to restrict application registration to administrators only.

2. "Restrict access to Azure AD administration portal" (Disabled - "No")

This setting controls whether non-admin users can access the Azure AD admin portal (<https://aad.portal.azure.com>).

If set to "No" (as shown in the image), all users can access the portal but with limited permissions.

If set to "Yes", only administrators can access the Azure AD admin portal.

Implications:

With "No" (Disabled) → Regular users can view limited information in Azure AD but cannot make administrative changes.

With "Yes" (Enabled) → Blocks non-admin users from accessing the portal entirely.

Security Best Practice:

In many organizations, setting this to "Yes" (enabled) restricts access to ensure that only administrators can access Azure AD settings.

Question: 134

CertyIQ

HOTSPOT

You have an Azure subscription named Sub1 that contains the blob containers shown in the following table.

Name	In storage account	Contains blob
cont1	storage1	blob1
cont2	storage2	blob2
cont3	storage3	blob3

Sub1 contains two users named User1 and User2. Both users are assigned the Reader role at the Sub1 scope.

You have a condition named Condition1 as shown in the following exhibit.

```
(  
  (  
    ! (ActionMatches('Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read'))  
  )  
  OR  
  (  
    @Resource[Microsoft.Storage/storageAccounts/blobServices/containers:name] StringEquals 'cont1'  
  )  
)
```

You have a condition named Condition2 as shown in the following exhibit.

```
(  
  (  
    ! (ActionMatches('Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write'))  
  )  
  OR  
  (  
    @Resource[Microsoft.Storage/storageAccounts/blobServices/blobs:path] StringLike '*2*'  
  )  
)
```

You assign roles to User1 and User2 as shown in the following table.

User	Role	Scope	Role assignment condition
User1	Storage Blob Data Reader	sub1	Condition1
User2	Storage Blob Data Owner	storage1	Condition2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can read blob2.	<input type="radio"/>	<input type="radio"/>
User1 can read blob3.	<input type="radio"/>	<input type="radio"/>
User2 can read blob1.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 can read blob2.	<input type="radio"/>	<input checked="" type="checkbox"/>
User1 can read blob3.	<input type="radio"/>	<input checked="" type="checkbox"/>
User2 can read blob1.	<input checked="" type="checkbox"/>	<input type="radio"/>

Explanation:

No

No

Yes

The conditions are difficult to read, but they mean (according to reference 1):

- a. If the user performs a reading operation, then he may only read from "cont1"
- b. If the user performs a writing operation, then he may only write to blobs like "*2*

Given that, then:

- 1- User 1 can read Blob2 - No, because he is reading, then the condition a. applies, and he is not reading cont1
- 2- User 1 can read Blob3 - No, because he is reading, then the condition a. applies, and he is not reading cont1
- 3- User 2 can read blob 1 - Yes. He is not writing, so the condition b. does not apply. He has permissions granted by the role on the scope he is reading - Storage Blob Data Owner on storage1, which contains blob1

References:

1. <https://learn.microsoft.com/en-us/azure/role-based-access-control/conditions-format>
2. <https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

Question: 135

CertyIQ

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 Active Directory (Azure AD) tenant named contoso.com.

You have a CSV file that contains the names and email addresses of 500 external users.

You need to create a guest user account in contoso.com for each of the 500 external users.

Solution: You create a PowerShell script that runs the New-MgUser cmdlet for each user.

Does this meet the goal?

- A.Yes
- B.No

Answer: B

Explanation:

New-Mg Invitation' is the command to add external users to the organization.

Instead use the New-AzureADMSInvitation cmdlet which is used to invite a new external user to your directory.

Reference:

<https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.identity.signins/new-mginvitation?view=graph-powershell-1.0>

Question: 136

CertyIQ

HOTSPOT

-

You purchase a new Azure subscription.

You create an Azure Resource Manager (ARM) template named deploy.json as shown in the following exhibit.

```
1  {
2    "$schema": "https://schema.management.azure.com/schemas/2019-04-
3    "contentVersion": "1.0.0.0",
4    "parameters": {
5      "obj1": {
6        "type": "object",
7        "defaultValue": {
8          "propA": "one",
9          "propB": "two",
10         "propC": "three",
11         "propD": {
12           "propD-1": "sub",
13           "propD-2": "sub"
14         }
15       }
16     },
17     "par1": {
18       "type": "string",
19       "allowedValues": [
20         "centralus",
21         "eastus",
22         "westus" ],
23       "defaultValue": "eastus"
24     }
25   },
26   "variables": {
27     "var1": [
28       "westus",
29       "centraus"
30       "eastus"
31     ]
32   },
33   "resources": [
34     {
35       "type": "Microsoft.Resources/resourceGroups",
36       "apiVersion": "2018-05-01",
37       "location": "eastus",
38       "name": [concat('RGS', copyIndex())]
39       "copy": {
40         "name": "copy",
41         "count": 2
42       }
43     },
44     {
45       "type": "Microsoft.Resources/resourceGroups",
46       "apiVersion": "2018-05-01",
47       "location": [last(variables('var1'))],
48       "name": "[concat('ResGrp', '8')]"
49     },
50     {
51       "type": "Microsoft.Resources/resourceGroups",
52       "apiVersion": "2018-05-01",
53       "location": "[parameters('part1')]",
54       "name": "[concat('RGroup', length(parameters('obj1')))]"
55     }

```

```
56  ],
57  "outputs": {}
58 }
```

You connect to the subscription and run the following command.

```
New-AzDeployment -Location westus -TemplateFile "deploy.json"
```

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Three resource groups are created when you run the script.	<input type="radio"/>	<input type="radio"/>
A resource group named RGroup5 is created.	<input type="radio"/>	<input type="radio"/>
All the resource groups are created in the East US Azure region.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Three resource groups are created when you run the script.	<input type="radio"/>	<input checked="" type="radio"/>
A resource group named RGroup5 is created.	<input type="radio"/>	<input checked="" type="radio"/>
All the resource groups are created in the East US Azure region.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

No

No

Yes

I run the ARM template in a lab environment. Before go to the explanation, it's valid to say that there are some errors in the script format and I have to fix it to run successfully.1- It's N, because it creates 4 Resource Groups and not 3 Resource Groups (RGS0, RGS1, RGroup4 and ResGrp8);1.1: The Resource Group named with "[concat('RGS', copyIndex())]", creates RGS0 and RGS1;1.2: The Resource Group named with "[concat('ResGrp', '8')]", creates ResGrp8;1.3: The Resource Group named with "[concat('RGroup', length(parameters('obj1')))]",

creates RGroup4 (As we can see, obj1 parameter has a length of 4 'propA', 'propB', 'propC' and 'propD');2 - It's N, because it doesn't create a resource group named RGroup5;3 - It's Y, because all resource groups were created in the East US Azure Region.

Question: 137

CertyIQ

Your on-premises network contains a VPN gateway.

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

Name	Type	Description
vgw1	Virtual network gateway	Gateway for Site-to-Site VPN to the on-premises network
storage1	Storage account	Standard performance tier
Vnet1	Virtual network	Enabled forced tunneling
VM1	Virtual machine	Connected to Vnet1

You need to ensure that all the traffic from VM1 to storage1 travels across the Microsoft backbone network.

What should you configure?

- A.Azure AD Application Proxy
- B.private endpoints
- C.a network security group (NSG)
- D.Azure Peering Service

Answer: B

Explanation:

A private endpoint is a network interface that uses a private IP address from your virtual network. This network interface connects you privately and securely to a service that's powered by Azure Private Link. By enabling a private endpoint, you're bringing the service into your virtual network."https://learn.microsoft.com/en-us/azure/private-link/private-endpoint-overview

Question: 138

CertyIQ

Your on-premises network contains a VPN gateway.

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

Name	Type	Description
vgw1	Virtual network gateway	Gateway for Site-to-Site VPN to the on-premises network
storage1	Storage account	Standard performance tier
Vnet1	Virtual network	Enabled forced tunneling
VM1	Virtual machine	Connected to Vnet1

You need to ensure that all the traffic from VM1 to storage1 travels across the Microsoft backbone network.

What should you configure?

- A.Azure AD Application Proxy
- B.service endpoints
- C.a network security group (NSG)
- D.Azure Firewall

Answer: B

Explanation:

"Virtual Network (VNet) service endpoint provides secure and direct connectivity to Azure services over an optimized route over the Azure backbone network.

["https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview"](https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview)

Question: 139

CertyIQ

Your on-premises network contains a VPN gateway.

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

Name	Type	Description
vgw1	Virtual network gateway	Gateway for Site-to-Site VPN to the on-premises network
storage1	Storage account	Standard performance tier
Vnet1	Virtual network	Enabled forced tunneling
VM1	Virtual machine	Connected to Vnet1

You need to ensure that all the traffic from VM1 to storage1 travels across the Microsoft backbone network.

What should you configure?

- A.Azure Application Gateway
- B.service endpoints
- C.a network security group (NSG)
- D.Azure Peering Service

Answer: B

Explanation:

B: service endpoints.

Service endpoints allow you to secure Azure service resources to your virtual network by extending the identity of your VNet to the service. By doing this, the traffic from your virtual machine (VM1) to the storage account (Storage1) remains within the Microsoft backbone network, rather than traversing the public internet. This ensures secure and fast traffic between your VM and storage account.

Question: 140

CertyIQ

You have an Azure subscription named Sub1 that contains the resources shown in the following table.

Name	Type
MG1	Management group
RG1	Resource group
VM1	Virtual machine

You create a user named Admin1.

To what can you add Admin1 as a co-administrator?

- A.RG1
- B.MG1
- C.Sub1
- D.VM1

Answer: C

Explanation:

The correct answer is: C. Sub1 You can add Admin1 as a co-administrator to the Sub1 subscription. You cannot add Admin1 as a co-administrator to the RG1 resource group, MG1 management group, or VM1 virtual machine. Co-administrators have full access to all resources in a subscription, including the ability to create, read, update, and delete resources. To add Admin1 as a co-administrator to Sub1: In the Azure portal, navigate to Sub1. Click Access control (IAM). Click Assign role. Select the Co-Administrator role. Select Admin1 in the Select drop-down list. Click Assign. Once the role has been assigned, Admin1 will have full access to all resources in Sub1. Note: Co-administrators can only be assigned at the subscription scope. You cannot assign co-administrators to resource groups, management groups, or virtual machines.

Question: 141

CertyIQ

HOTSPOT

-

You have a Microsoft Entra tenant that contains the groups shown in the following table.

Name	Type	Has an assigned license
Group1	Security	Yes
Group2	Security	No
Group3	Microsoft 365	Yes
Group4	Microsoft 365	No

The tenant contains the users shown in the following table.

Name	Member of	Has a direct assigned license
User1	None	Yes
User2	Group1	No
User3	Group4	Yes
User4	None	No

Which users and groups can you delete? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Users:

- User4 only
- User1 and User4 only
- User2 and User4 only
- User1, User2, User3, and User4

Groups:

- Group2 only
- Group2 and Group3 only
- Group2 and Group4 only
- Group1, Group2, Group3, and Group4

Answer:

Answer Area

Users:

- User4 only
- User1 and User4 only
- User2 and User4 only
- User1, User2, User3, and User4

Groups:

- Group2 only
- Group2 and Group3 only
- Group2 and Group4 only
- Group1, Group2, Group3, and Group4

Explanation:

Users = User1, User2, User3, User4 (can delete all users whether a license is assigned directly or via inheritance from a group membership)

Groups = Group 2 and Group 4 only. (Groups with active license assignments cannot be deleted. You get an error)

Question: 142

CertyIQ

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

Name	Type	Location
VM1	Virtual machine	East US
storage1	Storage account	West US

You need to ensure that data transfers between storage1 and VM1 do NOT traverse the internet

What should you configure for storage1?

- A.data protection
- B.a private endpoint
- C.Public network access in the Firewalls and virtual networks settings

D.a shared access signature (SAS)

Answer: B

Explanation:

B:a private endpoint.

To ensure that all the traffic from VM1 to storage1 travels across the Microsoft backbone network without going out to the public internet, you should use a private endpoint.

A private endpoint uses a private IP address from your VNet, effectively bringing the service into your VNet. Any traffic between your virtual machine and the storage account will traverse over the VNet and stay on the Microsoft backbone network, without ever leaving it.

Reference:

<https://learn.microsoft.com/en-us/azure/storage/common/storage-private-endpoints>

Question: 143

CertyIQ

HOTSPOT

You have a Microsoft Entra tenant that is linked to the subscriptions shown in the following table.

Name	Management group	Parent management group
Sub1	Tenant Root Group	<i>Not applicable</i>
Sub2	MG1	Tenant Root Group
Sub3	MG2	Tenant Root Group

You have the resource groups shown in the following table.

Name	Subscription	Description
RG1	Sub1	Contains a storage account named storage1
RG2	Sub2	Contains a web app named App1
RG3	Sub3	Contains a virtual machine named VM1

You assign roles to users as shown in the following table.

User	Role	Scope
User1	Contributor	MG2
User2	Storage Account Contributor	storage1
User3	User Access Administrator	Tenant Root Group

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can resize VM1.	<input type="radio"/>	<input type="radio"/>
User2 can create a new storage account in RG1.	<input type="radio"/>	<input type="radio"/>
User3 can assign User1 the Owner role for RG3.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 can resize VM1.	<input checked="" type="checkbox"/>	<input type="radio"/>
User2 can create a new storage account in RG1.	<input type="radio"/>	<input checked="" type="checkbox"/>
User3 can assign User1 the Owner role for RG3.	<input checked="" type="checkbox"/>	<input type="radio"/>

Explanation:

YES: user 1 is contributor to the scope MG2, which is linked to sub3 and contains RG3 and VM1. contributor role can resize vm in its scope.

NO: User2 is storage account contributor to the storage1 scope only not RG1.

YES: User3 is user access admin to the scope tenant root group that contains all the subscriptions and therefore sub3 that contains RG3, so he can assign roles to any users and to user1.

Question: 144

CertyIQ

Your on-premises network contains a VPN gateway.

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

Name	Type	Description
vgw1	Virtual network gateway	Gateway for Site-to-Site VPN to the on-premises network
storage1	Storage account	Standard performance tier
Vnet1	Virtual network	Enabled forced tunneling
VM1	Virtual machine	Connected to Vnet1

You need to ensure that all the traffic from VM1 to storage1 travels across the Microsoft backbone network.

What should you configure?

- A.a network security group (NSG)
- B.private endpoints
- C.Microsoft Entra Application Proxy
- D.Azure Virtual WAN

Answer: B

Explanation:

B: private endpoints.

Private endpoints enable you to connect to Azure services privately over a private IP address within your virtual network. By setting up a private endpoint for your storage account (Storage1), all traffic from VM1 to the storage account will travel through the private IP address within the Azure network, ensuring that the traffic remains on the Microsoft backbone network and does not traverse the public internet.

Question: 145

CertyIQ

You have a Microsoft Entra tenant.

You plan to perform a bulk import of users.

You need to ensure that imported user objects are added automatically as the members of a specific group based on each user's department. The solution must minimize 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.Create groups that use the Assigned membership type.
- B.Create an Azure Resource Manager (ARM) template.
- C.Create groups that use the Dynamic User membership type.
- D.Write a PowerShell script that parses an import file.
- E.Create an XML file that contains user information and the appropriate attributes.
- F.Create a CSV file that contains user information and the appropriate attributes.

Answer: CF

Explanation:

C: Create groups that use the Dynamic User membership type.

Dynamic groups automatically add and remove members based on user attributes, such as department, without any manual intervention.

By setting up dynamic membership rules based on department attributes, you can ensure that users are automatically added to the appropriate group upon import.

F: Create a CSV file that contains user information and the appropriate attributes.

CSV files are commonly used for bulk importing user data into Microsoft Entra (formerly known as Azure AD).

You can specify attributes like department in the CSV file, ensuring that the imported users have the necessary information for dynamic group membership.

Question: 146

CertyIQ

You have an Azure subscription that contains a storage account named storage1.

You need to ensure that the access keys for storage1 rotate automatically.

What should you configure?

- A.a backup vault
- B.redundancy for storage1
- C.lifecycle management for storage1
- D.an Azure key vault
- E.a Recovery Services vault

Answer: D**Explanation:**

D: Use Azure Key Vault for Key ManagementAzure Key Vault is a service that helps manage secrets, keys, and certificates. You can store and manage your storage account keys securely in Key Vault and use its features to automate key rotation.

Question: 147

CertyIQ

You have an Azure subscription that contains the Microsoft Entra identities shown in the following table.

Name	Type
User1	User
Group1	Security group
Group2	Microsoft 365 group

You need to enable self-service password reset (SSPR).

For which identities can you enable SSPR in the Azure portal?

- A.User1 only
- B.Group1 only
- C.User1 and Group1 only
- D.Group1 and Group2 only
- E.User1, Group1, and Group2

Answer: D**Explanation:**

Group1 and Group2: These groups can be configured with SSPR settings. By enabling SSPR for these groups, all members within the groups will have the ability to reset their passwords.

Question: 148

CertyIQ

DRAG DROP -

You have a Microsoft Entra tenant.

You need to ensure that when a new Microsoft 365 group is created, the group name is automatically formatted as follows:

<Department><Group name>

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

Actions**Answer Area**Set Add suffix to **Attribute**.

Create a group naming policy.

Set Add prefix to **Attribute**.Set Add suffix to **String**.Set Add prefix to **String**.Set Select type to **Department**.

Customize the company branding.

**Answer:****Answer Area**

Create a group naming policy.

Set Add prefix to **Attribute**.Set Select type to **Department**.**Explanation:**

- 1- Create a group naming policy: This is the first step to establish the framework for naming groups.
- 2- Set Add prefix to Attribute: This step specifies that the prefix will be an attribute rather than a static string.
- 3- Set Select type to Department: Finally, you specify that the 'Department' attribute will be used as the prefix.

Question: 149

CertyIQ

HOTSPOT

-

You have a Microsoft Entra tenant that contains the users shown in the following table.

Name	Member of	Assigned license
User1	Group1	Microsoft Entra ID P2
User2	Group2	None
User3	None	Microsoft Entra ID P2
User4	None	None

The tenant contains the groups shown in the following table.

Name	Member of	Assigned license
Group1	None	None
Group2	Group3	Microsoft Entra ID P2
Group3	Group4	None
Group4	None	Microsoft Entra ID P2

Which users and groups can be deleted? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Users:

- User4 only
- User3 and User4 only
- User2 and User4 only
- User1, User2, User3, and User4

Groups:

- Group1 only
- Group4 only
- Group1 and Group3 only
- Group1, Group2, Group3, and Group4

Answer:

Answer Area

Users:

- User4 only
- User3 and User4 only
- User2 and User4 only
- User1, User2, User3, and User4**

Groups:

- Group1 only
- Group4 only
- Group1 and Group3 only**
- Group1, Group2, Group3, and Group4

Explanation:

Users: "User1, User2, User3, and User4"

This selection implies that all four users are included in the specified operation (e.g., assignment, permission, access control).

This might be relevant in scenarios where multiple users need permissions or access in a system like Microsoft Entra ID (Azure AD).

Groups: "Group1 and Group3 only"

This selection indicates that the chosen operation applies only to Group1 and Group3.

Other groups (e.g., Group2, Group4) are not included in this selection.

This is useful in cases like role assignments, access policies, or security group filtering.

Question: 150

CertyIQ

HOTSPOT

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

Name	Resource group	Type	Location
app1	RG1	Container app	East US
Vault1	RG1	Azure Key Vault	East US
Vault2	RG1	Azure Key Vault	West US
Vault3	RG2	Azure Key Vault	East US

You plan to use an Azure key vault to provide a secret to app1.

What should you create for app1 to access the key vault, and from which key vault can the secret be used? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Create a:

Managed identity
Private endpoint
Service principal
User account

Use the secret from:

Vault1 only
Vault1 and Vault2 only
Vault1 and Vault3 only
Vault1, Vault2, or Vault3

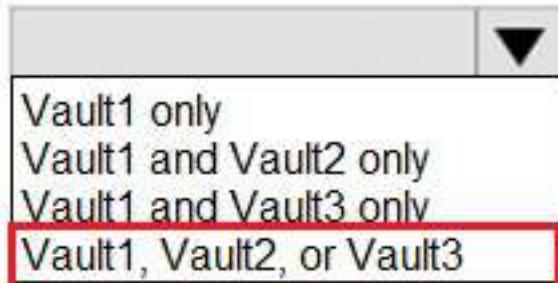
Answer:

Answer Area

Create a:



Use the secret from:



Explanation:

Create a: "Managed identity"

A Managed Identity is an Azure feature that provides an automatically managed identity in Azure Active Directory (Azure AD) for applications to use when connecting to resources.

It eliminates the need to manually manage credentials, improving security.

Use the secret from: "Vault1, Vault2, or Vault3"

This implies that the system or service has access to secrets stored in multiple Azure Key Vaults (Vault1, Vault2, or Vault3).

Azure Key Vault is a cloud service for securely storing and accessing secrets, such as API keys, passwords, and certificates.

Question: 151

CertyIQ

You have a Microsoft Entra tenant named contoso.com.

You collaborate with an external partner named fabrikam.com.

You plan to invite users in fabrikam.com to the contoso.com tenant.

You need to ensure that invitations can be sent only to fabrikam.com users.

What should you do in the Microsoft Entra admin center?

- A.From Cross-tenant access settings, configure the Tenant restrictions settings.
- B.From Cross-tenant access settings, configure the Microsoft cloud settings.
- C.From External collaboration settings, configure the Guest user access restrictions settings.
- D.From External collaboration settings, configure the Collaboration restrictions settings.

Answer: D

Explanation:

D: From External collaboration settings, configure the Collaboration restrictions settings.

In Microsoft Entra (formerly known as Azure AD), if you want to restrict invitations to users from a specific external domain, you need to configure collaboration restrictions. Here's how:

Collaboration restrictions settings: These settings allow you to specify which external domains can be invited as guests to your directory. By setting up these restrictions, you can ensure that only users from fabrikam.com can receive invitations to your contoso.com tenant.

Question: 152

CertyIQ

You have an Azure subscription that contains a storage account named storage1. The storage1 account contains blob data.

You need to assign a role to a user named User1 to ensure that the user can access the blob data in storage1. The role assignment must support conditions.

Which two roles can you assign to User1? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A.Owner
- B.Storage Account Contributor
- C.Storage Account Backup Contributor
- D.Storage Blob Data Contributor
- E.Storage Blob Data Owner
- F.Storage Blob Delegator

Answer: DE

Explanation:

D. Storage Blob Data Contributor.

This role allows the user to read, write, and delete blob data. It supports conditions, which means you can use Azure Role-Based Access Control (RBAC) to set conditions on the role assignment if necessary.

E. Storage Blob Data Owner.

This role allows the user to manage blob data including reading, writing, and deleting, and also managing the blob container and data. It supports conditions, making it possible to apply RBAC conditions on the role assignment.

Question: 153

CertyIQ

HOTSPOT

-

Case study

-

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

- To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

ADatum Corporation is consulting firm that has a main office in Montreal and branch offices in Seattle and New York.

Existing Environment

Azure Environment

ADatum has an Azure subscription that contains three resource groups named RG1, RG2, and RG3.

The subscription contains the storage accounts shown in the following table.

Name	Kind	Location	Hierarchical namespace	Container	File share
storage1	StorageV2	West US	Yes	cont1	share1
storage2	StorageV2	West US	No	cont2	share2

The subscription contains the virtual machines shown in the following table.

Name	Size	Operating system	Description
VM1	A	Red Hat Enterprise Linux (RHEL)	Uses ephemeral OS disks
VM2	D	Windows Server 2022	Has a basic volume
VM3	B	Red Hat Enterprise Linux (RHEL)	Uses a standard SSDs
VM4	M	Windows Server 2022	Uses Write Accelerator disks
VM5	E	Windows Server 2022	Has a dynamic volume

The subscription has an Azure container registry that contains the images shown in the following table.

Name	Operating system
Image1	Windows Server
Image2	Linux

The subscription contains the resources shown in the following table.

Name	Description	In resource group
Workspace1	Log Analytics workspace	RG1
WebApp1	Azure App Service web app	RG1
VNet1	Virtual network	RG2
zone1.com	Azure Private DNS zone	RG3

Azure Key Vault

The subscription contains an Azure key vault named Vault1.

Vault1 contains the certificates shown in the following table.

Name	Content type	Key type	Key size
Cert1	PKCS#12	RSA	2048
Cert2	PKCS#12	RSA	4096
Cert3	PEM	RSA	2048
Cert4	PEM	RSA	4096

Vault1 contains the keys shown in the following table.

Name	Type	Description
Key1	RSA	Has a key size of 4096
Key2	EC	Has Elliptic curve name set to P-256

Microsoft Entra Environment

ADatum has a Microsoft Entra tenant named adatum.com that is linked to the Azure subscription and contains the users shown in the following table.

Name	Microsoft Entra role	Azure role
Admin1	Global Administrator	<i>None</i>
Admin2	Attribute Definition Administrator	<i>None</i>
Admin3	Attribute Assignment Administrator	<i>None</i>
User1	<i>None</i>	Reader for RG2 and RG3

The tenant contains the groups shown in the following table.

Name	Type
Group1	Security group
Group2	Microsoft 365 group

The adatum.com tenant has a custom security attribute named Attribute1.

Planned Changes

ADatum plans to implement the following changes:

- Configure a data collection rule (DCR) named DCR1 to collect only system events that have an event ID of 4648 from VM2 and VM4.
- In storage1, create a new container named cont2 that has the following access policies:
 - Three stored access policies named Stored1, Stored2, and Stored3
 - A legal hold for immutable blob storage
- Whenever possible, use directories to organize storage account content.
- Grant User1 the permissions required to link Zone1 to VNet1.
- Assign Attribute1 to supported adatum.com resources.
- In storage2, create an encryption scope named Scope1.
- Deploy new containers by using Image1 or Image2.

Technical Requirements

-

ADatum must meet the following technical requirements:

- Use TLS for WebApp1.
- Follow the principle of least privilege.
- Grant permissions at the required scope only.
- Ensure that Scope1 is used to encrypt storage services.
- Use Azure Backup to back up cont1 and share1 as frequently as possible.
- Whenever possible, use Azure Disk Encryption and a key encryption key (KEK) to encrypt the virtual machines.

You need to implement the planned change for Attribute1.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Admin1 can assign Attribute1 to Group1.	<input type="radio"/>	<input type="radio"/>
Admin2 can assign Attribute1 to User1.	<input type="radio"/>	<input type="radio"/>
Admin3 can assign Attribute1 to Group2.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Admin1 can assign Attribute1 to Group1.	<input type="radio"/>	<input checked="" type="checkbox"/>
Admin2 can assign Attribute1 to User1.	<input type="radio"/>	<input checked="" type="checkbox"/>
Admin3 can assign Attribute1 to Group2.	<input type="radio"/>	<input checked="" type="checkbox"/>

Explanation:

Admin1 (Global Admin) can assign Attribute1 to Group1: No

Global Administrators do not have permissions to read, define, or assign custom security attributes by default.

Admin2 (Attribute Definition Admin) can assign Attribute1 to User1: No

The Attribute Definition Admin role can define and manage attribute definitions but cannot assign attributes to users or groups.

Admin3 (Attribute Assignment Admin) can assign Attribute1 to Group2: No

Question: 154

CertyIQ

You have a Microsoft Entra tenant configured as shown in the following exhibit.



Default Directory | Overview

...



Microsoft Entra ID

+ Add ▾



Manage tenants



What's new



Preview features

...



Azure Active Directory is now Microsoft Entra ID. [Learn more](#)

Overview

Monitoring

Properties

Recommendations

Tutorials



Search your tenant

Basic information

Name Default Directory

Tenant ID c4d2baba-3de9-4dbe-abdb-2892387a97dd

Primary domain sk230128outlook.onmicrosoft.com

License Microsoft Entra ID Free

The tenant contains the identities shown in the following table.

Name	Type
User1	User account
Group1	Security group
Group2	Microsoft 365 group

You purchase a Microsoft Fabric license.

To which identities can you assign the license?

- A.User1 only
- B.User1 and Group1 only
- C.User1 and Group2 only
- D.User1, Group1, and Group2

Answer: A

Explanation:

A: User1 only.

Microsoft Fabric licenses are assigned to individual user accounts, not to groups. When you purchase a Microsoft Fabric license, you can assign it directly to a specific user, like User1, who will then have access to

the services provided by the license.

Question: 155

CertyIQ

You have an Azure subscription that contains a storage account named storage. The storage account contains a blob that stores images.

Client access to storage1 is granted by using a shared access signature (SAS).

You need to ensure that users receive a warning message when they generate a SAS that exceeds a seven-day time period.

What should you do for storage?

- A.Enable a read-only lock.
- B.Configure an alert rule.
- C.Add a lifecycle management rule.
- D.Set Allow recommended upper limit for shared access signature (SAS) expiry interval to Enabled.

Answer: D

Explanation:

D: Set Allow recommended upper limit for shared access signature (SAS) expiry interval to Enabled.

Azure allows you to configure a recommended upper limit for the expiry interval of shared access signatures (SAS) for storage accounts. By setting this option to "Enabled," you can specify the maximum period a SAS token can be valid for, such as seven days. When users attempt to generate a SAS that exceeds this limit, they will receive a warning message.

Question: 156

CertyIQ

You have an Azure subscription named Subscription1 that contains the storage accounts shown in the following table:

Name	Account kind	Azure service that contains data
storage1	Storage	File
storage2	StorageV2 (general purpose v2)	File, Table
storage3	StorageV2 (general purpose v2)	Queue
storage4	BlobStorage	Blob

You plan to use the Azure Import/Export service to export data from Subscription1.

You need to identify which storage account can be used to export the data.

What should you identify?

- A. storage1
- B. storage2
- C. storage3

D. storage4

Answer: D

Explanation:

Azure Import/Export service supports the following of storage accounts:

- ⇒ Standard General Purpose v2 storage accounts (recommended for most scenarios)
 - ⇒ Blob Storage accounts
 - ⇒ General Purpose v1 storage accounts (both Classic or Azure Resource Manager deployments),
- Azure Import/Export service supports the following storage types:
- ⇒ Import supports Azure Blob storage and Azure File storage
 - ⇒ Export supports Azure Blob storage

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-requirements>

Question: 157

CertyIQ

HOTSPOT -

You have Azure Storage accounts as shown in the following exhibit.

The screenshot shows the Azure Storage accounts blade. At the top, there are buttons for 'Add', 'Edit columns', 'Refresh', 'Assign Tags', and 'Delete'. Below that is a filter bar with dropdowns for 'Subscription' (All 2 selected), 'Filter by home...', 'All subscriptions', 'All resource groups', 'All types', 'All locations', and 'No grouping'. A table below lists '3 items':

NAME	TYPE	KIND	RESOURCE...	LOCATION	SUBSCRIPTION	ACCESS T...	REPLICAT...
storageaccount1	Storage account	Storage	ContosoRG1	East US	Subscription 1	-	Read-access ge...
storageaccount2	Storage account	StorageV2	ContosoRG1	Central US	Subscription 1	Hot	Geo-redundant...
storageaccount3	Storage account	BlobStorage	ContosoRG1	East US	Subscription 1	Hot	Locally-redundant...

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

You can use [answer choice] for Azure Table Storage.

storageaccount1 only
storageaccount2 only
storageaccount3 only
storageaccount1 and storageaccount2 only
storageaccount2 and storageaccount3 only

You can use [answer choice] for Azure Blob storage.

storageaccount3 only
storageaccount2 and storageaccount3 only
storageaccount1 and storageaccount3 only
all the storage accounts

Answer:

Answer Area

You can use [answer choice] for Azure Table Storage.

storageaccount1 only
storageaccount2 only
storageaccount3 only
storageaccount1 and storageaccount2 only
storageaccount2 and storageaccount3 only

You can use [answer choice] for Azure Blob storage.

storageaccount3 only
storageaccount2 and storageaccount3 only
storageaccount1 and storageaccount3 only
all the storage accounts

Explanation:

Box 1: storageaccount1 and storageaccount2 only

Box 2: All the storage accounts .

Note: The three different storage account options are: General-purpose v2 (GPv2) accounts, General-purpose v1 (GPv1) accounts, and Blob storage accounts.

- ⇒ General-purpose v2 (GPv2) accounts are storage accounts that support all of the latest features for blobs, files, queues, and tables.
- ⇒ Blob storage accounts support all the same block blob features as GPv2, but are limited to supporting only block blobs.
- ⇒ General-purpose v1 (GPv1) accounts provide access to all Azure Storage services, but may not have the latest features or the lowest per gigabyte pricing.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-account-options>

Question: 158

CertyIQ

You have Azure subscription that includes data in following locations:

Name	Type
container1	Blob container
share1	Azure files share
DB1	SQL database
Table1	Azure Table

You plan to export data by using Azure import/export job named Export1.

You need to identify the data that can be exported by using Export1.

Which data should you identify?

- A. DB1
- B. container1
- C. share1
- D. Table1

Answer: B

Explanation:

B. container1

The following list of storage types is supported with Azure Import/Export service.

Export: Azure Blob Storage -> Block blobs, Page blobs, and Append blobs supported.

Azure Files not supported & Export from archive tier not supported

Reference:

<https://docs.microsoft.com/en-us/azure/import-export/storage-import-export-requirements#supported-storage-types>

Question: 159

CertyIQ

HOTSPOT -

You have an Azure Storage account named storage1.

You have an Azure App Service app named App1 and an app named App2 that runs in an Azure container instance. Each app uses a managed identity.

You need to ensure that App1 and App2 can read blobs from storage1. The solution must meet the following requirements:

- ⇒ Minimize the number of secrets used.
- ⇒ Ensure that App2 can only read from storage1 for the next 30 days.

What should you configure in storage1 for each app? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

App1:

Access keys
Advanced security
Access control (IAM)
Shared access signatures (SAS)

App2:

Access keys
Advanced security
Access control (IAM)
Shared access signatures (SAS)

Answer:

Answer Area

App1:

Access keys
Advanced security
Access control (IAM)
Shared access signatures (SAS)

App2:

Access keys
Advanced security
Access control (IAM)
Shared access signatures (SAS)

Explanation:

Box 1: Access Control (IAM)

Since the App1 uses Managed Identity, App1 can access the Storage Account via IAM. As per requirement, we need to minimize the number of secrets used, so Access keys is not ideal.

Box 2: Shared access signatures (SAS)

We need temp access for App2, so we need to use SAS.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-auth>

Question: 160

CertyIQ

HOTSPOT -

You need to create an Azure Storage account that meets the following requirements:

- ⇒ Minimizes costs
- ⇒ Supports hot, cool, and archive blob tiers
- ⇒ Provides fault tolerance if a disaster affects the Azure region where the account resides

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
az storage account create -g RG1 -n storageaccount1
```

--kind

FileStorage
Storage
StorageV2

--sku

Standard_GRS
Standard_LRS
Standard_RAGRS
Premium_LRS

Answer:

Answer Area

```
az storage account create -g RG1 -n storageaccount1
```

--kind

FileStorage
Storage
StorageV2

--sku

Standard_GRS
Standard_LRS
Standard_RAGRS
Premium_LRS

Explanation:

Box 1: StorageV2 -

You may only tier your object storage data to hot, cool, or archive in Blob storage and General Purpose v2 (GPv2) accounts. General Purpose v1 (GPv1) accounts do not support tiering.

General-purpose v2 accounts deliver the lowest per-gigabyte capacity prices for Azure Storage, as well as industry-competitive transaction prices.

Box 2: Standard_GRS -

Geo-redundant storage (GRS): Cross-regional replication to protect against region-wide unavailability.

Incorrect Answers:

Locally-redundant storage (LRS): A simple, low-cost replication strategy. Data is replicated within a single storage scale unit.

Read-access geo-redundant storage (RA-GRS): Cross-regional replication with read access to the replica. RA-GRS provides read-only access to the data in the secondary location, in addition to geo-replication across two regions, but is more expensive compared to GRS.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy-grs> <https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers>

Question: 161**CertyIQ**

You have an Azure subscription that contains the resources in the following table.

Name	Type
RG1	Resource group
store1	Azure Storage account
Sync1	Azure File Sync

Store1 contains a file share named data. Data contains 5,000 files.

You need to synchronize the files in the file share named data to an on-premises server named Server1.

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

NOTE: Each correct selection is worth one point.

- A. Create a container instance
- B. Register Server1
- C. Install the Azure File Sync agent on Server1
- D. Download an automation script
- E. Create a sync group

Answer: BCE**Explanation:**

Step 1 (C): Install the Azure File Sync agent on Server1

The Azure File Sync agent is a downloadable package that enables Windows Server to be synced with an Azure file share

Step 2 (B): Register Server1.

Register Windows Server with Storage Sync Service

Registering your Windows Server with a Storage Sync Service establishes a trust relationship between your server (or cluster) and the Storage Sync Service.

Step 3 (E): Create a sync group and a cloud endpoint.

A sync group defines the sync topology for a set of files. Endpoints within a sync group are kept in sync with each other. A sync group must contain one cloud endpoint, which represents an Azure file share and one or more server endpoints. A server endpoint represents a path on registered server.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-deployment-guide>

Question: 162

HOTSPOT -

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

Name	Type	Resource group
VNET1	Virtual network	RG1
VNET2	Virtual network	RG2
VM1	Virtual machine	RG2

The status of VM1 is Running.

You assign an Azure policy as shown in the exhibit. (Click the Exhibit tab.)

Home > Policy - Assignments > Assign Policy

Assign Policy

SCOPE

* Scope (Learn more about setting the scope)
Azure Pass/RG2

Exclusions
Optionally select resources to exempt from the policy assignment

BASICS

* Policy definition
Not allowed resource types

* Assignment name ⓘ
Not allowed resource types

Description

Assigned by
First User

PARAMETERS

* Not allowed resource types ⓘ
3 selected

Assign **Cancel**

You assign the policy by using the following parameters:

Microsoft.ClassicNetwork/virtualNetworks

Microsoft.Network/virtualNetworks

Microsoft.Compute/virtualMachines

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
An administrator can move VNET1 to RG2	<input type="radio"/>	<input type="radio"/>
The state of VM1 changed to deallocated	<input type="radio"/>	<input type="radio"/>
An administrator can modify the address space of VNET2	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
An administrator can move VNET1 to RG2	<input checked="" type="radio"/>	<input type="radio"/>
The state of VM1 changed to deallocated	<input type="radio"/>	<input checked="" type="radio"/>
An administrator can modify the address space of VNET2	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

1. An administrator can move VNET1 to RG2 : Yes.

Virtual Networks (VNETs) in Azure can be moved from one Resource Group (RG) to another, provided that:

The move follows Azure's resource move constraints.

The administrator has sufficient permissions (like Owner or Contributor).

There are no dependencies preventing the move.

Since "Yes" is selected, this indicates that the move is possible.

2. The state of VM1 changed to deallocated : No.

A Virtual Machine (VM) in Azure enters a deallocated state when:

It is explicitly stopped using Azure PowerShell, CLI, or Portal.

It is not assigned to a running resource group.

If "No" is selected, it implies that:

The VM has not been deallocated.

It might still be in a stopped (but allocated) state.

It could still be consuming resources, meaning billing continues.

3. An administrator can modify the address space of VNET2:**No**

In Azure Virtual Networks (VNets):

The address space can be modified only if there are no subnet dependencies.

If subnets already exist and are in use, modifying the address space is restricted.

Since "No" is selected, it suggests that:

The VNET has existing subnets or dependencies preventing modifications.

The administrator cannot change the address space directly.

CertyIQ

Question: 163

DRAG DROP -

You have an Azure subscription that contains a storage account.

You have an on-premises server named Server1 that runs Windows Server 2016. Server1 has 2 TB of data.

You need to transfer the data to the storage account by using the Azure Import/Export service.

In which order should you perform the actions? To answer, move all 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

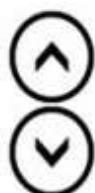
From the Azure portal, update the import job

From the Azure portal, create an import job

Attach an external disk to Server1 and then run waimportexport.exe

Detach the external disks from Server1 and ship the disks to an Azure data center

Answer Area



Answer:

Actions

From the Azure portal, update the import job

From the Azure portal, create an import job

Attach an external disk to Server1 and then run waimportexport.exe

Detach the external disks from Server1 and ship the disks to an Azure data center

Answer Area

Attach an external disk to Server1 and then run waimportexport.exe

From the Azure portal, create an import job

Detach the external disks from Server1 and ship the disks to an Azure data center



Explanation:

At a high level, an import job involves the following steps:

Step 1: Attach an external disk to Server1 and then run waimportexport.exe

Determine data to be imported, number of drives you need, destination blob location for your data in Azure storage.

Use the WALimportExport tool to copy data to disk drives. Encrypt the disk drives with BitLocker.

Step 2: From the Azure portal, create an import job.

Create an import job in your target storage account in Azure portal. Upload the drive journal files.

Step 3: Detach the external disks from Server1 and ship the disks to an Azure data center.

Provide the return address and carrier account number for shipping the drives back to you.

Ship the disk drives to the shipping address provided during job creation.

Step 4: From the Azure portal, update the import job

Update the delivery tracking number in the import job details and submit the import job.

The drives are received and processed at the Azure data center.

The drives are shipped using your carrier account to the return address provided in the import job.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-service>

Question: 164

CertyIQ

HOTSPOT -

You have Azure subscription that includes following Azure file shares:

Name	In storage account	Location
share1	storage1	West US
share2	storage1	West US

You have the following on-premises servers:

Name	Folders
Server1	D:\Folder1, E:\Folder2
Server2	D:\Data

You create a Storage Sync Service named Sync1 and an Azure File Sync group named Group1. Group1 uses share1 as a cloud endpoint.

You register Server1 and Server2 in Sync1. You add D:\Folder1 on Server1 as a server endpoint of Group1.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
share2 can be added as a cloud endpoint for Group1	<input type="radio"/>	<input type="radio"/>
E:\Folder2 on Server1 can be added as a server endpoint for Group1	<input type="radio"/>	<input type="radio"/>
D:\Data on Server2 can be added as a server endpoint for Group1	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
share2 can be added as a cloud endpoint for Group1	<input type="radio"/>	<input checked="" type="radio"/>
E:\Folder2 on Server1 can be added as a server endpoint for Group1	<input type="radio"/>	<input checked="" type="radio"/>
D:\Data on Server2 can be added as a server endpoint for Group1	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Box1: No.

An Azure file synchronization group can only have one cloud endpoint. Group1 uses share1 as a cloud endpoint.

Box2: No.

An Azure file synchronization group can have multiple server endpoints and a single server can be a member of multiple file synchronization groups within a single storage synchronization service. However, a single server can only have a single endpoint in a single file synchronization group. Server1 already has an endpoint in Group1. We cannot add a second folder path from Server1 as a server endpoint to Group1.

Box3: yes.

Server2 is registered in Sync1 and does not yet have an endpoint in Group1. We can include the D:\Data folder in the Group1 file synchronization group.

The following Technet article contains more information on the subject:

<https://docs.microsoft.com/en-us/azure/storage/file-sync/file-sync-deployment-guide?tabs=azure-portal%2Cproactive-portal>

Reference:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-deployment-guide>

Question: 165

CertyIQ

DRAG DROP -

You have an Azure subscription named Subscription1.

You create an Azure Storage account named contosostorage, and then you create a file share named data.

Which UNC path should you include in a script that references files from the data file share? To answer, drag the appropriate values to the correct targets. Each value may be used once, more than once or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Values

blob	blob.core.windows.net
contosostorage	data
file	file.core.windows.net
portal.azure.com	subscription1

Answer Area

\ \ [] , [] \ []

Answer:**Values**

blob	blob.core.windows.net
contosostorage	data
file	file.core.windows.net
portal.azure.com	subscription1

Answer Area

\ \ [contosostorage] , [file.core.windows.net] \ [data]

Explanation:

Box 1: contosostorage -

The name of account -

Box 2: file.core.windows.net -

Box 3: data -

The name of the file share is data.

Example:

The screenshot shows a 'Connect' dialog box for a file share named 'myazurefileshare'. Below it, a 'Connecting from Windows' section provides instructions to run a command to connect from a Windows computer. A code block shows the command:

```
> net use [drive letter]
\\myazurefileaccount.file.core.windows.net\myazurefiles
/u:AZURE\myazurefileaccount
mehLWRwJkxS2TBFs8QFd7Xl3qjwF8Tojea2Eu4BfT0e4/aIobuB1upW
```

Reference:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows>

Question: 166

HOTSPOT -

You have an Azure subscription that contains an Azure Storage account.

You plan to copy an on-premises virtual machine image to a container named `vmimages`.

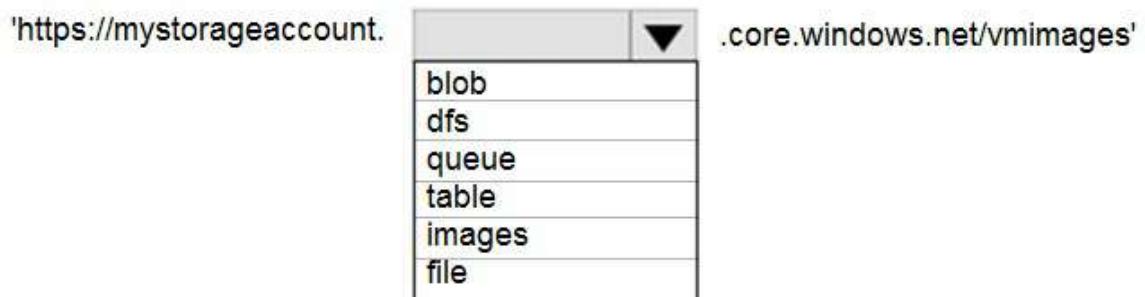
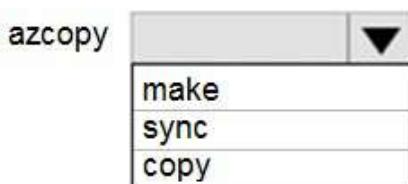
You need to create the container for the planned image.

Which command should you run? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

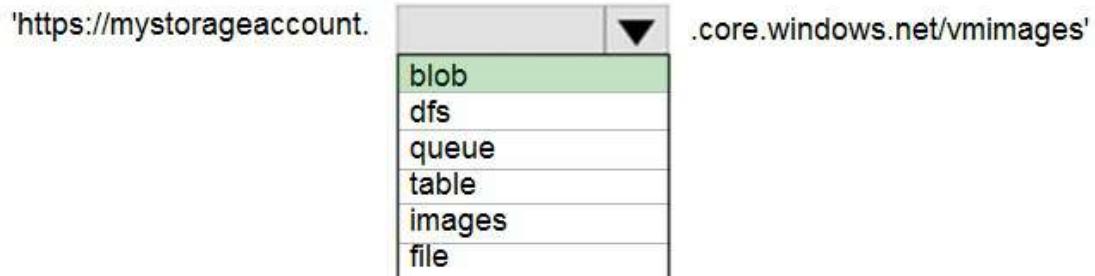
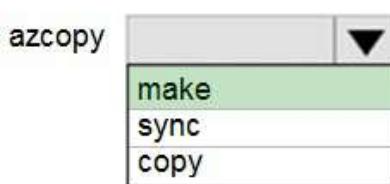
Hot Area:

Answer Area



Answer:

Answer Area



Explanation:

`azcopy make`.

`https://mystorageaccount.blob.core.windows.net/vmimages'`

Similar to OS Images, a VM Image is a collection of metadata and pointers to a set of VHDs (one VHD per disk) stored as page blobs in Azure Storage.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-ref-azcopy-make>

Question: 167

CertyIQ

HOTSPOT -

You have an Azure File sync group that has the endpoints shown in the following table.

Name	Type
Endpoint1	Cloud endpoint
Endpoint2	Server endpoint
Endpoint3	Server endpoint

Cloud tiering is enabled for Endpoint3.

You add a file named File1 to Endpoint1 and a file named File2 to Endpoint2.

On which endpoints will File1 and File2 be available within 24 hours of adding the files? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

File1:

▼

- Endpoint1 only
- Endpoint3 only
- Endpoint2 and Endpoint3 only
- Endpoint1, Endpoint2, and Endpoint3

File2:

▼

- Endpoint2 only
- Endpoint3 only
- Endpoint2 and Endpoint3 only
- Endpoint1, Endpoint2, and Endpoint3

Answer:

Answer Area

File1:

- Endpoint1 only
- Endpoint3 only
- Endpoint2 and Endpoint3 only
- Endpoint1, Endpoint2, and Endpoint3

File2:

- Endpoint2 only
- Endpoint3 only
- Endpoint2 and Endpoint3 only
- Endpoint1, Endpoint2, and Endpoint3

Explanation:

File1: Endpoint1 only.

It is a cloud endpoint, and it is scanned by the detection job every 24 hours.

File2: Endpoint1, Endpoint2 and Endpoint3.

With the on-premises servers the file is scanned and synced automatically after it's being added.

Note: They changed the question in Exam from "within 24 hours" to "after 24 hours".

Reference:

<https://docs.microsoft.com/en-us/learn/modules/extend-share-capacity-with-azure-file-sync/2-what-azure-file-sync>

Question: 168

CertyIQ

HOTSPOT -

You have several Azure virtual machines on a virtual network named VNet1.
You configure an Azure Storage account as shown in the following exhibit.

Home > Storage accounts >contoso – Firewalls and virtual networks

contoso – Firewalls and virtual networks

Storage Account

Search (Ctrl + /)

Save Discard

Allow access from

All networks Selected networks

Configure network security for your storage accounts. [Learn more.](#)

Virtual networks

Secure your storage account with virtual networks. [+ Add existing virtual network](#) [+ Add new virtual network](#)

VIRTUAL NET...	SUBNET	ADDRESS RA...	ENDPOINT ST...	RESOURCE G...	SUBSCRIPTION
▼ VNet1	1	10.2.0.0/16		DemoRG	Production subscrip ...
	Prod	10.2.0.0/24	✓ Enabled	DemoRG	Production subscrip ...

Firewall

Add IP ranges to allow access from the Internet or your on-premises networks. [Learn more.](#)

ADDRESS RANGE

IP address or CIDR

Exceptions

Allow trusted Microsoft services to access this storage account [?](#)

Allow read access to storage logging from any network

Allow read access to storage metrics from any network

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

The virtual machines on the 10.2.0.0/24 subnet will have network connectivity to the file shares in the storage account [answer choice].

▼

always
during a backup
never

Azure Backup will be able to back up the unmanaged hard disks of the virtual machines in the storage account [answer choice].

▼

always
during a backup
never

Answer:

Answer Area

The virtual machines on the 10.2.9.0/24 subnet will have network connectivity to the file shares in the storage account [answer choice].

always
during a backup
never

Azure Backup will be able to back up the unmanaged hard disks of the virtual machines in the storage account [answer choice].

always
during a backup
never

Explanation:

Box 1: never -

The 10.2.9.0/24 subnet is not whitelisted.

Box 2: never -

After you configure firewall and virtual network settings for your storage account, select Allow trusted Microsoft services to access this storage account as an exception to enable Azure Backup service to access the network restricted storage account.

The screenshot shows the 'Firewalls and virtual networks' blade for a storage account named 'sogupstorage'. The left sidebar lists various settings like Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. Under SETTINGS, 'Firewalls and virtual networks' is selected. The main area shows a table with columns: VIRTUAL NET..., SUBNET, ADDRESS RA..., ENDPOINT ST..., RESOURCE G..., and SUBSCRIPTION. A note says 'No network selected.' Below this is a 'Firewall' section with a note to add IP ranges. The 'ADDRESS RANGE' section has a 'IP address or CIDR' input field and a 'Exceptions' section. The 'Exceptions' section contains three checkboxes: 'Allow trusted Microsoft services to access this storage account' (which is checked and highlighted with a red box), 'Allow read access to storage logging from any network', and 'Allow read access to storage metrics from any network'.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows> <https://azure.microsoft.com/en-us/blog/azure-backup-now-supports-storage-accounts-secured-with-azure-storage-firewalls-and-virtual-networks/>

HOTSPOT -

You have a sync group named Sync1 that has a cloud endpoint. The cloud endpoint includes a file named File1.txt. Your on-premises network contains servers that run Windows Server 2016. The servers are configured as shown in the following table.

Name	Share	Share contents
Server1	Share1	File1.txt, File2.txt
Server2	Share2	File2.txt, File3.txt

You add Share1 as an endpoint for Sync1. One hour later, you add Share2 as an endpoint for Sync1.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
On the cloud endpoint, File1.txt is overwritten by File1.txt from Share1.	<input type="radio"/>	<input type="radio"/>
On Server1, File1.txt is overwritten by File1.txt from the cloud endpoint.	<input type="radio"/>	<input type="radio"/>
File1.txt from Share1 replicates to Share2.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
On the cloud endpoint, File1.txt is overwritten by File1.txt from Share1.	<input type="radio"/>	<input checked="" type="radio"/>
On Server1, File1.txt is overwritten by File1.txt from the cloud endpoint.	<input type="radio"/>	<input checked="" type="radio"/>
File1.txt from Share1 replicates to Share2.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

- 1) On the cloud endpoint, File1.txt is overwritten by File1.txt from Share1: "No"
- 2) On Server1, File1.txt is overwritten by File1.txt from the cloud endpoint: "No"
- 3) File1.txt from Share1 replicates to Share2: "Yes"

If the same file is changed on two servers at approximately the same time, what happens?

Azure File Sync uses a simple conflict-resolution strategy: we keep both changes to files that are changed in two endpoints at the same time. The most recently written change keeps the original file name. The older file (determined by LastWriteTime) has the endpoint name and the conflict number appended to the filename. For server endpoints, the endpoint name is the name of the server. For cloud endpoints, the endpoint name is Cloud. The name follows this taxonomy:

<FileNameWithoutExtension>-<endpointName>[-#].<ext>

For example, the first conflict of CompanyReport.docx would become CompanyReport-CentralServer.docx if CentralServer is where the older write occurred. The second conflict would be named CompanyReport-CentralServer-1.docx. Azure File Sync supports 100 conflict files per file. Once the maximum number of conflict files has been reached, the file will fail to sync until the number of conflict files is less than 100.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-planning>

Question: 170

CertyIQ

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

Name	Kind	Performance	Replication	Access tier
storage1	Storage (general purpose v1)	Premium	Geo-redundant storage (GRS)	None
storage2	StorageV2 (general purpose v2)	Standard	Locally-redundant storage (LRS)	Cool
storage3	StorageV2 (general purpose v2)	Premium	Read-access geo-redundant storage (RA-GRS)	Hot
storage4	BlobStorage	Standard	Locally-redundant storage (LRS)	Hot

You need to identify which storage account can be converted to zone-redundant storage (ZRS) replication by requesting a live migration from Azure support.

What should you identify?

- A. storage1
- B. storage2
- C. storage3
- D. storage4

Answer: B

Explanation:

ZRS currently supports standard general-purpose v2, FileStorage and BlockBlobStorage storage account types.

Incorrect Answers:

A, not C: Live migration is supported only for storage accounts that use LRS replication. If your account uses GRS or RA-GRS, then you need to first change your account's replication type to LRS before proceeding. This intermediary step removes the secondary endpoint provided by GRS/RA-GRS.

Also, only standard storage account types support live migration. Premium storage accounts must be migrated manually.

D: ZRS currently supports standard general-purpose v2, FileStorage and BlockBlobStorage storage account

types.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy-zrs>

Question: 171

CertyIQ

You have an Azure subscription that contains a storage account named account1.

You plan to upload the disk files of a virtual machine to account1 from your on-premises network. The on-premises network uses a public IP address space of 131.107.1.0/24.

You plan to use the disk files to provision an Azure virtual machine named VM1. VM1 will be attached to a virtual network named VNet1. VNet1 uses an IP address space of 192.168.0.0/24.

You need to configure account1 to meet the following requirements:

- ⇒ Ensure that you can upload the disk files to account1.
- ⇒ Ensure that you can attach the disks to VM1.
- ⇒ Prevent all other access to account1.

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

NOTE: Each correct selection is worth one point.

- A. From the Networking blade of account1, select Selected networks.
- B. From the Networking blade of account1, select Allow trusted Microsoft services to access this storage account.
- C. From the Networking blade of account1, add the 131.107.1.0/24 IP address range.
- D. From the Networking blade of account1, add VNet1.
- E. From the Service endpoints blade of VNet1, add a service endpoint.

Answer: AC

Explanation:

Virtual machine disk traffic (including mount and unmount operations, and disk IO) is not affected by network rules. REST access to page blobs is protected by network rules.

Endpoints are enabled on subnets configured in Azure virtual networks. Endpoints can't be used for traffic from your premises to Azure services. For more information, see Secure Azure service access from on-premises.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview>

<https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security>

Question: 172

CertyIQ

DRAG DROP -

You have an on-premises file server named Server1 that runs Windows Server 2016.

You have an Azure subscription that contains an Azure file share.

You deploy an Azure File Sync Storage Sync Service, and you create a sync group.

You need to synchronize files from Server1 to Azure.

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

Answer Area

Install the Azure File Sync agent on Server1

Create an Azure on-premises data gateway

Create a Recovery Services vault



Register Server1

Add a server endpoint

Install the DFS Replication server role on Server1



Answer:

Actions

Answer Area

Install the Azure File Sync agent on Server1

Install the Azure File Sync agent on Server1

Create an Azure on-premises data gateway

Register Server1

Create a Recovery Services vault



Register Server1

Add a server endpoint

Add a server endpoint



Install the DFS Replication server role on Server1

Explanation:

Step 1: Install the Azure File Sync agent on Server1

The Azure File Sync agent is a downloadable package that enables Windows Server to be synced with an Azure file share

Step 2: Register Server1.

Register Windows Server with Storage Sync Service

Registering your Windows Server with a Storage Sync Service establishes a trust relationship between your server (or cluster) and the Storage Sync Service.

Step 3: Add a server endpoint -

Create a sync group and a cloud endpoint.

A sync group defines the sync topology for a set of files. Endpoints within a sync group are kept in sync with each other. A sync group must contain one cloud endpoint, which represents an Azure file share and one or more server endpoints. A server endpoint represents a path on registered server.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-deployment-guide>

Question: 173

CertyIQ

HOTSPOT -

You plan to create an Azure Storage account in the Azure region of East US 2.

You need to create a storage account that meets the following requirements:

- ⇒ Replicates synchronously.
- ⇒ Remains available if a single data center in the region fails.

How should you configure the storage account? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Replication:

Geo-redundant storage (GRS)
Locally-redundant storage (LRS)
Read-access geo-redundant storage (RA GRS)
Zone-redundant storage (ZRS)

Account type:

Blob storage
Storage (general purpose v1)
StorageV2 (general purpose v2)

Answer:

Answer Area

Replication:

Geo-redundant storage (GRS)
Locally-redundant storage (LRS)
Read-access geo-redundant storage (RA GRS)
Zone-redundant storage (ZRS)

Account type:

Blob storage
Storage (general purpose v1)
StorageV2 (general purpose v2)

Explanation:

Box 1: Zone-redundant storage (ZRS)

ZRS replicates your data synchronously across three storage clusters in a single region.

LRS would not remain available if a data center in the region fails

GRS and RA GRS use asynchronous replication.

Box 2: StorageV2 (general purpose V2)

ZRS only support GPv2.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy> <https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy-zrs>

Question: 174

CertyIQ

You plan to use the Azure Import/Export service to copy files to a storage account.
Which two files should you create before you prepare the drives for the import job? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. an XML manifest file
- B. a dataset CSV file
- C. a JSON configuration file
- D. a PowerShell PS1 file
- E. a driveset CSV file

Answer: BE

Explanation:

B: Modify the dataset.csv file in the root folder where the tool resides. Depending on whether you want to import a file or folder or both, add entries in the dataset.csv file

E: Modify the driveset.csv file in the root folder where the tool resides.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-data-to-files>

Question: 175

CertyIQ

You have a Recovery Service vault that you use to test backups. The test backups contain two protected virtual machines.

You need to delete the Recovery Services vault.

What should you do first?

- A. From the Recovery Service vault, delete the backup data.
- B. Modify the disaster recovery properties of each virtual machine.
- C. Modify the locks of each virtual machine.
- D. From the Recovery Service vault, stop the backup of each backup item.

Answer: D

Explanation:

You can't delete a Recovery Services vault if it is registered to a server and holds backup data. If you try to delete a vault, but can't, the vault is still configured to receive backup data.

Remove vault dependencies and delete vault

In the vault dashboard menu, scroll down to the Protected Items section, and click Backup Items. In this menu, you can stop and delete Azure File Servers, SQL Servers in Azure VM, and Azure virtual machines.

The screenshot shows the Azure Recovery Services vault interface. On the left, there's a sidebar with 'PROTECTED ITEMS' and 'MANAGE' sections. Under 'PROTECTED ITEMS', 'Backup items' is selected and highlighted with a red box. Under 'MANAGE', 'Site Recovery Infrastructure' and 'Backup Infrastructure' are listed. The main area displays 'BACKUP MANAGEMENT TYPE' and 'BACKUP ITEM COUNT' for various resources. The data is as follows:

Backup Management Type	Backup Item Count
Azure Storage (Azure Files)	4
Azure Backup Server	3
SQL in Azure VM	1
Azure Backup Agent	1
Azure Virtual Machine	1
DPM	0

Reference:

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-delete-vault>

Question: 176

CertyIQ

HOTSPOT -

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

Name	Type	Location	Resource group
RG1	Resource group	West US	<i>Not applicable</i>
RG2	Resource group	West US	<i>Not applicable</i>
Vault1	Recovery Services vault	Central US	RG1
Vault2	Recovery Services vault	West US	RG2
VM1	Virtual machine	Central US	RG2
storage1	Storage account	West US	RG1
SQL1	Azure SQL database	East US	RG2

In storage1, you create a blob container named blob1 and a file share named share1.

Which resources can be backed up to Vault1 and Vault2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Can use Vault1 for backups:

VM1 only
VM1 and share1 only
VM1 and SQL1 only
VM1, storage1, and SQL1 only
VM1, blob1, share1, and SQL1

Can use Vault2 for backups:

storage1 only
share1 only
VM1 and share1 only
blob1 and share1 only
storage1 and SQL1 only

Answer:

Answer Area

Can use Vault1 for backups:

VM1 only
VM1 and share1 only
VM1 and SQL1 only
VM1, storage1, and SQL1 only
VM1, blob1, share1, and SQL1

Can use Vault2 for backups:

storage1 only
share1 only
VM1 and share1 only
blob1 and share1 only
storage1 and SQL1 only

Explanation:

Box 1: VM1 only -

VM1 is in the same region as Vault1.

File1 is not in the same region as Vault1.

SQL is not in the same region as Vault1.

Blobs cannot be backed up to service vaults.

Note: To create a vault to protect virtual machines, the vault must be in the same region as the virtual machines.

Box 2: Share1 only.

Storage1 is in the same region (West USA) as Vault2. Share1 is in Storage1.

Note: After you select Backup, the Backup pane opens and prompts you to select a storage account from a list of discovered supported storage accounts. They're either associated with this vault or present in the same region as the vault, but not yet associated to any Recovery Services vault.

Reference:

<https://docs.microsoft.com/en-us/bs-cyrl-ba/azure/backup/backup-create-rs-vault> <https://docs.microsoft.com/en-us/azure/backup/backup-afs>

Question: 177

CertyIQ

You have an Azure subscription named Subscription1.

You have 5 TB of data that you need to transfer to Subscription1.

You plan to use an Azure Import/Export job.

What can you use as the destination of the imported data?

- A. a virtual machine
- B. an Azure Cosmos DB database

- C. Azure File Storage
- D. the Azure File Sync Storage Sync Service

Answer: C

Explanation:

Azure Import/Export service is used to securely import large amounts of data to Azure Blob storage and Azure Files by shipping disk drives to an Azure datacenter.

The maximum size of an Azure Files Resource of a file share is 5 TB.

Note:

There are several versions of this question in the exam. The question has two correct answers:

- 1. Azure File Storage
- 2. Azure Blob Storage

The question can have other incorrect answer options, including the following:

- ⇒ Azure Data Lake Store
- ⇒ Azure SQL Database
- ⇒ Azure Data Factory

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-service>

Question: 178

CertyIQ

HOTSPOT -

You have an Azure subscription.

You create the Azure Storage account shown in the following exhibit.

Create storage account X

✓ Validation passed

Basics Networking Advanced Tags Review + create

Basics

Subscription Subscription1
Resource group RG1

Location {Europe} North Europe

Storage account name storage16852
Deployment model Resource manager
Account kind StorageV2 (general purpose v2)
Replication Locally-redundant storage (LRS)
Performance Standard
Access tier (default) Hot

Networking

Connectivity method Private endpoint
Private Endpoint {New} StorageEndpoint1 (blob) (privatelink.blob.core.windows.net)

Advanced

Secure transfer required Enabled
Large file shares Disabled
Blob soft delete Disabled
Blob change feed Disabled
Hierarchical namespace Disabled
NFS v3 Disabled

Create

< Previous

Next >

[Download a template for automation](#)

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

The minimum number of copies of the storage account will be [answer choice]

1
2
3
4

To reduce the cost of infrequently accessed data in the storage account, you must modify the [answer choice] setting

Access tier (default)
Performance
Account kind
Replication

Answer:

Answer Area

The minimum number of copies of the storage account will be [answer choice]

1
2
3
4

To reduce the cost of infrequently accessed data in the storage account, you must modify the [answer choice] setting

Access tier (default)
Performance
Account kind
Replication

Explanation:

Box 1: 3 -

Locally Redundant Storage (LRS) provides highly durable and available storage within a single location (sub region). We maintain an equivalent of 3 copies

(replicas) of your data within the primary location as described in our SOSP paper; this ensures that we can recover from common failures (disk, node, rack) without impacting your storage account's availability and durability.

Box 2: Access tier -

Change the access tier from Hot to Cool.

Note: Azure storage offers different access tiers, which allow you to store blob object data in the most cost-effective manner. The available access tiers include:

Hot - Optimized for storing data that is accessed frequently.

Cool - Optimized for storing data that is infrequently accessed and stored for at least 30 days.

Archive - Optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements (on the order of hours).

Reference:

<https://azure.microsoft.com/en-us/blog/data-series-introducing-locally-redundant-storage-for-windows-azure-storage/> <https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers>

CertyIQ

Question: 179

You have an Azure Storage account named storage1.

You plan to use AzCopy to copy data to storage1.

You need to identify the storage services in storage1 to which you can copy the data.

Which storage services should you identify?

- A. blob, file, table, and queue
- B. blob and file only
- C. file and table only
- D. file only
- E. blob, table, and queue only

Answer: B

Explanation:

AzCopy is a command-line utility that you can use to copy blobs or files to or from a storage account.

Incorrect Answers:

A, C, E: AzCopy does not support table and queue storage services.

D: AzCopy supports file storage services, as well as blob storage services.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10>

CertyIQ

Question: 180

HOTSPOT -

You have an Azure Storage account named storage1 that uses Azure Blob storage and Azure File storage.

You need to use AzCopy to copy data to the blob storage and file storage in storage1.

Which authentication method should you use for each type of storage? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Blob storage:	<table border="1"><tr><td>Azure Active Directory (Azure AD) only</td></tr><tr><td>Shared access signatures (SAS) only</td></tr><tr><td>Access keys and shared access signatures (SAS) only</td></tr><tr><td>Azure Active Directory (Azure AD) and shared access signatures (SAS) only</td></tr><tr><td>Azure Active Directory (Azure AD), access keys, and shared access signatures (SAS)</td></tr></table>	Azure Active Directory (Azure AD) only	Shared access signatures (SAS) only	Access keys and shared access signatures (SAS) only	Azure Active Directory (Azure AD) and shared access signatures (SAS) only	Azure Active Directory (Azure AD), access keys, and shared access signatures (SAS)
Azure Active Directory (Azure AD) only						
Shared access signatures (SAS) only						
Access keys and shared access signatures (SAS) only						
Azure Active Directory (Azure AD) and shared access signatures (SAS) only						
Azure Active Directory (Azure AD), access keys, and shared access signatures (SAS)						
File storage:	<table border="1"><tr><td>Azure Active Directory (Azure AD) only</td></tr><tr><td>Shared access signatures (SAS) only</td></tr><tr><td>Access keys and shared access signatures (SAS) only</td></tr><tr><td>Azure Active Directory (Azure AD) and shared access signatures (SAS) only</td></tr><tr><td>Azure Active Directory (Azure AD), access keys, and shared access signatures (SAS)</td></tr></table>	Azure Active Directory (Azure AD) only	Shared access signatures (SAS) only	Access keys and shared access signatures (SAS) only	Azure Active Directory (Azure AD) and shared access signatures (SAS) only	Azure Active Directory (Azure AD), access keys, and shared access signatures (SAS)
Azure Active Directory (Azure AD) only						
Shared access signatures (SAS) only						
Access keys and shared access signatures (SAS) only						
Azure Active Directory (Azure AD) and shared access signatures (SAS) only						
Azure Active Directory (Azure AD), access keys, and shared access signatures (SAS)						

Answer:

Answer Area

Blob storage:	<table border="1"><tr><td>Azure Active Directory (Azure AD) only</td></tr><tr><td>Shared access signatures (SAS) only</td></tr><tr><td>Access keys and shared access signatures (SAS) only</td></tr><tr><td>Azure Active Directory (Azure AD) and shared access signatures (SAS) only</td></tr><tr><td>Azure Active Directory (Azure AD), access keys, and shared access signatures (SAS)</td></tr></table>	Azure Active Directory (Azure AD) only	Shared access signatures (SAS) only	Access keys and shared access signatures (SAS) only	Azure Active Directory (Azure AD) and shared access signatures (SAS) only	Azure Active Directory (Azure AD), access keys, and shared access signatures (SAS)
Azure Active Directory (Azure AD) only						
Shared access signatures (SAS) only						
Access keys and shared access signatures (SAS) only						
Azure Active Directory (Azure AD) and shared access signatures (SAS) only						
Azure Active Directory (Azure AD), access keys, and shared access signatures (SAS)						
File storage:	<table border="1"><tr><td>Azure Active Directory (Azure AD) only</td></tr><tr><td>Shared access signatures (SAS) only</td></tr><tr><td>Access keys and shared access signatures (SAS) only</td></tr><tr><td>Azure Active Directory (Azure AD) and shared access signatures (SAS) only</td></tr><tr><td>Azure Active Directory (Azure AD), access keys, and shared access signatures (SAS)</td></tr></table>	Azure Active Directory (Azure AD) only	Shared access signatures (SAS) only	Access keys and shared access signatures (SAS) only	Azure Active Directory (Azure AD) and shared access signatures (SAS) only	Azure Active Directory (Azure AD), access keys, and shared access signatures (SAS)
Azure Active Directory (Azure AD) only						
Shared access signatures (SAS) only						
Access keys and shared access signatures (SAS) only						
Azure Active Directory (Azure AD) and shared access signatures (SAS) only						
Azure Active Directory (Azure AD), access keys, and shared access signatures (SAS)						

Explanation:

1. Blob Storage:

Correct Answer: **Azure Active Directory (Azure AD) and shared access signatures (SAS) only.**

Blob Storage in Azure Storage Accounts can be accessed using:

Azure Active Directory (Azure AD) - Role-based access control (RBAC) can be used for authentication.

Shared Access Signatures (SAS) - Temporary, token-based access to storage resources.

Access Keys (storage account keys) are not required when using Azure AD authentication.

2. File Storage:

Correct Answer: **Shared access signatures (SAS) only.**

Azure File Storage supports:

SAS Tokens for controlled access.

Azure AD DS (Domain Services) for authentication when using SMB (Server Message Block) protocol.

Azure AD authentication for direct access to Azure Files is not yet fully supported for all scenarios, meaning SAS remains the preferred method.

Question: 181

CertyIQ

You have an Azure subscription that contains an Azure Storage account. You plan to create an Azure container instance named container1 that will use a Docker image named Image1. Image1 contains a Microsoft SQL Server instance that requires persistent storage. You need to configure a storage service for Container1. What should you use?

- A. Azure Files
- B. Azure Blob storage
- C. Azure Queue storage
- D. Azure Table storage

Answer: A**Explanation:**

A. Azure Files.

Azure Files is the recommended storage service for use with Azure Container Instances when you need to share data between containers or persist data across container restarts. Since Image1 contains a Microsoft SQL Server instance that requires persistent storage, you should use Azure Files as the storage service for container1.

Azure Blob storage, Azure Queue storage, and Azure Table storage are not recommended for use with Azure Container Instances when you need to persist data across container restarts. These storage services are more appropriate for other types of data storage and retrieval scenarios.

Question: 182

CertyIQ

You have an app named App1 that runs on two Azure virtual machines named VM1 and VM2. You plan to implement an Azure Availability Set for App1. The solution must ensure that App1 is available during planned maintenance of the hardware hosting VM1 and VM2.

What should you include in the Availability Set?

- A. one update domain
- B. two fault domains
- C. one fault domain
- D. two update domains

Answer: D**Explanation:**

Microsoft updates, which Microsoft refers to as planned maintenance events, sometimes require that VMs be rebooted to complete the update. To reduce the impact on VMs, the Azure fabric is divided into update domains to ensure that not all VMs are rebooted at the same time.

Incorrect Answers:

A: An update domain is a group of VMs and underlying physical hardware that can be rebooted at the same time.

B, C: A fault domain shares common storage as well as a common power source and network switch. It is used to protect against unplanned system failure.

Reference:

<https://petri.com/understanding-azure-availability-sets>

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/tutorial-availability-sets>

CertyIQ

Question: 183

You have an Azure subscription named Subscription1.
You have 5 TB of data that you need to transfer to Subscription1.
You plan to use an Azure Import/Export job.
What can you use as the destination of the imported data?

- A. an Azure Cosmos DB database
- B. Azure Blob storage
- C. Azure Data Lake Store
- D. the Azure File Sync Storage Sync Service

Answer: B

Explanation:

Azure Import/Export service is used to securely import large amounts of data to Azure Blob storage and Azure Files by shipping disk drives to an Azure datacenter.

Note:

There are several versions of this question in the exam. The question has two correct answers:

1. Azure File Storage
2. Azure Blob Storage

The question can have other incorrect answer options, including the following:

- ⇒ a virtual machine
- ⇒ Azure SQL Database
- ⇒ Azure Data Factory

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-service>

CertyIQ

Question: 184

DRAG DROP -

You have an Azure subscription that contains an Azure file share.

You have an on-premises server named Server1 that runs Windows Server 2016.

You plan to set up Azure File Sync between Server1 and the Azure file share.

You need to prepare the subscription for the planned Azure File Sync.

Which two actions should you perform in the Azure subscription? To answer, drag the appropriate actions to the correct targets. Each action may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Actions

- Create a Storage Sync Service
- Install the Azure File Sync agent
- Create a sync group
- Run Server Registration

Answer Area

First action:

Action

Second action:

Action

Answer:

Actions

-
-
- Create a sync group
- Run Server Registration

Answer Area

First action:

Create a Storage Sync Service

Second action:

Install the Azure File Sync agent

Explanation:

First action: Create a Storage Sync Service

The deployment of Azure File Sync starts with placing a Storage Sync Service resource into a resource group of your selected subscription.

Second action: Install the Azure File Sync agent

The Azure File Sync agent is a downloadable package that enables Windows Server to be synced with an Azure file share.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-deployment-guide>

Question: 185

CertyIQ

HOTSPOT -

You have an Azure subscription that contains the file shares shown in the following table.

Name	Location
share1	West US
share2	West US
share3	East US

You have the on-premises file shares shown in the following table.

Name	Server	Path
data1	Server1	D:\Folder1
data2	Server2	E:\Folder2
data3	Server3	E:\Folder2

You create an Azure file sync group named Sync1 and perform the following actions:

- ⇒ Add share1 as the cloud endpoint for Sync1.
- ⇒ Add data1 as a server endpoint for Sync1.
- ⇒ Register Server1 and Server2 to Sync1.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
You can add share3 as an additional cloud endpoint for Sync1.	<input type="radio"/>	<input type="radio"/>
You can add data2 as an additional server endpoint for Sync1.	<input type="radio"/>	<input type="radio"/>
You can add data3 as an additional server endpoint for Sync1.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
You can add share3 as an additional cloud endpoint for Sync1.	<input type="radio"/>	<input checked="" type="radio"/>
You can add data2 as an additional server endpoint for Sync1.	<input checked="" type="radio"/>	<input type="radio"/>
You can add data3 as an additional server endpoint for Sync1.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Box 1: No -

A sync group must contain one cloud endpoint, which represents an Azure file share and one or more server endpoints.

Box 2: Yes -

Data2 is located on Server2 which is registered to Sync1.

Box 3: No -

Data3 is located on Server3 which is not registered to Sync1.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-deployment-guide?tabs=azure-portal%2Cproactive-portal#create-a-sync-group-and-a-cloud-endpoint>

Question: 186

CertyIQ

HOTSPOT -

You have an Azure subscription named Subscription1 that contains the resources shown in the following table:

Name	Type	Location	Resource group
RG1	Resource group	East US	<i>Not applicable</i>
RG2	Resource group	West US	<i>Not applicable</i>
Vault1	Recovery Services vault	West Europe	RG1
storage1	Storage account	East US	RG2
storage2	Storage account	West US	RG1
storage3	Storage account	West Europe	RG2
Analytics1	Log Analytics workspace	East US	RG1
Analytics2	Log Analytics workspace	West US	RG2
Analytics3	Log Analytics workspace	West Europe	RG1

You plan to configure Azure Backup reports for Vault1.

You are configuring the Diagnostics settings for the AzureBackupReports log.

Which storage accounts and which Log Analytics workspaces can you use for the Azure Backup reports of Vault1?

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Storage accounts:

storage1 only
storage2 only
storage3 only
storage1, storage2, and storage3

Log Analytics workspaces:

Analytics1 only
Analytics2 only
Analytics3 only
Analytics1, Analytics2, and Analytics3

Answer:

Answer Area

Storage accounts:

storage1 only
storage2 only
storage3 only
storage1, storage2, and storage3

Log Analytics workspaces:

Analytics1 only
Analytics2 only
Analytics3 only
Analytics1, Analytics2, and Analytics3

Explanation:

Storage accounts: Storage 3 only

Storage Account must be in the same Region as the Recovery Services Vault.

Log Analytics workspaces: Analytics1, Analytics2, and Analytics3

Set up one or more Log Analytics workspaces to store your Backup reporting data. The location and subscription where this Log Analytics workspace can be created is independent of the location and subscription where your Vaults exist.

Reference:

<https://docs.microsoft.com/en-us/azure/backup/configure-reports#1-create-a-log-analytics-workspace-or-use-an-existing-one>

Question: 187

CertyIQ

HOTSPOT -

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

Storage accounts

Default Directory

+ Add Manage view Refresh Export to CSV Assign tags Delete Feedback

Filter by name...

Subscription == all

Resource group == all

Location == all

+ Add filter

Showing 1 to 4 of 4 records.

<input type="checkbox"/>	Name ↑	Type ↑	Kind ↑	Resource group ↑	Location ↑
<input type="checkbox"/>	contoso101	Storage account	StorageV2	RG1	East US
<input type="checkbox"/>	contoso102	Storage account	Storage	RG1	East US
<input type="checkbox"/>	contoso103	Storage account	BlobStorage	RG1	East US
<input type="checkbox"/>	contoso104	Storage account	FileStorage	RG1	East US

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

You can create a premium file share in

contoso101only
contoso104 only
contoso101 or contoso104 only
contoso101, contoso102, or contoso104 only
contoso101, contoso102, contoso103, or contoso104

You can use the Archive access tier in

contoso101only
contoso101 or contoso103 only
contoso101, contoso102, and contoso103 only
contoso101, contoso102, and contoso104 only
contoso101, contoso102, contoso103, and contoso104

Answer:

Answer Area

You can create a premium file share in

contoso101only
contoso104 only
contoso101 or contoso104 only
contoso101, contoso102, or contoso104 only
contoso101, contoso102, contoso103, or contoso104

You can use the Archive access tier in

contoso101only
contoso101 or contoso103 only
contoso101, contoso102, and contoso103 only
contoso101, contoso102, and contoso104 only
contoso101, contoso102, contoso103, and contoso104

Explanation:

Box 1: contoso104 only.

Premium file shares are hosted in a special purpose storage account kind, called a FileStorage account.

Box 2: contoso101 and contos103 only.

Object storage data tiering between hot, cool, and archive is supported in Blob Storage and General Purpose v2 (GPv2) accounts. General Purpose v1 (GPv1) accounts don't support tiering.

The archive tier supports only LRS, GRS, and RA-GRS.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-account-overview>

<https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-create-premium-fileshare?tabs=azure-portal>

<https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers>

Question: 188

CertyIQ

HOTSPOT -

You have an Azure subscription named Subscription1.

In Subscription1, you create an Azure file share named share1.

You create a shared access signature (SAS) named SAS1 as shown in the following exhibit:

Allowed services

Blob File Queue Table

Allowed resource types

Service Container Object

Allowed permissions

Read Write Delete List Add Create Update Process

Start and expiry date/time

Start

2018-09-01  2:00:00 PM

End

2018-09-14  2:00:00 PM

(UTC+02:00) --- Current Timezone --- 

Allowed IP addresses

193.77.134.10-193.77.134.50 

Allowed protocols

HTTPS only HTTPS and HTTP

Signing key

key1 

Generate SAS and connection string

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

If on September 2, 2018, you run Microsoft Azure Storage Explorer on a computer that has an IP address of 193.77.134.1, and you use SAS1 to connect to the storage account, you [answer choice].

will be prompted for credentials
will have no access
will have read, write, and list access
will have read-only access

If on September 10, 2018, you run the net use command on a computer that has an IP address of 193.77.134.50, and you use SAS1 as the password to connect to share1, you [answer choice].

will be prompted for credentials
will have no access
will have read, write, and list access
will have read-only access

Answer:

Answer Area

If on September 2, 2018, you run Microsoft Azure Storage Explorer on a computer that has an IP address of 193.77.134.1, and you use SAS1 to connect to the storage account, you [answer choice].

will be prompted for credentials
will have no access
will have read, write, and list access
will have read-only access

If on September 10, 2018, you run the net use command on a computer that has an IP address of 193.77.134.50, and you use SAS1 as the password to connect to share1, you [answer choice].

will be prompted for credentials
will have no access
will have read, write, and list access
will have read-only access

Explanation:

Box 1: will have no access

The IP 193.77.134.1 does not have access on the SAS, because it is not matching the SAS requirements. IP is out of range.

Box 2: will have no access

The SAS token is not supported in mounting Azure File share currently, it just supports the Azure storage account key.

Since it is using "net use" where it uses SMB, the SMB (Server Message Broker) protocol does not support SAS. It still asks for username/password. Accordingly, it will give error wrong username/pass and will not provide access.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-dotnet-shared-access-signature-part-1>

<https://docs.microsoft.com/en-us/azure/vs-azure-tools-storage-manage-with-storage-explorer?tabs=windows>

<https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows>

<https://docs.microsoft.com/en-us/answers/questions/40741/sas-key-for-unc-path.html>

Question: 189

CertyIQ

You have two Azure virtual machines named VM1 and VM2. You have two Recovery Services vaults named RSV1 and RSV2.

VM2 is backed up to RSV1.

You need to back up VM2 to RSV2.

What should you do first?

- A. From the RSV1 blade, click Backup items and stop the VM2 backup
- B. From the RSV2 blade, click Backup. From the Backup blade, select the backup for the virtual machine, and then click Backup
- C. From the VM2 blade, click Disaster recovery, click Replication settings, and then select RSV2 as the Recovery Services vault
- D. From the RSV1 blade, click Backup Jobs and export the VM2 job

Answer: A

Explanation:

If you want to change the recovery service vault you need to disassociate the previous RSV and delete the backup data. To delete backup data, you need to stop the backup first.

So:

1. Stop the backup in RSV1 (D)
2. Remove the backup data.
3. Disassociate the VM in RSV1.
4. Associate the VM in RSV2.

CertyIQ

Question: 190

You have a general-purpose v1 Azure Storage account named storage1 that uses locally-redundant storage (LRS). You need to ensure that the data in the storage account is protected if a zone fails. The solution must minimize costs and administrative effort.

What should you do first?

- A. Create a new storage account.
- B. Configure object replication rules.
- C. Upgrade the account to general-purpose v2.
- D. Modify the Replication setting of storage1.

Answer: C

Explanation:

General-purpose v2 storage accounts support the latest Azure Storage features and incorporate all of the functionality of general-purpose v1 and Blob storage accounts. General-purpose v2 accounts are recommended for most storage scenarios. General-purpose v2 accounts deliver the lowest per-gigabyte capacity prices for Azure Storage, as well as industry-competitive transaction prices. General-purpose v2 accounts support default account access tiers of hot or cool and blob level tiering between hot, cool, or archive.

Upgrading to a general-purpose v2 storage account from your general-purpose v1 or Blob storage accounts is straightforward. You can upgrade using the Azure portal, PowerShell, or Azure CLI. There is no downtime or risk of data loss associated with upgrading to a general-purpose v2 storage account. The account upgrade happens via a simple Azure Resource Manager operation that changes the account type.

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

Name	Type	Performance
storage1	StorageV2	Standard
storage2	BlobStorage	Standard
storage3	BlockBlobStorage	Premium
storage4	FileStorage	Premium

You plan to manage the data stored in the accounts by using lifecycle management rules.

To which storage accounts can you apply lifecycle management rules?

- A. storage1 only
- B. storage1 and storage2 only
- C. storage3 and storage4 only
- D. storage1, storage2, and storage3 only
- E. storage1, storage2, storage3, and storage4

Answer: D**Explanation:**

Lifecycle management policies are supported for block blobs and append blobs in general-purpose v2, premium block blob, and Blob Storage accounts.

The lifecycle management feature is available in all Azure regions for general purpose v2 (GPv2) accounts, blob storage accounts, premium block blobs storage accounts, and Azure Data Lake Storage Gen2 accounts.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/blobs/storage-lifecycle-management-concepts?tabs=azure-portal>

Question: 192

You create an Azure Storage account named contosostorage.

You plan to create a file share named data.

Users need to map a drive to the data file share from home computers that run Windows 10.

Which outbound port should you open between the home computers and the data file share?

- A. 80
- B. 443
- C. 445
- D. 3389

Answer: C**Explanation:**

Server Message Block (SMB) is used to connect to an Azure file share over the internet. The SMB protocol requires TCP port 445 to be open.

Incorrect Answers:

- A: Port 80 is required for HTTP to a web server
- B: Port 443 is required for HTTPS to a web server
- D: Port 3389443 is required for Remote desktop protocol (RDP) connections

Reference:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows>

CertyIQ

Question: 193

You have an Azure subscription named Subscription1.
You have 5 TB of data that you need to transfer to Subscription1.
You plan to use an Azure Import/Export job.
What can you use as the destination of the imported data?

- A. Azure File Storage
- B. an Azure Cosmos DB database
- C. Azure Data Factory
- D. Azure SQL Database

Answer: A

Explanation:

"Azure Import/Export service is used to securely import large amounts of data to Azure Blob storage and Azure Files by shipping disk drives to an Azure datacenter."

Reference:

<https://docs.microsoft.com/en-us/azure/import-export/storage-import-export-service>

CertyIQ

Question: 194

HOTSPOT -

You have an Azure subscription that contains an Azure Storage account named storageaccount1.
You export storageaccount1 as an Azure Resource Manager template. The template contains the following sections.

```
{  
    "type": "Microsoft.Storage/storageAccount",  
    "apiVersion": "2019-06-01",  
    "name": "storageaccount1",  
    "location": "eastus",  
    "sku": {  
        "name": "Standard_LRS",  
        "tier": "Standard"  
    },  
    "kind": "StorageV2",  
    "properties": {  
        "networkAcls": {  
            "bypass": "AzureServices",  
            "virtualNetworkRules": [],  
            "ipRules": [],  
            "defaultAction": "Allow",  
        },  
        "supportsHttpsTrafficOnly": true,  
        "encryption": {  
            "services": {  
                "file": {  
                    "keyType": "Account",  
                    "enabled": true  
                }  
                "blob": {  
                    "keyType": "Account",  
                    "enabled": true  
                }  
            },  
            "keySource": "Microsoft.Storage"  
        },  
        "accessTier": "Hot"  
    }  
},
```

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point

Hot Area:

Answer Area

Statements	Yes	No
A server that has a public IP address of 131.107.103.10 can access storageaccount1	<input type="radio"/>	<input type="radio"/>
Individual blobs in storageaccount1 can be set to use the archive tier	<input type="radio"/>	<input type="radio"/>
Global administrations in Azure Active Directory (Azure AD) can access a file share hosted in storageaccount1 by using their Azure AD credentials	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
A server that has a public IP address of 131.107.103.10 can access storageaccount1	<input checked="" type="radio"/>	<input type="radio"/>
Individual blobs in storageaccount1 can be set to use the archive tier	<input checked="" type="radio"/>	<input type="radio"/>
Global administrations in Azure Active Directory (Azure AD) can access a file share hosted in storageaccount1 by using their Azure AD credentials	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Box 1- Yes. VirtualNetworkRules & IpRules are blank, with the default action Allow.

Box 2- Yes. Individual blobs can be set to the archive tier - ref.<https://docs.microsoft.com/en-us/azure/storage/blobs/access-tiers-overview>

Box 3. No. To access blob data in the Azure portal with Azure AD credentials, a user must have the following role assignments:

A data access role, such as Storage Blob Data Contributor

The Azure Resource Manager Reader role

Reference:

<https://docs.microsoft.com/en-us/azure/storage/blobs/assign-azure-role-data-access?tabs=portal>

Question: 195

CertyIQ

You have an Azure subscription that contains a storage account named storage1. You have the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Linux
Device3	macOS

From which devices can you use AzCopy to copy data to storage1?

- A. Device 1 only
- B. Device1, Device2 and Device3
- C. Device1 and Device2 only
- D. Device1 and Device3 only

Answer: B

Explanation:

B:Device1, Device2 and Device3.

Az Copy is supported in all these three operating systems.

<https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10#download-azcopy>

Question: 196

CertyIQ

You have an Azure Storage account named storage1 that contains a blob container named container1. You need to prevent new content added to container1 from being modified for one year. What should you configure?

- A. the access tier
- B. an access policy
- C. the Access control (IAM) settings
- D. the access level

Answer: B

Explanation:

B.an access policy.

Using SAS in conjunction with a stored Access Policy the desired outcome can be achieved: "You can use a stored access policy to change the start time, expiry time, or permissions for a signature. You can also use a stored access policy to revoke a signature after it has been issued."

Reference:

<https://docs.microsoft.com/en-us/rest/api/storageservices/define-stored-access-policy>

Question: 197

CertyIQ

HOTSPOT -

You have an Azure Storage account named storage1 that contains a blob container. The blob container has a default access tier of Hot. Storage1 contains a container named container1.

You create lifecycle management rules in storage1 as shown in the following table.

Name	Rule scope	Blob type	Blob subtype	Rule block	Prefix match
Rule1	Limit blobs by using filters.	Block blobs	Base blobs	If base blobs were not modified for two days, move to archive storage. If base blobs were not modified for nine days, delete the blob.	container1/Dep1
Rule2	Apply to all blobs in storage1.	Block blobs	Base blobs	If base blobs were not modified for three days, move to cool storage. If base blobs were not modified for nine days, move to archive storage.	Not applicable

You perform the actions shown in the following table.

Date	Action
October 1	Upload three files named Dep1File1.docx, File2.docx, and File3.docx to container 1.
October 2	Edit Dep1File1.docx and File3.docx.
October 5	Edit File2.docx.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
On October 10, you can read Dep1File1.docx.	<input type="radio"/>	<input type="radio"/>
On October 10, you can read File2.docx.	<input type="radio"/>	<input type="radio"/>
On October 10, you can read File3.docx.	<input type="radio"/>	<input type="radio"/>

Answer:**Answer Area**

Statements	Yes	No
On October 10, you can read Dep1File1.docx.	<input type="radio"/>	<input checked="" type="radio"/>
On October 10, you can read File2.docx.	<input checked="" type="radio"/>	<input type="radio"/>
On October 10, you can read File3.docx.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

1) On October 10, you can read Dep1File1.docx: "No"

2) On October 10, you can read File2.docx: "Yes"

3) On October 10, you can read File3.docx: "Yes"

Cool Storage can be read immediately, but archived one needs to first be rehydrated.

Usage scenarios for the cool access tier include:

Short-term data backup and disaster recovery.

Older data sets that aren't used frequently, but are expected to be available for immediate access.

Large data sets that need to be stored in a cost-effective way while other data is being gathered for processing.

To learn how to move a blob to the hot or cool tier, see Set a blob's access tier.

Data in the cool tier has slightly lower availability, but offers the same high durability, retrieval latency, and throughput characteristics as the hot tier. For data in the cool tier, slightly lower availability and higher access costs may be acceptable trade-offs for lower overall storage costs, as compared to the hot tier. For more information, see SLA for storage.

Question: 198

CertyIQ

You are configuring Azure Active Directory (Azure AD) authentication for an Azure Storage account named storage1.

You need to ensure that the members of a group named Group1 can upload files by using the Azure portal. The solution must use the principle of least privilege.

Which two roles should you configure for storage1? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Storage Account Contributor
- B. Storage Blob Data Contributor
- C. Reader
- D. Contributor
- E. Storage Blob Data Reader

Answer: BC

Explanation:

To access blob data in the Azure portal with Azure AD credentials, a user must have the following role assignments:

* A data access role, such as Storage Blob Data Reader or Storage Blob Data Contributor

* The Azure Resource Manager Reader role, at a minimum

The Reader role is an Azure Resource Manager role that permits users to view storage account resources, but not modify them. It does not provide read permissions to data in Azure Storage, but only to account management resources. The Reader role is necessary so that users can navigate to blob containers in the Azure portal.

Note: in order from least to greatest permissions:

The Reader and Data Access role -

The Storage Account Contributor role

The Azure Resource Manager Contributor role

The Azure Resource Manager Owner role

Reference:

<https://docs.microsoft.com/en-us/azure/storage/blobs/assign-azure-role-data-access>

Question: 199

CertyIQ

HOTSPOT -

You have an Azure Storage account named storage1 that stores images.

You need to create a new storage account and replicate the images in storage1 to the new account by using object replication.

How should you configure the new account? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Account type:

- StorageV2 only
- StorageV2 or FileStorage only
- StorageV2 or BlobStorage only
- StorageV2, BlobStorage, or FileStorage

Object type to create in the new account:

- Container
- File share
- Table
- Queue

Answer:

Answer Area

Account type:

- StorageV2 only
- StorageV2 or FileStorage only
- StorageV2 or BlobStorage only
- StorageV2, BlobStorage, or FileStorage

Object type to create in the new account:

- Container
- File share
- Table
- Queue

Explanation:

Account type: StorageV2 or BlobStorage only

Object type to create in the new account: Container

Object Replication supports General Purpose V2 and Premium Blob accounts.

Blob versioning should be enabled on both the source and destination storage account.

Change feed is enabled on the source storage account.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/blobs/object-replication-overview>

CertyIQ

Question: 200

You have an on-premises server that contains a folder named D:\Folder1.

You need to copy the contents of D:\Folder1 to the public container in an Azure Storage account named contosodata.

Which command should you run?

- A. `https://contosodata.blob.core.windows.net/public`
- B. `azcopy sync D:\folder1 https://contosodata.blob.core.windows.net/public --snapshot`
- C. `azcopy copy D:\folder1 https://contosodata.blob.core.windows.net/public --recursive`
- D. `az storage blob copy start-batch D:\Folder1 https://contosodata.blob.core.windows.net/public`

Answer: C

Explanation:

The azcopy copy command copies a directory (and all of the files in that directory) to a blob container. The result is a directory in the container by the same name.

Incorrect Answers:

B: The azcopy sync command replicates the source location to the destination location. However, the file is skipped if the last modified time in the destination is more recent.

D: The az storage blob copy start-batch command copies multiple blobs to a blob container.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-blobs> <https://docs.microsoft.com/en-us/azure/storage/common/storage-ref-azcopy-copy>

CertyIQ

Question: 201

You have an Azure subscription.

In the Azure portal, you plan to create a storage account named storage1 that will have the following settings:

- ⇒ Performance: Standard
- ⇒ Replication: Zone-redundant storage (ZRS)
- ⇒ Access tier (default): Cool
- ⇒ Hierarchical namespace: Disabled

You need to ensure that you can set Account kind for storage1 to BlockBlobStorage.

Which setting should you modify first?

- A. Performance
- B. Replication
- C. Access tier (default)
- D. Hierarchical namespace

Answer: A

Explanation:

Select Standard performance for general-purpose v2 storage accounts (default). This type of account is recommended by Microsoft for most scenarios. For more information, see [Types of storage accounts](#).

Select Premium for scenarios requiring low latency. After selecting Premium, select the type of premium storage account to create. The following types of premium storage accounts are available:

Block blobs

File shares

Page blobs

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-account-overview>

<https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-performance-tiers>

CertyIQ

Question: 202

DRAG DROP -

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

Name	Azure Active Directory (Azure AD) authentication	Contents
storage1	Enabled	A blob container named container1 that has a public access level of No public access
storage2	Enabled	A file share named share1

You plan to use AzCopy to copy a blob from container1 directly to share1.

You need to identify which authentication method to use when you use AzCopy.

What should you identify for each account? To answer, drag the appropriate authentication methods to the correct accounts. Each method may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Methods

OAuth

Anonymous

A storage account access key

A shared access signature (SAS) token

Answer Area

storage1: Method

storage2: Method

Answer:**Methods**

OAuth

Anonymous

A storage account access key

A shared access signature (SAS) token

Answer Area

storage1: A shared access signature (SAS) token

storage2: A shared access signature (SAS) token

Explanation:

Box 1: A shared access signature (SAS) token.

You can provide authorization credentials by using Azure Active Directory (AD), or by using a Shared Access Signature (SAS) token.

For Blob storage you can use Azure AD & SAS.

Note: In the current release, if you plan to copy blobs between storage accounts, you'll have to append a SAS token to each source URL. You can omit the SAS token only from the destination URL.

Box 2: A shared access signature (SAS) token.

For File storage you can only use SAS.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10>

CertyIQ**Question: 203**

You create an Azure Storage account.

You plan to add 10 blob containers to the storage account.

For one of the containers, you need to use a different key to encrypt data at rest.

What should you do before you create the container?

- A. Generate a shared access signature (SAS).
- B. Modify the minimum TLS version.
- C. Rotate the access keys.
- D. Create an encryption scope.

Answer: D**Explanation:**

Encryption scopes enable you to manage encryption with a key that is scoped to a container or an individual blob. You can use encryption scopes to create secure boundaries between data that resides in the same storage account but belongs to different customers.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/blobs/encryption-scope-overview>

HOTSPOT

You have an Azure subscription. The subscription contains a storage account named storage1 that has the lifecycle management rules shown in the following table.

Name	Blob prefix	If base were last modified more than (days ago)	Then
Rule1	container1/	3 days	Move to archive storage
Rule2	<i>Not applicable</i>	5 days	Move to cool storage
Rule3	container2/	10 days	Delete the blob
Rule4	container2/	15 days	Move to archive storage

On June 1, you store two blobs in storage1 as shown in the following table.

Name	Location	Access tier
File1	container1	Hot
File2	container2	Hot

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
On June 6, File1 will be stored in the Cool access tier.	<input type="radio"/>	<input type="radio"/>
On June 1, File2 will be stored in the Cool access tier.	<input type="radio"/>	<input type="radio"/>
On June 16, File2 will be stored in the Archive access tier.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
On June 6, File1 will be stored in the Cool access tier.	<input type="radio"/>	<input checked="" type="radio"/>
On June 1, File2 will be stored in the Cool access tier.	<input type="radio"/>	<input checked="" type="radio"/>
On June 16, File2 will be stored in the Archive access tier.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

No

No

No

On June 6, File1 will be in archive because File1 is in container 1, and rule 1 applies 3 days after june 1.

On June 1, File2 will still be in Hot tier because File2 is in container2, Rule3 and Rule4 havent hit yet.

On June 16, File2 will be deleted because Rule3 applies 10 days after June 1.

Question: 205

CertyIQ

HOTSPOT

-

You have an Azure subscription.

You plan to deploy a storage account named storage1 by using the following Azure Resource Manager (ARM) template.

```

{
    "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "resources": [
        {
            "name": "storage1",
            "type": "Microsoft.Storage/storageAccounts",
            "apiVersion": "2021-06-01",
            "location": "East US",
            "properties": {
                "allowBlobPublicAccess": true,
                "defaultToOAuthAuthentication": false,
                "networkAcls": {
                    "bypass": "AzureServices",
                    "defaultAction": "Allow",
                    "ipRules": []
                }
            },
            "sku": {
                "name": "Standard_LRS"
            },
            "kind": "StorageV2"
        },
        {
            "name": "storage1/default",
            "type": "Microsoft.Storage/storageAccounts/blobServices",
            "apiVersion": "2021-06-01",
            "properties": {
                "restorePolicy": {
                    "enabled": true,
                    "days": 6
                },
                "deleteRetentionPolicy": {
                    "enabled": true,
                    "days": 7
                },
                "containerDeleteRetentionPolicy": {
                    "enabled": true,
                    "days": 7
                },
                "changeFeed": {
                    "enabled": true
                },
                "isVersioningEnabled": true
            },
            "dependsOn": [
                "[concat('Microsoft.Storage/storageAccounts/', 'storage1')]"
            ]
        }
    ]
}

```

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Changes made to the data in storage1 can be rolled back after seven days.	<input type="radio"/>	<input type="radio"/>
Only users located in the East US Azure region can connect to storage1.	<input type="radio"/>	<input type="radio"/>
Three copies of storage1 will be maintained in the East US Azure region.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
Changes made to the data in storage1 can be rolled back after seven days.	<input type="radio"/>	<input checked="" type="checkbox"/>
Only users located in the East US Azure region can connect to storage1.	<input type="radio"/>	<input checked="" type="checkbox"/>
Three copies of storage1 will be maintained in the East US Azure region.	<input checked="" type="checkbox"/>	<input type="radio"/>

Explanation:

No

No

Yes

deleteRetentionPolicy is 7 days, so can not be restored after 7 days. Means, backup is deleted after 7 days.

allowBlobPublicAccess is true, so anyone can access the blob, not just on Azure.

kind is Standard_LRS, so 3 local copies are stored.

Question: 206

CertyIQ

You have an on-premises server that contains a folder named D:\Folder1.

You need to copy the contents of D:\Folder1 to the public container in an Azure Storage account named contosodata.

Which command should you run?

- A. az storage blob copy start D:\Folder1 https://contosodata.blob.core.windows.net/public
- B. azcopy sync D:\folder1 https://contosodata.blob.core.windows.net/public --snapshot
- C. azcopy copy D:\folder1 https://contosodata.blob.core.windows.net/public --recursive
- D. az storage blob copy start-batch D:\Folder1 https://contosodata.blob.core.windows.net/public

Answer: C

Explanation:

A: URL of the Storage Account.

B: The azcopy sync command replicates the source location to the destination location. However, the file is skipped if the last modified time in the destination is more recent.

C: The azcopy copy command copies a directory (and all the files in that directory) to a blob container. The result is a directory in the container by the same name.

D: The az storage blob copy start-batch command copies multiple blobs to a blob container.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-blobs>

<https://docs.microsoft.com/en-us/azure/storage/common/storage-ref-azcopy-copy>

Question: 207

CertyIQ

HOTSPOT

-

You have an Azure subscription that contains a storage account named storage1. The storage1 account contains a container named container1.

You need to create a lifecycle management rule for storage1 that will automatically move the blobs in container1 to the lowest-cost tier after 90 days.

How should you complete the rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

```
{  
  "rules": [  
    {  
      "enabled": true,  
      "name": "rule1",  
      "type": "Lifecycle",  
      "definition": {  
        "actions": {  
          "baseBlob": {  
            "enableAutoTierToHotFromCool":{  
              "tierToArchive":{  
                "tierToCool":{  
                  "daysAfterModificationGreaterThan": 90  
                }  
              }  
            }  
          }  
        }  
      }  
    }  
  ]  
}  
***  
  "filters": {  
    "blobIndexMatch": [  
      "blobTypes": [  
        "prefixMatch": [  
          "container1/"  
        ]  
      ]  
    ]  
  }  
***
```

Answer:

```
{  
  "rules": [  
    {  
      "enabled": true,  
      "name": "rule1",  
      "type": "Lifecycle",  
      "definition": {  
        "actions": {  
          "baseBlob": {  
            "enableAutoTierToHotFromCool":{  
              "tierToArchive":{  
                "tierToCool":{  
                  "daysAfterModificationGreaterThanOrEqual": 90  
                }  
              }  
            }  
          }  
        }  
      }  
    }  
  ]  
}
```

Explanation:

tierToArchive and prefixMatch

- tierToArchive because it's the lowest cost tier, and doesn't say anything about needing to read data after 90 days. However, rehydration costs will occur if they did need to read it.

- prefixMatch because we only want the blob in the container1.

You have an Azure subscription that contains a virtual machine named VM1.

You need to back up VM1. The solution must ensure that backups are stored across three availability zones in the primary region.

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.

Actions	Answer Area
Configure a replication policy.	
Set Replication to Zone-redundant storage (ZRS) .	
For VM1, create a backup policy and configure the backup.	
Set Replication to Locally-redundant storage (LRS) .	
Create a Recovery Services vault.	

Answer:

Actions	Answer Area
Configure a replication policy.	Create a Recovery Services vault.
Set Replication to Zone-redundant storage (ZRS) .	
For VM1, create a backup policy and configure the backup.	
Set Replication to Locally-redundant storage (LRS) .	
Create a Recovery Services vault.	

Explanation:

1. Create a Recovery Services vault: This is the first step to set up a backup solution in Azure. The Recovery Services vault will store the backup data.
2. Set Replication to Zone redundant storage (ZRS): This ensures that the backup data is replicated across three availability zones in the primary region, providing high availability and durability.
3. For VM1, create a backup policy and configure the backup: This step involves creating a backup policy that defines the schedule and retention of the backups, and then applying this policy to VM1 to start the backup process.

Question: 209

CertyIQ

You have an Azure subscription named Subscription1.

You have 5 TB of data that you need to transfer to Subscription1.

You plan to use an Azure Import/Export job.

What can you use as the destination of the imported data?

- A. an Azure Cosmos DB database
- B. Azure File Storage
- C. Azure SQL Database
- D. a virtual machine

Answer: B

Explanation:

<https://learn.microsoft.com/en-us/azure/import-export/storage-import-export-service>

Azure Import/Export service is used to securely import large amounts of data to Azure Blob storage and Azure Files by shipping disk drives to an Azure datacenter. This service can also be used to transfer data from Azure Blob storage to disk drives and ship to your on-premises sites. Data from one or more disk drives can be imported either to Azure Blob storage or Azure Files.

Question: 210**CertyIQ**

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

Name	Type
storage1	Storage account
container1	Blob container
table1	Storage table

You need to perform the tasks shown in the following table.

Name	Type
Task1	Create a new storage account.
Task2	Upload an append blob to container1.
Task3	Create a file share in storage1.
Task4	Add data to table1.

Which tasks can you perform by using Azure Storage Explorer?

- A. Task1 and Task3 only
- B. Task1, Task2, and Task3 only
- C. Task1, Task3, and Task4 only
- D. Task2, Task3, and Task4 only
- E. Task1, Task2, Task3, and Task4

Answer: D**Explanation:**

Azure Storage Explorer cannot be used to create a storage account. It is a tool designed to manage and interact with existing Azure storage accounts and their associated resources, such as blobs, files, queues, and tables. However, it does not have the functionality to create storage accounts.

Question: 211**CertyIQ**

HOTSPOT

-

You have an Azure AD user named User1 and a read-access geo-redundant storage (RA-GRS) account named

contoso2023.

You need to meet the following requirements:

- User1 must be able to write blob data to contoso2023.
- The contoso2023 account must fail over to its secondary endpoint.

Which two settings should you configure? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.



contoso2023



Storage account

Search (Ctrl+ /)

Diagnose and solve problems

Access Control (IAM)

Data migration

Events

Storage browser

Data storage

Containers

File shares

Queues

Tables

Security + networking

Networking

Azure CDN

Advanced blade

 Access Keys

 Shared access signature

 Encryption

 Microsoft Defender for Cloud

Data management

 Geo-replication

 Data protection

 Object replication

 Blob inventory

 Static website

 Lifecycle management

Answer:



contoso2023



Storage account

 Search (Ctrl+ /)

 Diagnose and solve problems

 Access Control (IAM)

 Data migration

 Events

 Storage browser

Data storage

 Containers

 File shares

 Queues

 Tables

Security + networking

 Networking

 Azure CDN

 Access keys

 Shared access signature

 Encryption

 Microsoft Defender for Cloud

Data management

 Geo-replication

 Data protection

 Object replication

 Blob inventory

 Static website

 Lifecycle management

Explanation:

1. Access Control (IAM).

Located under the "Diagnose and solve problems" section.

IAM (Identity and Access Management) allows role-based access control (RBAC) for managing permissions to the storage account.

2. Geo-replication.

Found under "Data management" settings.

This feature is used for replicating storage account data across different Azure regions to ensure high availability and disaster recovery.

CertyIQ

Question: 212

You have an Azure subscription that contains a storage account named storage1.

You plan to create a blob container named container1.

You need to use customer-managed key encryption for container1.

Which key should you use?

- A. an EC key that uses the P-384 curve only
- B. an EC key that uses the P-521 curve only
- C. an EC key that uses the P-384 curve or P-521 curve only
- D. an RSA key with a key size of 4096 only
- E. an RSA key type with a key size of 2048, 3072, or 4096 only

Answer: E

Explanation:

E: an RSA key type with a key size of 2048, 3072, or 4096 only.

For Azure Storage accounts, customer-managed keys (CMK) can be used for encryption. When using CMKs, Azure supports RSA keys with key sizes of 2048, 3072, or 4096 bits. These keys can be managed in Azure Key Vault and used to encrypt and decrypt data in your storage account.

CertyIQ

Question: 213

HOTSPOT

-

You have an Azure subscription that contains a user named User1 and a storage account named storage1. The storage1 account contains the resources shown in the following table.

Name	Type
container1	Container
folder1	File share
Table1	Table

User1 is assigned the following roles for storage1:

- Storage Blob Data Reader
- Storage Table Data Contributor
- Storage File Data SMB Share Contributor

For storage1, you create a shared access signature (SAS) named SAS1 that has the settings shown in the following exhibit. (Click the Exhibit tab.)

Allowed services ⓘ

Blob File Queue Table

Allowed resource types ⓘ

Service Container Object

Allowed permissions ⓘ

Read Write Delete List Add Create Update Process

Immutable storage

Blob versioning permissions ⓘ

Enables deletion of versions

Allowed blob index permissions ⓘ

Read/Write Filter

Start and expiry date/time ⓘ

Start

12:00:00 PM

End

12:00:00 PM

(UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague

Allowed IP addresses ⓘ

For example, 168.1.5.65 or 168.1.5.65-168.1.5.70

Allowed protocols ⓘ

HTTPS only HTTPS and HTTP

Preferred routing tier ⓘ

Basic (default) Microsoft network routing Internet routing

i Some routing options are disabled because the endpoints are not published.

Signing key ⓘ

Generate SAS and connection string

To which resources can User1 write by using SAS1 and key1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

key1:

- Table1 only
- Table1 and container1 only
- folder1 and Table1 only
- folder1 and container1 only
- Table1, folder1, and container1

SAS1:

- Table1 only
- Table1 and container1 only
- folder1 and Table1 only
- folder1 and container1 only
- Table1, folder1, and container1

Answer:

Answer Area

key1:

- Table1 only
- Table1 and container1 only
- folder1 and Table1 only
- folder1 and container1 only
- Table1, folder1, and container1

SAS1:

- Table1 only
- Table1 and container1 only
- folder1 and Table1 only
- folder1 and container1 only
- Table1, folder1, and container1

Explanation:

key1: Table1, folder1, and container1.

SAS1: Table1 only.

When you create a storage account, Azure generates two 512-bit storage account access keys for that account. These keys can be used to authorize access to data in your storage account via Shared Key authorization.

Your storage account access keys are similar to a root password for your storage account. Always be careful to protect your access keys.

Question: 214

CertyIQ

HOTSPOT

You have an Azure subscription that contains the storage account shown in the following exhibit.

The screenshot shows the 'Access policy' section of the Azure Storage Container settings. On the left, there's a sidebar with icons for Overview, Diagnose and solve problems, Access Control (IAM), Shared access tokens, Access policy (selected), Properties, and Metadata. The main area has tabs for 'Stored access policies' and 'Immutable blob storage'. Under 'Stored access policies', there are two entries: 'Policy1' (Identifier: Policy1, Start time: Not specified, Expiry time: Not specified, Permissions: rcw) and 'Policy2' (Identifier: Policy2, Start time: Not specified, Expiry time: Not specified, Permissions: c). Under 'Immutable blob storage', there's a single entry: 'Time-based retention' (Scope: Container, Retention interval: 14 days, State: Unlocked).

Identifier	Start time	Expiry time	Permissions	...
Policy1			rcw	...
Policy2			c	...

Identifier	Scope	Retention interval	State	...
Time-based retention	Container	14 days	Unlocked	...

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

NOTE: Each correct selection is worth one point.

Answer Area

The maximum number of additional stored access policies that you can create for container1 is [answer choice].

0
1
3
5
6

The maximum number of additional immutable blob storage policies that you can create for container1 is [answer choice].

0
1
2
4
5

Answer:

Answer Area

The maximum number of additional stored access policies that you can create for container1 is [answer choice].

0
1
3
5
6

The maximum number of additional immutable blob storage policies that you can create for container1 is [answer choice].

0
1
2
4
5

Explanation:

Max stored access policies: 3, because max total of stored access policy is 5 and we already have 2, so additional 3 available.

Max immutable blob storage: 1, because max total of immutable blob storage policy is 2 - one Legal hold policy and one Time-based retention policy. We already have one, so additional 1 available.

Question: 215

CertyIQ

You have an Azure subscription named Subscription1.

You have 5 TB of data that you need to transfer to Subscription1.

You plan to use an Azure Import/Export job.

What can you use as the destination of the imported data?

- A. Azure Blob Storage
- B. Azure Data Lake Store
- C. Azure SQL Database
- D. a virtual machine

Answer: A

Explanation:

Azure Import/Export service is used to securely import large amounts of data to Azure Blob storage and Azure Files by shipping disk drives to an Azure datacenter. This service can also be used to transfer data from Azure Blob storage to disk drives and ship to your on-premises sites. Data from one or more disk drives can be imported either to Azure Blob storage or Azure Files. The maximum size of an Azure Files Resource of a file share is 5 TB.

Note: There are several versions of this question in the exam. The question has two correct answers:

- 1. Azure File Storage

or

- 2. Azure Blob Storage

Question: 216

CertyIQ

You have an Azure subscription. The subscription contains a storage account named storage1 that has the lifecycle management rules shown in the following table.

Name	If base blobs were last modified more than (days)	Then
Rule1	5 days	Move to cool storage
Rule2	5 days	Delete the blob
Rule3	5 days	Move to archive storage

On June 1, you store a blob named File1 in the Hot access tier of storage1.

What is the state of File1 on June 7?

- A. stored in the Cool access tier
- B. stored in the Archive access tier
- C. stored in the Hot access tier
- D. deleted

Answer: D

Explanation:

If you define more than one action on the same blob, lifecycle management applies the least expensive action to the blob. For example, action delete is cheaper than action tierToArchive. Action tierToArchive is cheaper than action tierToCool.

<https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-overview>

HOTSPOT

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

Name	Kind	Redundancy
storage1	StorageV2	Geo-zone-redundant storage (GZRS)
storage2	BlobStorage	Read-access geo-redundant storage (RA-GRS)
storage3	BlockBlobStorage	Zone-redundant storage (ZRS)

You need to identify which storage accounts support lifecycle management, and which storage accounts support moving data to the Archive access tier.

Which storage accounts should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Lifecycle management:

- storage1 only
- storage2 only
- storage1 and storage3 only
- storage2 and storage3 only
- storage1, storage2, and storage3

The Archive access tier:

- storage1 only
- storage2 only
- storage1 and storage3 only
- storage2 and storage3 only
- storage1, storage2, and storage3

Answer:

Answer Area

Lifecycle management:

- storage1 only
- storage2 only
- storage1 and storage3 only
- storage2 and storage3 only
- storage1, storage2, and storage3**

The Archive access tier:

- storage1 only
- storage2 only**
- storage1 and storage3 only
- storage2 and storage3 only
- storage1, storage2, and storage3

Explanation:

1 - storage1, storage2, storage3

Lifecycle management policies are supported for block blobs and append blobs in general-purpose v2, premium block blob, and Blob Storage accounts.

2 - storage2 only.

Only storage accounts that are configured for LRS, GRS, or RA-GRS support moving blobs to the archive tier. The archive tier isn't supported for ZRS, GZRS, or RA-GZRS accounts.

<https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-overview>

<https://learn.microsoft.com/en-us/azure/storage/blobs/access-tiers-overview>

Question: 218

CertyIQ

You have an Azure subscription named Subscription1.

You have 5 TB of data that you need to transfer to Subscription1.

You plan to use an Azure Import/Export job.

What can you use as the destination of the imported data?

- A. an Azure Cosmos DB database
- B. Azure Data Lake Store
- C. Azure Blob storage
- D. Azure Data Factory

Answer: C

Explanation:

<https://learn.microsoft.com/en-us/azure/import-export/storage-import-export-service>

Azure Import/Export service is used to securely import large amounts of data to Azure Blob storage and Azure Files by shipping disk drives to an Azure datacenter. This service can also be used to transfer data from Azure Blob storage to disk drives and ship to your on-premises sites. Data from one or more disk drives can be imported either to Azure Blob storage or Azure Files.

Question: 219

CertyIQ

HOTSPOT

-

You have an Azure subscription that contains a storage account named storage1. The storage1 account contains a container named container1.

You create a blob lifecycle rule named rule1.

You need to configure rule1 to automatically move blobs that were NOT updated for 45 days from contained to the Cool access tier.

How should you complete the rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

```
{  
  "rules": [  
    {  
      "enabled": true,  
      "name": "rule1",  
      "type": "Lifecycle",  
      "definition": {  
        "actions": {  
          "baseBlob": {  
            "tierToCool": {  
              "daysAfterCreationGreater Than"  
              "daysAfterLastAccessTimeGreater Than"  
              "daysAfterModificationGreater Than"  
            }  
          }  
        },  
        "filters": {  
          "blobTypes": [  
            "AppendBlob"  
            "Blockblob"  
            "Pageblob"  
          ],  
          "prefixMatch": [  
            "container1"  
          ]  
        }  
      }  
    }  
  ]  
}
```

Answer:

Answer Area

```
{  
  "rules": [  
    {  
      "enabled": true,  
      "name": "rule1",  
      "type": "Lifecycle",  
      "definition": {  
        "actions": {  
          "baseBlob": {  
            "tierToCool": {  
              "daysAfterModificationGreaterThan": 45  
            }  
          }  
        }  
      },  
      "filters": {  
        "blobTypes": [  
          "AppendBlob",  
          "Blockblob",  
          "Pageblob"  
        ],  
        "prefixMatch": [  
          "container1"  
        ]  
      }  
    }  
  ]  
}
```

Explanation:

1. daysAfterModificationGreaterThan
2. Blockblob

<https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-overview#rule-actions>

daysAfterModificationGreaterThan

- The condition for actions on a current version of a blob

Tiering is not yet supported in a premium block blob storage account. For all other accounts, tiering is allowed only on block blobs and not for append and page blobs.

tierToCool

- Supported for blockBlob

Question: 220

CertyIQ

You have an Azure subscription named Subscription1.

You have 5 TB of data that you need to transfer to Subscription1.

You plan to use an Azure Import/Export job.

What can you use as the destination of the imported data?

- A.an Azure Cosmos DB database
- B.Azure Blob Storage
- C.Azure SQL Database
- D.the Azure File Sync Storage Sync Service

Answer: B

Explanation:

<https://learn.microsoft.com/en-us/azure/import-export/storage-import-export-service> Azure Import/Export service is used to securely import large amounts of data to Azure Blob storage and Azure Files by shipping disk drives to an Azure datacenter. This service can also be used to transfer data from Azure Blob storage to disk drives and ship to your on-premises sites. Data from one or more disk drives can be imported either to Azure Blob storage or Azure Files.

Question: 221

CertyIQ

You plan to create an Azure Storage account named storage1 that will contain a file share named share1.

You need to ensure that share1 can support SMB Multichannel. The solution must minimize costs.

How should you configure storage?

- A.Premium performance with locally-redundant storage (LRS)
- B.Standard performance with zone-redundant storage (ZRS)
- C.Premium performance with geo-redundant storage (GRS)
- D.Standard performance with locally-redundant storage (LRS)

Answer: A

Explanation:

A: Premium performance with locally-redundant storage (LRS).

Premium Performance.

Premium file shares in Azure Storage provide high-performance, low-latency storage, which is necessary to support the SMB Multichannel feature. Standard performance tiers do not support this feature.

Locally-Redundant Storage (LRS).

Locally-redundant storage (LRS) is the most cost-effective redundancy option for Azure Storage. It replicates your data within a single datacenter in the region and is less expensive compared to geo-redundant storage (GRS) and zone-redundant storage (ZRS).

CertyIQ

Question: 222

You have an Azure subscription named Subscription1.

You have 5 TB of data that you need to transfer to Subscription1.

You plan to use an Azure Import/Export job.

What can you use as the destination of the imported data?

- A. Azure Data Lake Store
- B. Azure File Storage
- C. Azure SQL Database
- D. the Azure File Sync Storage Sync Service

Answer: B

Explanation:

Azure Import/Export service is used to securely import large amounts of data to Azure Blob storage and Azure Files by shipping disk drives to an Azure datacenter. This service can also be used to transfer data from Azure Blob storage to disk drives and ship to your on-premises sites. Data from one or more disk drives can be imported either to Azure Blob storage or Azure Files.

Reference:

<https://learn.microsoft.com/en-us/azure/import-export/storage-import-export-service>

Question: 223

CertyIQ

You have an Azure subscription that contains a storage account named storage1.

You plan to use conditions when assigning role-based access control (RBAC) roles to storage1.

Which storage1 services support conditions when assigning roles?

- A.containers only
- B.file shares only
- C.tables only
- D.queues only
- E.containers and queues only
- F.files shares and tables only

Answer: E

Explanation:

containers and queues only.

"Currently, conditions can be added to built-in or custom role assignments that have blob storage or queue storage data actions."

<https://learn.microsoft.com/en-us/azure/role-based-access-control/conditions-overview#where-can-conditions-be-added>

Question: 224

CertyIQ

HOTSPOT

You have an Azure subscription that contains the resource groups shown in the following table.

Name	Region
RG1	West US
RG2	West US
RG3	East US

The subscription contains the virtual networks shown in the following table.

Name	Resource group	Region	Subnet	Subnet IP address space
VNet1	RG1	West US	Subnet1	10.1.0.0/16
VNet2	RG2	Central US	Subnet2	10.2.0.0/24
VNet3	RG3	East US	Subnet3	10.3.0.0/24

You plan to deploy the Azure Kubernetes Service (AKS) clusters shown in the following table.

Name	Resource group	Region	Number of nodes	Network configuration
AKS1	RG1	West US	30	Azure Container Network Interface (CNI)
AKS2	RG2	West US	100	Azure Container Network Interface (CNI)
AKS3	RG3	East US	50	Kubenet

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
You can deploy AKS1 to VNet2.	<input type="radio"/>	<input type="radio"/>
You can deploy AKS2 to VNet1.	<input type="radio"/>	<input type="radio"/>
You can deploy AKS3 to VNet3.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
You can deploy AKS1 to VNet2.	<input type="radio"/>	<input checked="" type="radio"/>
You can deploy AKS2 to VNet1.	<input checked="" type="radio"/>	<input type="radio"/>
You can deploy AKS3 to VNet3.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

NNY

VNET is created by default but we can connect to an existing VNET"you can create an AKS cluster that uses kubenet and connect to an existing virtual network subnet""With kubenet, a route table must exist on your cluster subnet(s). AKS supports bringing your own existing subnet and route table.

"<https://learn.microsoft.com/en-us/azure/aks/configure-kubenet>

You plan to deploy several Azure virtual machines that will run Windows Server 2019 in a virtual machine scale set by using an Azure Resource Manager template.

You need to ensure that NGINX is available on all the virtual machines after they are deployed.

What should you use?

- A. the Publish-AzVMDscConfiguration cmdlet
- B. Azure Application Insights
- C. a Desired State Configuration (DSC) extension
- D. Azure AD Application Proxy

Answer: C

Explanation:

Answer is C) a Desired State Configuration (DSC) extension

To ensure that NGINX is available on all the virtual machines in a virtual machine scale set, you can use the Desired State Configuration (DSC) extension.

Option A (the Publish-AzVMDscConfiguration cmdlet) is used to generate a configuration file for DSC.

Option B (Azure Application Insights) is a monitoring service that provides application performance and availability telemetry.

Option D (Azure AD Application Proxy) is a service that enables remote access to on-premises applications.

Therefore, the correct option for this scenario is C: a Desired State Configuration (DSC) extension. The DSC extension can be used to configure and manage the state of the virtual machines in the virtual machine scale set, including the installation of NGINX.

Question: 226

CertyIQ

HOTSPOT

You have an Azure subscription that has offices in the East US and West US Azure regions.

You plan to create the storage account shown in the following exhibit.

Create a storage account

Basics	Advanced	Networking	Data protection	Encryption	Tags	Review
Basics						
Subscription				Azure subscription 1		
Resource Group				RG1		
Location				eastus		
Storage account name				adatum22		

Deployment model	Resource manager
Performance	Premium
Premium account type	File shares
Replication	Zone-redundant storage (ZRS)

Advanced

Secure transfer	Enabled
Allow storage account key access	Enabled
Allow cross-tenant replication	Disabled
Default to Azure Active Directory authorization in the Azure portal	Disabled
Blob public access	Enabled
Minimum TLS version	Version 1.2
Permitted scope for copy operations (preview)	From any storage account
Enable hierarchical namespace	Disabled
Enable network file system v3	Disabled
Enable SFTP	Disabled
Large file shares	Disabled

Networking

Network connectivity	Public endpoint (all networks)
Default routing tier	Microsoft network routing
Endpoint type	Standard

Data protection

Point-in-time restore	Disabled
Blob soft delete	Disabled
Container soft delete	Disabled
File share soft delete	Enabled
File share retention period in days	7
Versioning	Disabled
Blob change feed	Disabled
Version-level immutability support	Disabled

Encryption

Encryption type	Microsoft-managed keys (MMK)
Enable support for customer-managed keys	Blobs and files only
Enable infrastructure encryption	Disabled

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

NOTE: Each correct selection is worth one point.

Answer Area

To minimize the network costs of accessing adatum22, modify the [answer choice] setting.

- Default routing tier
- Endpoint type
- Location
- Network connectivity
- Performance

After adatum22 is created, you can modify the [answer choice] setting.

- Enable infrastructure encryption
- Enable support for customer-managed keys
- Encryption type
- Premium account type

Answer:

Answer Area

To minimize the network costs of accessing adatum22, modify the [answer choice] setting.

- Default routing tier
- Endpoint type
- Location
- Network connectivity
- Performance

After adatum22 is created, you can modify the [answer choice] setting.

- Enable infrastructure encryption
- Enable support for customer-managed keys
- Encryption type
- Premium account type

Explanation:

1. Default Routing Tier

The default routing tier influences how network traffic is managed and priced.

Choosing an appropriate routing tier helps reduce egress (outbound) data transfer costs.

Some tiers optimize data delivery based on cost-efficient paths, ensuring lower expenses for accessing resources.

Often used in cloud environments like Microsoft Azure or Google Cloud, where routing options affect data transfer pricing.

2. Enable Support for Customer-Managed Keys.

Customer-managed keys (CMKs) allow users to control encryption keys rather than relying on provider-managed encryption.

Organizations needing higher security and compliance (such as GDPR, HIPAA) can enforce their own key management policies.

Provides enhanced security by ensuring that only authorized users can access or decrypt stored data.

This setting is usually modifiable after the initial creation of a storage account or database in cloud platforms.

Question: 227

CertyIQ

HOTSPOT

-

You have an Azure subscription.

You plan to deploy a new storage account.

You need to configure encryption for the account. The solution must meet the following requirements:

- Use a customer-managed key stored in a key vault.
- Use the maximum supported bit length.

Which type of key and which bit length should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Key:

AES
3DES
RSA

Bit length:

2048
3072
4096
8192

Answer:

Answer Area

Key:

AES
3DES
RSA

Bit length:

2048
3072
4096
8192

Explanation:

Key: **RSA**.

RSA is an asymmetric cryptographic algorithm widely used for secure data transmission.

It relies on the mathematical difficulty of factoring large prime numbers.

RSA is commonly used for encryption, digital signatures, and key exchange in secure communication protocols.

Bit Length :**4096**

The bit length determines the security strength of the RSA key.

A 4096-bit RSA key is considered highly secure for most applications, as it provides strong resistance against brute-force attacks.

Longer key lengths increase security but also require more computational power for encryption and decryption.

Question: 228

CertyIQ

You have an Azure Storage account that contains 5,000 blobs accessed by multiple users.

You need to ensure that the users can view only specific blobs based on blob index tags.

What should you include in the solution?

- A.a role assignment condition
- B.a stored access policy
- C.just-in-time (JIT) VM access
- D.a shared access signature (SAS)

Answer: A

Explanation:

A. A Role Assignment Condition.

Azure Storage supports Azure RBAC (Role-Based Access Control) with role assignment conditions, allowing administrators to grant access based on blob index tags. This means users can only view specific blobs that match the conditions defined in the role assignment.

CertyIQ

Question: 229

You have an Azure Storage account named storage1.

For storage1, you create an encryption scope named Scope1.

Which storage types can you encrypt by using Scope?

- A.file shares only
- B.containers only
- C.file shares and containers only
- D.containers and tables only
- E.file shares, containers, and tables only
- F.file shares, containers, tables, and queues

Answer: B

Explanation:

Containers only.

Encryption scopes enable you to manage encryption at the level of an individual blob or container.

The encryption scope in Azure Storage is available for Azure Blob / Data Lake Gen2 storage account1. The key that protects an encryption scope may be either a Microsoft-managed key or a customer-managed key in Azure Key Vault1. containers only as blobs are stored in containers in Azure Blob Storage.

Reference:

<https://learn.microsoft.com/en-us/azure/storage/blobs/encryption-scope-manage?tabs=portal>

CertyIQ

Question: 230

HOTSPOT

-

You have an Azure subscription.

You plan to create a role definition to meet the following requirements:

- Users must be able to view the configuration data of a storage account.
- Users must be able to perform all actions on a virtual network.
- The solution must use the principle of least privilege.

What should you include in the role definition for each requirement? To answer, select the appropriate options in

the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Perform all actions on a virtual network:

"Microsoft.Network/virtualNetworks/*"
"Microsoft.Network/virtualNetworks/delete"
"Microsoft.Network/virtualNetworks/write"

View the configuration data of a storage account:

"Microsoft.Storage/StorageAccounts/*"
"Microsoft.Storage/StorageAccounts/read"
"Microsoft.Storage/StorageAccounts/blobServices/containers/blob/read"

Answer:

Answer Area

Perform all actions on a virtual network:

"Microsoft.Network/virtualNetworks/*"
"Microsoft.Network/virtualNetworks/delete"
"Microsoft.Network/virtualNetworks/write"

View the configuration data of a storage account:

"Microsoft.Storage/StorageAccounts/*"
"Microsoft.Storage/StorageAccounts/read"
"Microsoft.Storage/StorageAccounts/blobServices/containers/blob/read"

Explanation:

1. Perform All Actions on a Virtual Network

"Microsoft.Network/virtualNetworks/*"

The asterisk (*) is a wildcard, which means full access to all operations on virtual networks.

This permission includes:

Creating, updating, and deleting virtual networks.

Managing subnets, peerings, and network configurations.

This is typically assigned to network administrators who need complete control over Azure Virtual Networks.

2. View the Configuration Data of a Storage Account

"Microsoft.Storage/storageAccounts/read"

This permission allows users to view (but not modify) the configuration and properties of a storage account.

This does not grant access to read/write data inside the storage account (such as blobs or files).

It is useful for auditors, monitoring teams, or read-only users who need to check storage settings without

making changes.

CertyIQ

Question: 231

You have an Azure subscription named Subscription1.

You have 5 TB of data that you need to transfer to Subscription1.

You plan to use an Azure Import/Export job.

What can you use as the destination of the imported data?

- A.Azure Data Factory
- B.the Azure File Sync Storage Sync Service
- C.Azure File Storage
- D.Azure SQL Database

Answer: C

Explanation:

Correct Answer: C

Azure Import/Export service is used to securely import large amounts of data to Azure Blob storage and Azure Files by shipping disk drives to an Azure datacenter. This service can also be used to transfer data from Azure Blob storage to disk drives and ship to your on-premises sites. Data from one or more disk drives can be imported either to Azure Blob storage or Azure Files. The maximum size of an Azure Files Resource of a file share is 5 TB.

Note: There are several versions of this question in the exam. The question has two correct answers:

1. Azure File Storage

or

2. Azure Blob Storage

The question can have other incorrect answer options, including the following:

- ⇒ Azure Data Lake Store
- ⇒ Azure SQL Database
- ⇒ Azure Data Factory

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-service>

Question: 232

CertyIQ

HOTSPOT

-

You have an Azure subscription that contains a virtual machine named VM1.

To VM1, you plan to add a 1-TB data disk that meets the following requirements:

- Provides data resiliency in the event of a datacenter outage.
- Provides the lowest latency and the highest performance.
- Ensures that no data loss occurs if a host fails.

You need to recommend which type of storage and host caching to configure for the new data disk.

Answer Area

Storage type:

Premium SSD that uses locally-redundant storage (LRS)
Premium SSD that uses zone-redundant storage (ZRS)
Standard SSD that uses locally-redundant storage (LRS)
Standard SSD that uses zone-redundant storage (ZRS)

Host caching:

None
Read-only
Read/Write

Answer:

Answer Area

Storage type:

Premium SSD that uses locally-redundant storage (LRS)
Premium SSD that uses zone-redundant storage (ZRS)
Standard SSD that uses locally-redundant storage (LRS)
Standard SSD that uses zone-redundant storage (ZRS)

Host caching:

None
Read-only
Read/Write

Explanation:

Storage type: Premium SSD that uses zone-redundant storage (ZRS)

Host-caching: Read-only

Rationale ZRS replicates to different locations Host caching: Write cache stores information in memory, no host, no memory, no dataRedundancy options for Azure managed disks - Azure Virtual Machines | Microsoft Learn
Enable and configure Azure VM disk cache with the Azure portal - Training | Microsoft Learn

Question: 233

You have an Azure virtual machine named VM1 and an Azure key vault named Vault1.

On VM1, you plan to configure Azure Disk Encryption to use a key encryption key (KEK).

You need to prepare Vault1 for Azure Disk Encryption.

Which two actions should you perform on Vault1? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A.Select Azure Virtual machines for deployment.
- B.Create a new key.
- C.Create a new secret.
- D.Configure a key rotation policy.
- E.Select Azure Disk Encryption for volume encryption.

Answer: BE**Explanation:**

B. Create a new key.

Azure Disk Encryption with KEK requires a key in the Key Vault to encrypt the disk encryption key (DEK). Therefore, you need to create a key in the key vault.

E. Select Azure Disk Encryption for volume encryption.

You need to select Azure Disk Encryption as it will integrate the key vault with the disk encryption process.

Question: 234

You have an Azure subscription that contains a virtual machine named VM1 and an Azure key vault named KV1.

You need to configure encryption for VM1. The solution must meet the following requirements:

- Store and use the encryption key in KV1.
- Maintain encryption if VM1 is downloaded from Azure.
- Encrypt both the operating system disk and the data disks.

Which encryption method should you use?

- A.customer-managed keys
- B.Confidential disk encryption
- C.Azure Disk Encryption
- D.encryption at host

Answer: C**Explanation:**

You can protect your managed disks by using Azure Disk Encryption for Linux VMs, which uses DM-Crypt, or Azure Disk Encryption for Windows VMs, which uses Windows BitLocker, to protect both operating system disks and data disks with full volume encryption.

Encryption keys and secrets are safeguarded in your Azure Key Vault subscription. By using the Azure Backup

service, you can back up and restore encrypted virtual machines (VMs) that use Key Encryption Key (KEK) configuration.

Reference:

<https://learn.microsoft.com/en-us/azure/security/fundamentals/encryption-overview>

Question: 235

CertyIQ

HOTSPOT

-

You have an Azure subscription that contains a storage account named storage1.

You need to configure a shared access signature (SAS) to ensure that users can only download blobs securely by name.

Which two settings should you configure? To answer, select the appropriate settings in the answer area.

NOTE: Each correct answer is worth one point.

Answer Area

Allowed services (radio button)

Blob File Queue Table

Allowed resource types (radio button)

Service Container Object

Allowed permissions (radio button)

Read Write Delete List Add Create Update Process Immutable storage Permanent delete

Blob versioning permissions (radio button)

Enables deletion of versions

Allowed blob index permissions (radio button)

Read/Write Filter

Start and expiry date/time (radio button)

Answer:

Answer Area

Allowed services: Blob File Queue Table

Allowed resource types: Service Container Object

Allowed permissions: Read Write Delete List Add Create Update Process Immutable storage Permanent delete

Blob versioning permissions: Enables deletion of versions

Allowed blob index permissions: Read/Write Filter

Start and expiry date/time:

Explanation:

Allowed resource types: Object (you want users to access a specific blob by name).

Allowed permissions: Read (to allow downloading).

CertyIQ

Question: 236

You have an Azure subscription that contains a storage account named storage1. The storage1 account contains a container named container1.

You need to configure access to container1. The solution must meet the following requirements:

- Only allow read access.
- Allow both HTTP and HTTPS protocols.
- Apply access permissions to all the content in the container.

What should you use?

- A.an access policy
- B.a shared access signature (SAS)
- C.Azure Content Delivery Network (CDN)
- D.access keys

Answer: B

Explanation:

B. a shared access signature (SAS)

Shared Access Signatures (SAS) are used to grant limited access to specific resources in your storage account while maintaining fine-grained control over the allowed operations, including read access. You can create a SAS token with the necessary permissions and then provide this token to the users or applications that need access to the container.

Question: 237

CertyIQ

You need to create an Azure Storage account named storage1. The solution must meet the following requirements:

- Support Azure Data Lake Storage.
- Minimize costs for infrequently accessed data.
- Automatically replicate data to a secondary Azure region.

Which three options should you configure for storage1? Each correct answer presents part of the solution.

NOTE: Each correct answer is worth one point.

- A.zone-redundant storage (ZRS)
- B.the Cool access tier
- C.geo-redundant storage (GRS)
- D.the Hot access tier
- E.hierarchical namespace

Answer: BCE

Explanation:

- B. The Cool access tier: The Cool access tier is suitable for infrequently accessed data and offers lower storage costs compared to the Hot access tier.
- C. Geo-redundant storage (GRS): Geo-redundant storage replicates data to a secondary Azure region, providing data redundancy and disaster recovery capabilities.
- E. Hierarchical namespace: The hierarchical namespace is required for Azure Data Lake Storage, as it enables the storage account to support the data lake's file system structure.

Question: 238

CertyIQ

HOTSPOT

-

You have an Azure Storage account named storage1 that contains two containers named container1 and container2. Blob versioning is enabled for both containers.

You periodically take blob snapshots of critical blobs.

You create the following lifecycle management policy.

```
{  
  "rules": [  
    {  
      "enabled": true,  
      "name": "rule1",  
      "type": "Lifecycle",  
      "definition": {  
        "actions": {  
          "version": {  
            "tierToCool": {  
              "daysAfterCreationGreaterThanOrEqual": 15  
            },  
            "tierToArchive": {  
              "daysAfterLastTierChangeGreaterThanOrEqual": 7,  
              "daysAfterCreationGreaterThanOrEqual": 30  
            }  
          }  
        },  
        "filters": {  
          "blobTypes": [  
            "blockBlob"  
          ],  
          "prefixMatch": [  
            "container1/"  
          ]  
        }  
      }  
    }  
  ]  
}
```

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
A blob snapshot automatically moves to the Cool access tier after 15 days.	<input type="radio"/>	<input type="radio"/>
A blob version in container2 automatically moves to the Archive access tier after 30 days.	<input type="radio"/>	<input type="radio"/>
A rehydrated version automatically moves to the Archive access tier after 30 days.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
A blob snapshot automatically moves to the Cool access tier after 15 days.	<input checked="" type="radio"/>	<input type="radio"/>
A blob version in container2 automatically moves to the Archive access tier after 30 days.	<input type="radio"/>	<input checked="" type="radio"/>
A rehydrated version automatically moves to the Archive access tier after 30 days.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

A blob snapshot automatically moves to the Cool access tier after 15 days.

Yes .

Incorrect Selection: Blob snapshots do not automatically move between tiers.

If an organization sets a Lifecycle Management policy, blobs can move to the Cool tier, but the minimum retention period is 30 days, not 15.

A blob version in container2 automatically moves to the Archive access tier after 30 days.

No.

Correct Selection: Blob versions do not automatically move unless a Lifecycle Policy is configured.

If a Lifecycle Policy exists, blobs can be moved to Archive after a set period, but this is not the default behavior.

A rehydrated version automatically moves to the Archive access tier after 30 days.

No.

Correct Selection: Rehydrated blobs do not automatically move back to Archive.

Once a blob is rehydrated from Archive (moved to Hot/Cool), it stays there until a new policy moves it back to Archive.

Question: 239

CertyIQ

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

Name	Kind	Performance	Replication	Access tier
storage1	Storage (general purpose v1)	Premium	Locally-redundant storage (LRS)	Not applicable
storage2	StorageV2 (general purpose v2)	Standard	Locally-redundant storage (LRS)	Cool
storage3	StorageV2 (general purpose v2)	Standard	Read-access geo-redundant storage (RA-GRS)	Hot
storage4	BlobStorage	Premium	Locally-redundant storage (LRS)	Hot

Which storage account can be converted to zone-redundant storage (ZRS) replication?

- A.storage1
- B.storage2
- C.storage3
- D.storage4

Answer: B**Explanation:**

B. storage2 to convert to ZRS must the Kind be: Standard general-purpose v2 (StorageV2), Premium block blobs (BlockBlobStorage) or Premium file shares (FileStorage) and the Replication is from LRS possible (... from GRS/RA-GRS convert to LRS first)

<https://learn.microsoft.com/en-us/azure/storage/common/storage-redundancy#supported-storage-account-types>

<https://learn.microsoft.com/en-us/azure/storage/common/redundancy-migration?tabs=portal#replication-change-table>

Question: 240

CertyIQ

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

Name	Platform
Device1	Windows
Device2	Ubuntu Linux
Device3	macOS
Device4	Android

On which devices can you install Azure Storage Explorer?

- A.Device1 only
- B.Device1 and Device2 only
- C.Device1 and Device3 only
- D.Device1, Device2, and Device3 only
- E.Device1, Device3, and Device4 only

Answer: D

Explanation:

D: Device1, Device2, and Device3 only.

Azure Storage Explorer is compatible with Windows, macOS, and Linux operating systems, which correspond to Device1, Device2, and Device3 in this context. Device4 does not meet the requirements for Azure Storage Explorer.

Question: 241

CertyIQ

HOTSPOT

-

You have an Azure subscription.

You plan to create the Azure Storage account as shown in the following exhibit.



Home > Subscriptions > Subscription1 - Resources > New > Create storage account

Create storage account



Validation passed

[Basics](#) [Networking](#) [Advanced](#) [Tags](#) [Review + create](#)**Basics**

Subscription	Subscription1
Resource group	RG1
Location	(Europe) North Europe
Storage account name	storage16852
Deployment model	Resource manager
Account kind	StorageV2 (general purpose v2)
Replication	Locally-redundant storage (LRS)
Performance	Standard
Access tier (default)	Hot

Networking

Connectivity method	Private endpoint
Private Endpoint	(New) StorageEndpoint1 (blob) (privatelink.blob.core.windows.net)

Advanced

Secure transfer required	Enabled
Large file shares	Disabled
Blob soft delete	Disabled
Blob change feed	Disabled
Hierarchical namespace	Disabled
NFS v3	Disabled

[Create](#)

< Previous

Next >

[Download a template for automation](#)

presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

The minimum number of copies of the storage account will be [answer choice].

A dropdown menu with a white background and a thin black border. It contains four options: '1', '2', '3', and '4'. The '1' option is at the top, followed by '2', '3', and '4' at the bottom. A small downward-pointing arrow is located in the top right corner of the menu.

To reduce the cost of infrequently accessed data in the storage account, you must modify the [answer choice] setting.

A dropdown menu with a white background and a thin black border. It contains four options: 'Access tier (default)', 'Performance', 'Account kind', and 'Replication'. The 'Access tier (default)' option is at the top, followed by 'Performance', 'Account kind', and 'Replication' at the bottom. A small downward-pointing arrow is located in the top right corner of the menu.

Answer:

Answer Area

The minimum number of copies of the storage account will be [answer choice].

A dropdown menu with a white background and a thin black border. It contains four options: '1', '2', '3', and '4'. The '3' option is highlighted with a thick black square outline around its entire box. A small downward-pointing arrow is located in the top right corner of the menu.

To reduce the cost of infrequently accessed data in the storage account, you must modify the [answer choice] setting.

A dropdown menu with a white background and a thin black border. It contains four options: 'Access tier (default)', 'Performance', 'Account kind', and 'Replication'. The 'Access tier (default)' option is highlighted with a thick black square outline around its text. A small downward-pointing arrow is located in the top right corner of the menu.

Explanation:

1. Minimum Number of Copies of the Storage Account.

The selected value in the dropdown is **3**.

This likely refers to Locally Redundant Storage (LRS), which keeps three copies of the data within a single Azure region.

Other redundancy options include:

ZRS (Zone Redundant Storage): Distributes copies across three availability zones.

GRS (Geo-Redundant Storage): Replicates data across different regions.

Thus, selecting 3 is correct in this context as it aligns with Azure's replication methods.

2. Reducing the Cost of Infrequently Accessed Data

The selected value is "**Access tier (default)**".

Azure Storage offers different access tiers:

Hot Tier: Optimized for frequently accessed data.

Cool Tier: Suitable for infrequently accessed data, offering lower storage costs but higher access costs.

Archive Tier: Used for long-term data storage at the lowest cost but with high retrieval latency.

To reduce costs for infrequently accessed data, moving data from Hot to Cool or Archive tiers is the correct approach.

Question: 242

CertyIQ

HOTSPOT

-

You have an Azure Storage account named storage1 that contains a container named container1. The container1 container stores thousands of image files.

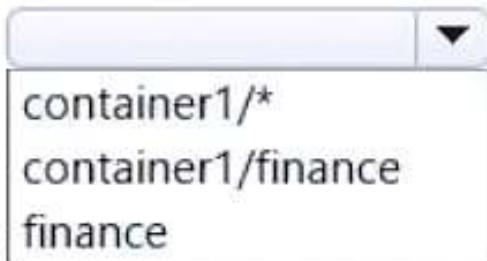
You plan to use an Azure Resource Manager (ARM) template to create a blob inventory rule named rule1.

You need to ensure that only blobs whose names start with the word finance are stored daily as a CSV file in container1.

How should you complete rule1? To answer, select the options in the answer area.

NOTE: Each correct answer is worth one point.

Answer Area

```
...  
{  
    "definition": {  
        "filters": {  
            "blobTypes":   
                ["appendBlob",  
                 "blockBlob",  
                 "pageBlob"]  
            },  
            "includeBlobVersions": true,  
            "includeSnapshots": true,  
            "prefixMatch":   
                ["container1/*",  
                 "container1/finance",  
                 "finance"]  
            },  
            "format": "string",  
            "objectType": "blob",  
            "schedule": "daily",  
            "schemaFields": ["Name"]  
        },  
        "destination": "CSV",  
        "enabled": true,  
        "name": "rule1"  
    }  
...  
}
```

Answer:

Answer Area

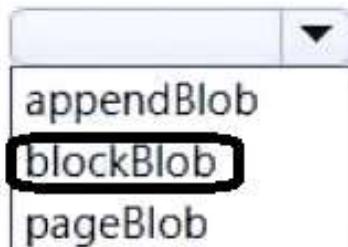
...

{

 "definition": {

 "filters": {

 "blobTypes":

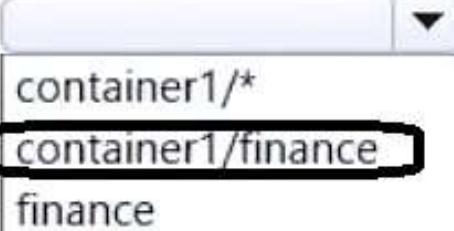


 "includeBlobVersions": true,

 "includeSnapshots": true,

 "prefixMatch":

 },



 "format": "string", finance

 "objectType": "blob",

 "schedule": "daily",

 "schemaFields": ["Name"]

 },

 "destination": "CSV",

 "enabled": true,

 "name": "rule1"

}

...

Explanation:

1. Blob Types Selection.

The "blobTypes" field defines the type of Azure Blob Storage objects to filter.

The selected option "**blockBlob**" is one of the three possible blob types:

Append Blob: Used for logging and append-only scenarios.

Block Blob :The most commonly used blob type for storing general-purpose files.

Page Blob: Used for Azure Virtual Machine disks.

Since Block Blob is the most commonly used for general storage, selecting this makes sense.

2. Prefix Match

"prefixMatch" is used to filter blobs within a specific path or folder inside a container.

The selected option "**container1/finance**" means that only blobs inside the "finance" subdirectory of "container1" will be processed.

The other option "container1/*" would include all blobs within container1, but this is more restrictive.

Since "container1/finance" is selected, it means the rule applies only to that specific subdirectory.

Question: 243

CertyIQ

HOTSPOT

-

You have an Azure subscription that contains a storage account named storage1. The storage1 account contains blobs in a container named container1.

You plan to share access to storage1.

You need to generate a shared access signature (SAS). The solution must meet the following requirements:

- Ensure that the SAS can only be used to enumerate and download blobs stored in container1.
- Use the principle of least privilege.

Which three settings should you enable? To answer, select the appropriate settings in the answer area.

Answer Area

Allowed services ⓘ
 Blob File Queue Table

Allowed resource types ⓘ
 Service Container Object

Allowed permissions ⓘ
 Read Write Delete List Add Create Update Process Immutable storage Permanent delete

Blob versioning permissions ⓘ
 Enables deletion of versions

Allowed blob index permissions ⓘ
 Read/Write Filter

Answer:

Answer Area

Allowed services ⓘ
 Blob File Queue Table

Allowed resource types ⓘ
 Service Container Object

Allowed permissions ⓘ
 Read Write Delete List Add Create Update Process Immutable storage Permanent delete

Blob versioning permissions ⓘ
 Enables deletion of versions

Allowed blob index permissions ⓘ
 Read/Write Filter

Explanation:

Allowed resource types: Container

Allowed permissions: Read and list.

Container: "Grants access to the content and metadata of any blob in the container, and to the list of blobs in the container."

Source: <https://learn.microsoft.com/en-us/rest/api/storageservices/create-user-delegation-sas#specify-the-signed-resource-field>

Specifying "Object" additionally would be redundant because it is a subset of "Container".

List: "List blobs non-recursively."

<https://learn.microsoft.com/en-us/rest/api/storageservices/create-user-delegation-sas#specify-permissions>

Satisfies the requirement of enumeration.

Read: "Read the content, blocklist, properties, and metadata of any blob in the container or directory. Use a blob as the source of a copy operation."

<https://learn.microsoft.com/en-us/rest/api/storageservices/create-user-delegation-sas#specify-permissions>

Satisfies the requirement of download.

Question: 244

CertyIQ

HOTSPOT

You have an Azure subscription. The subscription contains a storage account named storage1 that has the lifecycle management rules shown in the following table.

Name	Blob prefix	If base were last modified more than (days ago)	Then
Rule1	container1/	3 days	Move to archive storage
Rule2	<i>Not applicable</i>	5 days	Move to cool storage
Rule3	container2/	10 days	Delete the blob
Rule4	container2/	15 days	Move to archive storage

On June 1, you store two blobs in storage1 as shown in the following table.

Name	Location	Access tier
File1	container1	Hot
File2	container2	Hot

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

- | Statements | Yes | No |
|--|-----------------------|-----------------------|
| On June 6, File1 will be stored in the Cool access tier. | <input type="radio"/> | <input type="radio"/> |
| On June 7, File2 will be stored in the Cool access tier. | <input type="radio"/> | <input type="radio"/> |
| On June 16, File2 will be stored in the Archive access tier. | <input type="radio"/> | <input type="radio"/> |

Answer:

Answer Area

Statements	Yes	No
On June 6, File1 will be stored in the Cool access tier.	<input type="radio"/>	<input checked="" type="radio"/>
On June 7, File2 will be stored in the Cool access tier.	<input checked="" type="radio"/>	<input type="radio"/>
On June 16, File2 will be stored in the Archive access tier.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

On June 6, File 1 will be stored in the Cool access tier: **NO** Rule 1 applies and File 1 will be in archive storage.

On June 7, File 2 will be stored in the Cool access tier: **YES** - Rule 5 applies to all files due to the lack of a prefix, and File 2 will be in cool storage.

On June 16, File 2 will be stored in the Archive access tier: **NO** -Rule 3 applies and File 2 will be deleted.

Question: 245

CertyIQ

HOTSPOT

You have an Azure Storage account named contoso2024 that contains the resources shown in the following table.

Name	Type	Contents
container1	Blob container	File1
share1	Azure Files share	File2

You have users that have permissions for contoso2024 as shown in the following table.

Name	Permission
User1	Reader role
User2	Storage Account Contributor role
User3	Has an access key for contoso2024

The contoso2024 account is configured as shown in the following exhibit.

contoso2024 | Configuration

Storage account

Save Discard Refresh Give feedback

The cost of your storage account depends on the usage and the options you choose below. [Learn more about storage pricing](#)

Account kind

StorageV2 (general purpose v2)

Performance

Standard Premium

i This setting cannot be changed after the storage account is created.

Secure transfer required

Disabled Enabled

Allow Blob public access

Disabled Enabled

Allow storage account key access

Disabled Enabled

Allow recommended upper limit for shared access signature (SAS) expiry interval

Disabled Enabled

Default to Azure Active Directory authorization in the Azure portal

Disabled Enabled

Minimum TLS version

Version 1.2

Permitted scope for copy operations (preview)

From any storage account

Blob access tier (default)

Cool Hot

Large file shares

Disabled Enabled

i The current combination of subscription, storage account kind, performance, replication and location does not support large file share

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
------------	-----	----

User1 can read File1.

User2 can read File2.

User3 can read File1 and File2.

Answer:

Answer Area

Statements	Yes	No
User1 can read File1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can read File2.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can read File1 and File2.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

- 1-Yes: Public Access is enabled for blob
- 2- No: Azure Storage Account Contributor role can't access the file share
- 3- No: Access Key is disabled on the storage account

Question: 246

CertyIQ

HOTSPOT

You have an Azure subscription linked to a hybrid Microsoft Entra tenant. The tenant contains the users shown in the following table.

Name	On-premises sync enabled
User1	No
User2	Yes

You create the Azure Files shares shown in the following table.

Name	Storage account
share1	contoso2024
share2	contoso2024
share3	contoso2025

You configure identity-based access for contoso2024 as shown in the following exhibit.

contoso2024 | Active Directory

File shares

Refresh

Step 1: Enable an Active Directory source

Choose the Active Directory source that contains the user accounts that will access a share in this storage account. You can set up identity-based access control for user accounts located in either one of these three domain services.

- Active Directory domain controller you host on a Windows Server (generally referred to as "on-premises AD" even though you might host these servers in Azure)
- Azure Active Directory Domain Services (Azure AD DS), a platform as a service, hosted directory service and domain controller in Azure
- Azure AD Kerberos allows using Kerberos authentication from Azure AD-joined clients. In order to use Azure AD Kerberos, user accounts must be hybrid identities.

Active Directory Enabled Configure	Azure Active Directory Domain Services Another access method is already configured	Azure AD Kerberos Another access method is already configured
---	--	---

Azure Active Directory (Azure AD) is not a domain controller, only a directory service. User accounts solely based in Azure AD are currently not supported.

Step 2: Set share-level permissions

Once you have enabled Active Directory source on your storage account, you must configure share-level permissions in order to get access to your file shares. There are two ways you can assign share level permissions. You can assign them to all authenticated identities as a default share level permission and you can assign them to specific Azure AD users/user group. [Learn more](#)

Permissions for all authenticated users and groups

Default share-level permissions Disable permissions and no access is allowed to file shares Enable permissions for all authenticated users and groups

Select appropriate role *

Storage File Data SMB Share Contributor

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can access the content in share1.	<input type="radio"/>	<input type="radio"/>
User2 can access the content in share2.	<input type="radio"/>	<input type="radio"/>
User2 can access the content in share3.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 can access the content in share1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access the content in share2.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can access the content in share3.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

No - User1 does not have access to any Azure resources since it is not synced to Entra AD, even if AD is configured as the authentication source.

Yes - User2 has access to the storage account since it is a cloud-synced user, and AD is configured as the authentication source for storage2024.

No - User2 can't access the content in Share3 since AD isn't configured as a source for storage2025.

Question: 247

CertyIQ

HOTSPOT

Your network contains an on-premises Active Directory Domain Services (AD DS) domain.

The domain contains the identities shown in the following table.

Name	Description	In organizational unit (OU)
User1	User	OU2
User2	User	OU1
Group1	Global group that contains User1	OU1

You have an Azure subscription that contains a storage account named storage1. The file shares in storage1 have an identity source of AD DS and Default share-level permissions set to Enable permissions for all authenticated users and groups.

You create an Azure Files share named share1 that has the roles shown in the following table.

Identity	Role
User2	Storage File Data SMB Share Reader
Group1	Storage File Data SMB Share Contributor

You have a Microsoft Entra tenant that contains a cloud-only user named User3.

You use Microsoft Entra Connect to sync OU1 from the AD DS domain to the Microsoft Entra tenant.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can access content in share1.	<input type="radio"/>	<input type="radio"/>
User2 can access content in share1.	<input type="radio"/>	<input type="radio"/>
User3 can access content in share1.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 can access content in share1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access content in share1.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can access content in share1.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

No - User 1 is in organizational unit 2, but OU2 isn't configured to sync from the AD DS domain to the Entra Tenant.

Yes - User2 is in the OU1 domain which IS synced to the Entra tenant

No - User3 has not been granted access either as an authenticated user or through an authenticated group.

Question: 248

CertyIQ

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

Name	Kind	Performance	Replication	Access tier
storage1	StorageV2 (general purpose v2)	Standard	Locally redundant storage (LRS)	Cool
storage2	StorageV2 (general purpose v2)	Standard	Read-access geo-redundant storage (RA-GRS)	Hot
storage3	BlobStorage	Premium	Locally redundant storage (LRS)	Hot

Which storage account can be converted to zone-redundant storage (ZRS) replication?

- A.storage1 only
- B.storage2 only
- C.storage3 only
- D.storage2 and storage3
- E.storage1, storage2, and storage3

Answer: A

Explanation:

Storage1 only : This storage account might be in a region that supports ZRS and is of a type that is compatible with ZRS.

Question: 249

CertyIQ

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 Storage account named storage1.

You need to enable a user named User1 to list and regenerate storage account keys for storage1.

Solution: You assign the Reader and Data Access role to User1.

Does this meet the goal?

- A.Yes
- B.No

Answer: B

Explanation:

NO To enable User1 to list and regenerate storage account keys, you should assign the Storage Account Key Operator Service Role1.

Question: 250

CertyIQ

You have an Azure subscription that contains a Standard SKU Azure container registry named ContReg1.

You need to ensure that ContReg1 supports geo-replication.

What should you do first for ContReg1?

- A.Enable Admin user.
- B.Add a scope map.
- C.Add an automation task.
- D.Create a cache rule.
- E.Upgrade the SKU.

Answer: E

Explanation:

E: Upgrade the SKU. This is necessary because geo-replication is a Premium SKU feature, and your current registry is on the Standard SKU. Upgrading the SKU will unlock the geo-replication capability.

Question: 251

CertyIQ

HOTSPOT

-

Case study

-

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

-

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

-

ADatum Corporation is consulting firm that has a main office in Montreal and branch offices in Seattle and New York.

Existing Environment

-

Azure Environment

ADatum has an Azure subscription that contains three resource groups named RG1, RG2, and RG3.

The subscription contains the storage accounts shown in the following table.

Name	Kind	Location	Hierarchical namespace	Container	File share
storage1	StorageV2	West US	Yes	cont1	share1
storage2	StorageV2	West US	No	cont2	share2

The subscription contains the virtual machines shown in the following table.

Name	Size	Operating system	Description
VM1	A	Red Hat Enterprise Linux (RHEL)	Uses ephemeral OS disks
VM2	D	Windows Server 2022	Has a basic volume
VM3	B	Red Hat Enterprise Linux (RHEL)	Uses a standard SSDs
VM4	M	Windows Server 2022	Uses Write Accelerator disks
VM5	E	Windows Server 2022	Has a dynamic volume

The subscription has an Azure container registry that contains the images shown in the following table.

Name	Operating system
Image1	Windows Server
Image2	Linux

The subscription contains the resources shown in the following table.

Name	Description	In resource group
Workspace1	Log Analytics workspace	RG1
WebApp1	Azure App Service web app	RG1
VNet1	Virtual network	RG2
zone1.com	Azure Private DNS zone	RG3

Azure Key Vault

The subscription contains an Azure key vault named Vault1.

Vault1 contains the certificates shown in the following table.

Name	Content type	Key type	Key size
Cert1	PKCS#12	RSA	2048
Cert2	PKCS#12	RSA	4096
Cert3	PEM	RSA	2048
Cert4	PEM	RSA	4096

Vault1 contains the keys shown in the following table.

Name	Type	Description
Key1	RSA	Has a key size of 4096
Key2	EC	Has Elliptic curve name set to P-256

Microsoft Entra Environment

ADatum has a Microsoft Entra tenant named adatum.com that is linked to the Azure subscription and contains the users shown in the following table.

Name	Microsoft Entra role	Azure role
Admin1	Global Administrator	<i>None</i>
Admin2	Attribute Definition Administrator	<i>None</i>
Admin3	Attribute Assignment Administrator	<i>None</i>
User1	<i>None</i>	Reader for RG2 and RG3

The tenant contains the groups shown in the following table.

Name	Type
Group1	Security group
Group2	Microsoft 365 group

The adatum.com tenant has a custom security attribute named Attribute1.

Planned Changes

ADatum plans to implement the following changes:

- Configure a data collection rule (DCR) named DCR1 to collect only system events that have an event ID of 4648 from VM2 and VM4.
- In storage1, create a new container named cont2 that has the following access policies:
 - Three stored access policies named Stored1, Stored2, and Stored3
 - A legal hold for immutable blob storage
- Whenever possible, use directories to organize storage account content.
- Grant User1 the permissions required to link Zone1 to VNet1.
- Assign Attribute1 to supported adatum.com resources.
- In storage2, create an encryption scope named Scope1.
- Deploy new containers by using Image1 or Image2.

Technical Requirements

ADatum must meet the following technical requirements:

- Use TLS for WebApp1.
- Follow the principle of least privilege.
- Grant permissions at the required scope only.
- Ensure that Scope1 is used to encrypt storage services.
- Use Azure Backup to back up cont1 and share1 as frequently as possible.
- Whenever possible, use Azure Disk Encryption and a key encryption key (KEK) to encrypt the virtual machines.

You implement the planned changes for cont2.

What is the maximum number of additional access policies you can create for cont2? To answer, select the

appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Stored access policies:

	▼
0	
1	
2	
3	
4	
5	

Immutable blob storage policies:

	▼
0	
1	
2	
3	
4	
5	

Answer:

Answer Area

Stored access policies:

0
1
2
3
4
5

Immutable blob storage policies:

0
1
2
3
4
5

Explanation:

Stored Access Policies :2

Stored access policies provide additional control over shared access signatures (SAS) by defining a set of restrictions that apply to multiple SAS tokens. Instead of defining permissions and expiration for each SAS token individually, you can link multiple SAS tokens to a single stored access policy. This allows:

Centralized management of SAS permissions.

The ability to revoke access by deleting or modifying the policy instead of each individual SAS token.

Easier enforcement of security best practices.

In the given image, the number of stored access policies is set to **2** meaning the Azure storage account allows up to two stored access policies to be created.

Immutable Blob Storage Policies:1.

Immutable blob storage policies are used to protect data from being modified or deleted for a specified retention period. Azure provides two types of immutable policies:

Time-based retention – Ensures data cannot be modified until a set duration expires.

Legal hold – Prevents modification indefinitely until the hold is lifted.

In the image, the number of immutable blob storage policies is set to **1** meaning only one immutable storage policy is allowed.

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

ADatum Corporation is consulting firm that has a main office in Montreal and branch offices in Seattle and New York.

Existing Environment -**Azure Environment -**

ADatum has an Azure subscription that contains three resource groups named RG1, RG2, and RG3.

The subscription contains the storage accounts shown in the following table.

Name	Kind	Location	Hierarchical namespace	Container	File share
storage1	StorageV2	West US	Yes	cont1	share1
storage2	StorageV2	West US	No	cont2	share2

The subscription contains the virtual machines shown in the following table.

Name	Size	Operating system	Description
VM1	A	Red Hat Enterprise Linux (RHEL)	Uses ephemeral OS disks
VM2	D	Windows Server 2022	Has a basic volume
VM3	B	Red Hat Enterprise Linux (RHEL)	Uses a standard SSDs
VM4	M	Windows Server 2022	Uses Write Accelerator disks
VM5	E	Windows Server 2022	Has a dynamic volume

The subscription has an Azure container registry that contains the images shown in the following table.

Name	Operating system
Image1	Windows Server
Image2	Linux

The subscription contains the resources shown in the following table.

Name	Description	In resource group
Workspace1	Log Analytics workspace	RG1
WebApp1	Azure App Service web app	RG1
VNet1	Virtual network	RG2
zone1.com	Azure Private DNS zone	RG3

Azure Key Vault -

The subscription contains an Azure key vault named Vault1.

Vault1 contains the certificates shown in the following table.

Name	Content type	Key type	Key size
Cert1	PKCS#12	RSA	2048
Cert2	PKCS#12	RSA	4096
Cert3	PEM	RSA	2048
Cert4	PEM	RSA	4096

Vault1 contains the keys shown in the following table.

Name	Type	Description
Key1	RSA	Has a key size of 4096
Key2	EC	Has Elliptic curve name set to P-256

Microsoft Entra Environment -

ADatum has a Microsoft Entra tenant named adatum.com that is linked to the Azure subscription and contains the users shown in the following table.

Name	Microsoft Entra role	Azure role
Admin1	Global Administrator	<i>None</i>
Admin2	Attribute Definition Administrator	<i>None</i>
Admin3	Attribute Assignment Administrator	<i>None</i>
User1	<i>None</i>	Reader for RG2 and RG3

The tenant contains the groups shown in the following table.

Name	Type
Group1	Security group
Group2	Microsoft 365 group

The adatum.com tenant has a custom security attribute named Attribute1.

Planned Changes -

ADatum plans to implement the following changes:

- Configure a data collection rule (DCR) named DCR1 to collect only system events that have an event ID of 4648 from VM2 and VM4.
- In storage1, create a new container named cont2 that has the following access policies: oThree stored access policies named Stored1, Stored2, and Stored3 oA legal hold for immutable blob storage
- Whenever possible, use directories to organize storage account content.
- Grant User1 the permissions required to link Zone1 to VNet1.
- Assign Attribute1 to supported adatum.com resources.
- In storage2, create an encryption scope named Scope1.
- Deploy new containers by using Image1 or Image2.

Technical Requirements -

ADatum must meet the following technical requirements:

- Use TLS for WebApp1.
- Follow the principle of least privilege.
- Grant permissions at the required scope only.
- Ensure that Scope1 is used to encrypt storage services.
- Use Azure Backup to back up cont1 and share1 as frequently as possible.
- Whenever possible, use Azure Disk Encryption and a key encryption key (KEK) to encrypt the virtual machines.

You need to configure encryption for the virtual machines. The solution must meet the technical requirements.

Which virtual machines can you encrypt?

- A. VM1 and VM3
- B. VM4 and VM5
- C. VM2 and VM3
- D. VM2 and VM4

Answer: C

Explanation:

<https://learn.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-windows>

Azure Disk Encryption does not work for the following scenarios for window, Hence we can not encrypt VM4 and VM5.

M-series VMs with Write Accelerator disks.

Dynamic volumes.

<https://learn.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-linux?tabs=azcliazure%2Cenableadecli%2Cefacli%2Cadedatacli>

Azure Disk Encryption does not work for the following Linux scenarios, Hence we can not encrypt VM1

Ephemeral OS disks.

Question: 253

CertyIQ

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

ADatum Corporation is consulting firm that has a main office in Montreal and branch offices in Seattle and New York.

Existing Environment -

Azure Environment -

ADatum has an Azure subscription that contains three resource groups named RG1, RG2, and RG3.

The subscription contains the storage accounts shown in the following table.

Name	Kind	Location	Hierarchical namespace	Container	File share
storage1	StorageV2	West US	Yes	cont1	share1
storage2	StorageV2	West US	No	cont2	share2

The subscription contains the virtual machines shown in the following table.

Name	Size	Operating system	Description
VM1	A	Red Hat Enterprise Linux (RHEL)	Uses ephemeral OS disks
VM2	D	Windows Server 2022	Has a basic volume
VM3	B	Red Hat Enterprise Linux (RHEL)	Uses a standard SSDs
VM4	M	Windows Server 2022	Uses Write Accelerator disks
VM5	E	Windows Server 2022	Has a dynamic volume

The subscription has an Azure container registry that contains the images shown in the following table.

Name	Operating system
Image1	Windows Server
Image2	Linux

The subscription contains the resources shown in the following table.

Name	Description	In resource group
Workspace1	Log Analytics workspace	RG1
WebApp1	Azure App Service web app	RG1
VNet1	Virtual network	RG2
zone1.com	Azure Private DNS zone	RG3

Azure Key Vault -

The subscription contains an Azure key vault named Vault1.

Vault1 contains the certificates shown in the following table.

Name	Content type	Key type	Key size
Cert1	PKCS#12	RSA	2048
Cert2	PKCS#12	RSA	4096
Cert3	PEM	RSA	2048
Cert4	PEM	RSA	4096

Vault1 contains the keys shown in the following table.

Name	Type	Description
Key1	RSA	Has a key size of 4096
Key2	EC	Has Elliptic curve name set to P-256

Microsoft Entra Environment -

ADatum has a Microsoft Entra tenant named adatum.com that is linked to the Azure subscription and contains the users shown in the following table.

Name	Microsoft Entra role	Azure role
Admin1	Global Administrator	<i>None</i>
Admin2	Attribute Definition Administrator	<i>None</i>
Admin3	Attribute Assignment Administrator	<i>None</i>
User1	<i>None</i>	Reader for RG2 and RG3

The tenant contains the groups shown in the following table.

Name	Type
Group1	Security group
Group2	Microsoft 365 group

The adatum.com tenant has a custom security attribute named Attribute1.

Planned Changes -

ADatum plans to implement the following changes:

- Configure a data collection rule (DCR) named DCR1 to collect only system events that have an event ID of 4648 from VM2 and VM4.
- In storage1, create a new container named cont2 that has the following access policies: oThree stored access

- policies named Stored1, Stored2, and Stored3 oA legal hold for immutable blob storage
- Whenever possible, use directories to organize storage account content.
 - Grant User1 the permissions required to link Zone1 to VNet1.
 - Assign Attribute1 to supported adatum.com resources.
 - In storage2, create an encryption scope named Scope1.
 - Deploy new containers by using Image1 or Image2.

Technical Requirements -

ADatum must meet the following technical requirements:

- Use TLS for WebApp1.
- Follow the principle of least privilege.
- Grant permissions at the required scope only.
- Ensure that Scope1 is used to encrypt storage services.
- Use Azure Backup to back up cont1 and share1 as frequently as possible.
- Whenever possible, use Azure Disk Encryption and a key encryption key (KEK) to encrypt the virtual machines.

You need to implement the planned changes for the storage account content.

Which containers and file shares can you use to organize the content?

- A.share1 only
- B.cont1 and share1 only
- C.share1 and share2 only
- D.cont1, share1, and share2 only
- E.cont1, cont2, share1, and share2

Answer: D

Explanation:

cont1: The container in storage1 with a hierarchical namespace is specifically designed to organize content efficiently.

share1 and share2: Both are file shares in storage2 and are not restricted by the hierarchical namespace feature. They can still be used to organize content effectively.

Using all three (cont1, share1, and share2) allows for a comprehensive organization strategy across different storage types, adhering to the planned changes and technical requirements.

Question: 254

CertyIQ

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 deploy an Azure Kubernetes Service (AKS) cluster named AKS1.

You need to deploy a YAML file to AKS1.

Solution: From Azure CLI, you run az aks.

Does this meet the goal?

- A. Yes
- B. No

Answer: B**Explanation:**

To deploy the YAML file you need to runs kubectl apply -f file_name.yaml

Reference:

<https://docs.microsoft.com/en-us/azure/aks/kubernetes-walkthrough>

CertyIQ**Question: 255**

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 deploy an Azure Kubernetes Service (AKS) cluster named AKS1.

You need to deploy a YAML file to AKS1.

Solution: From Azure CLI, you run the kubectl client.

Does this meet the goal?

A. Yes

B. No

Answer: A**Explanation:**

To manage a Kubernetes cluster, use the Kubernetes command-line client, kubectl

then run "kubectl apply -f azure-vote.yaml"

Reference:

<https://docs.microsoft.com/en-us/azure/aks/kubernetes-walkthrough>

CertyIQ**Question: 256**

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 deploy an Azure Kubernetes Service (AKS) cluster named AKS1.

You need to deploy a YAML file to AKS1.

Solution: From Azure CLI, you run azcopy.

Does this meet the goal?

A. Yes

B. No

Answer: B**Explanation:**

To deploy a YAML file, the command is:

```
kubectl apply -f example.yaml
```

Reference:

<https://docs.microsoft.com/en-us/azure/aks/kubernetes-walkthrough>

CertyIQ

Question: 257

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 machine named VM1 that runs Windows Server 2016.

You need to create an alert in Azure when more than two error events are logged to the System event log on VM1 within an hour.

Solution: You create an Azure storage account and configure shared access signatures (SASs). You install the Microsoft Monitoring Agent on VM1. You create an alert in Azure Monitor and specify the storage account as the source.

Does that meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Instead: You create an Azure Log Analytics workspace and configure the data settings. You install the Microsoft Monitoring Agent on VM1. You create an alert in Azure Monitor and specify the Log Analytics workspace as the source.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agents-overview>

CertyIQ

Question: 258

HOTSPOT -

You have an Azure subscription named Subscription1. Subscription1 contains the resources in the following table.

Name	Type
RG1	Resource group
RG2	Resource group
VNet1	Virtual network
VNet2	Virtual network

VNet1 is in RG1. VNet2 is in RG2. There is no connectivity between VNet1 and VNet2.

An administrator named Admin1 creates an Azure virtual machine named VM1 in RG1. VM1 uses a disk named Disk1 and connects to VNet1. Admin1 then installs a custom application in VM1.

You need to move the custom application to VNet2. The solution must minimize administrative effort.

Which two actions should you perform? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

First action:

- Create a network interface in RG2.
- Detach a network interface.
- Delete VM1.
- Move a network interface to RG2.

Second action:

- Attach a network interface.
- Create a network interface in RG2.
- Create a new virtual machine.
- Move VM1 to RG2.

Answer:

Answer Area

First action:

- Create a network interface in RG2.
- Detach a network interface.
- Delete VM1.**
- Move a network interface to RG2.

Second action:

- Attach a network interface.
- Create a network interface in RG2.
- Create a new virtual machine.**
- Move VM1 to RG2.

Explanation:

We cannot just move a virtual machine between networks. What we need to do is identify the disk used by the VM, delete the VM itself while retaining the disk, and recreate the VM in the target virtual network and then attach the original disk to it.

Reference:

<https://blogs.technet.microsoft.com/canitpro/2014/06/16/step-by-step-move-a-vm-to-a-different-vnet-on-azure/> <https://4sysops.com/archives/move-an-azure-vm-to-another-virtual-network-vnet/#migrate-an-azure-vm-between-vnets>

Question: 259

CertyIQ

You download an Azure Resource Manager template based on an existing virtual machine. The template will be used to deploy 100 virtual machines.

You need to modify the template to reference an administrative password. You must prevent the password from being stored in plain text.

What should you create to store the password?

- A. an Azure Key Vault and an access policy
- B. an Azure Storage account and an access policy
- C. a Recovery Services vault and a backup policy
- D. Azure Active Directory (AD) Identity Protection and an Azure policy

Answer: A**Explanation:**

You can use a template that allows you to deploy a simple Windows VM by retrieving the password that is stored in a Key Vault. Therefore, the password is never put in plain text in the template parameter file.

Reference:

<https://azure.microsoft.com/en-us/resources/templates/101-vm-secure-password/>

Question: 260**CertyIQ**

HOTSPOT -

You have the App Service plans shown in the following table.

Name	Operating system	Location
ASP1	Windows	West US
ASP2	Windows	Central US
ASP3	Linux	West US

You plan to create the Azure web apps shown in the following table.

Name	Runtime stack	Location
WebApp1	.NET Core 3.0	West US
WebApp2	ASP.NET 4.7	West US

You need to identify which App Service plans can be used for the web apps.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

WebApp1:

ASP1 only
ASP3 only
ASP1 and ASP2 only
ASP1 and ASP3 only
ASP1, ASP2, and ASP3

WebApp2:

ASP1 only
ASP3 only
ASP1 and ASP2 only
ASP1 and ASP3 only
ASP1, ASP2, and ASP3

Answer:

Answer Area

WebApp1:

ASP1 only
ASP3 only
ASP1 and ASP2 only
ASP1 and ASP3 only
ASP1, ASP2, and ASP3

WebApp2:

ASP1 only
ASP3 only
ASP1 and ASP2 only
ASP1 and ASP3 only
ASP1, ASP2, and ASP3

Explanation:

Box 1: ASP1 ASP3 -

Asp1, ASP3: ASP.NET Core apps can be hosted both on Windows or Linux.

Not ASP2: The region in which your app runs is the region of the App Service plan it's in.

Box 2: ASP1 -

ASP.NET apps can be hosted on Windows only.

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/quickstart-dotnetcore?pivots=platform-linux> <https://docs.microsoft.com/en-us/azure/app-service/app-service-plan-manage#>

Question: 261

CertyIQ

HOTSPOT -

You create a virtual machine scale set named Scale1. Scale1 is configured as shown in the following exhibit.

Create a virtual machine scale set

Basics Disks Networking Scaling Management Health Advanced

An Azure virtual machine scale set can automatically increase or decrease the number of VM instances that run your application. This automated and elastic behavior reduces the management overhead to monitor and optimize the performance of your application. [Learn more about VMSS scaling](#)

Instance

Initial instance count *



Scaling

Scaling policy

Manual Custom

Minimum number of VMs *



Maximum number of VMs *



Scale out

CPU threshold (%) *



Duration in minutes *



Number of VMs to increase by *



Scale in

CPU threshold (%) *



Number of VMs to decrease by *



Diagnostic logs

Collect diagnostic logs from Autoscale Disabled Enabled

Review + create

< Previous

Next: Management >

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

If Scale1 is utilized at 85 percent for six minutes after it is deployed, Scale1 will be running [answer choice].

▼
2 virtual machines
4 virtual machines
6 virtual machines
10 virtual machines
20 virtual machines

If Scale1 is first utilized at 25 percent for six minutes after it is deployed, and then utilized at 50 percent for six minutes, Scale1 will be running [answer choice].

▼
2 virtual machines
4 virtual machines
6 virtual machines
8 virtual machines
10 virtual machines

Answer:

Answer Area

If Scale1 is utilized at 85 percent for six minutes after it is deployed, Scale1 will be running [answer choice].

▼
2 virtual machines
4 virtual machines
6 virtual machines
10 virtual machines
20 virtual machines

If Scale1 is first utilized at 25 percent for six minutes after it is deployed, and then utilized at 50 percent for six minutes, Scale1 will be running [answer choice].

▼
2 virtual machines
4 virtual machines
6 virtual machines
8 virtual machines
10 virtual machines

Explanation:

Box 1: 6 virtual machines -

The Autoscale scale out rule increases the number of VMs by 2 if the CPU threshold is 80% or higher. The initial instance count is 4 and rises to 6 when the 2 extra instances of VMs are added.

Box 2: 2 virtual machines -

The Autoscale scale in rule decreases the number of VMs by 4 if the CPU threshold is 30% or lower. The initial instance count is 4 and thus cannot be reduced to

0 as the minimum instances is set to 2. Instances are only added when the CPU threshold reaches 80%.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/autoscale-overview> <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/autoscale-best-practices> <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/autoscale-common-scale-patterns>

Question: 262

CertyIQ

You plan to automate the deployment of a virtual machine scale set that uses the Windows Server 2016 Datacenter image.

You need to ensure that when the scale set virtual machines are provisioned, they have web server components installed.

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

NOTE: Each correct selection is worth one point.

- A. Upload a configuration script
- B. Create an automation account
- C. Create an Azure policy
- D. Modify the extensionProfile section of the Azure Resource Manager template
- E. Create a new virtual machine scale set in the Azure portal

Answer: AD**Explanation:**

The Custom Script Extension downloads and executes scripts on Azure VMs. This extension is useful for post deployment configuration, software installation, or any other configuration / management task. Scripts can be downloaded from Azure storage or GitHub, or provided to the Azure portal at extension run-time.

The Custom Script extension integrates with Azure Resource Manager templates, and can also be used with the Azure CLI, Azure PowerShell, Azure portal, or the REST API

The following Custom Script Extension definition downloads a sample script from GitHub, installs the required packages, then writes the VM instance hostname to a basic HTML page.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/tutorial-install-apps-template>

Question: 263

CertyIQ

HOTSPOT -

You have an Azure Kubernetes Service (AKS) cluster named AKS1 and a computer named Computer1 that runs Windows 10. Computer1 has the Azure CLI installed.

You need to install the kubectl client on Computer1.

Which command should you run? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

<input type="checkbox"/>	az
<input type="checkbox"/>	docker
<input type="checkbox"/>	msiexec.exe
<input type="checkbox"/>	Install-Module

<input type="checkbox"/>	aks
<input type="checkbox"/>	/package
<input type="checkbox"/>	-name
<input type="checkbox"/>	pull

Install-cli

Answer:

Answer Area

		Install-cli
	az docker msiexec.exe Install-Module	aks /package -name pull

Explanation:

To install kubectl locally, use the az aks install-cli command: az aks install-cli

Reference:

<https://docs.microsoft.com/en-us/azure/aks/kubernetes-walkthrough>

Question: 264

CertyIQ

DRAG DROP -

You onboard 10 Azure virtual machines to Azure Automation State Configuration.

You need to use Azure Automation State Configuration to manage the ongoing consistency of the virtual machine configurations.

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.

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

Assign tags to the virtual machines

Check the compliance status of the node

Compile a configuration into a node configuration

Upload a configuration to Azure Automation State Configuration

Create a management group



Answer:

Actions

Assign tags to the virtual machines

Check the compliance status of the node

Compile a configuration into a node configuration

Upload a configuration to Azure Automation State Configuration

Create a management group

Answer Area

Upload a configuration to Azure Automation State Configuration

Compile a configuration into a node configuration

Check the compliance status of the node



Explanation:

Step 1: Upload a configuration to Azure Automation State Configuration.

Import the configuration into the Automation account.

Step 2: Compile a configuration into a node configuration.

A DSC configuration defining that state must be compiled into one or more node configurations (MOF document), and placed on the Automation DSC Pull Server.

Step 3: Check the compliance status of the node.

Step 1: Create and upload a configuration to Azure Automation

Step 2: Compile a configuration into a node configuration

Step 3: Register a VM to be managed by State Configuration

Step 4: Specify configuration mode settings

Step 5: Assign a node configuration to a managed node

Step 6: Check the compliance status of a managed node

Question: 265

CertyIQ

You have an Azure Resource Manager template named Template1 that is used to deploy an Azure virtual machine. Template1 contains the following text:

```
"location": {  
    "type": "String",  
    "defaultValue": "eastus",  
    "allowedValues": [  
        "canadacentral",  
        "eastus",  
        "westeurope",  
        "westus" ]  
}
```

The variables section in Template1 contains the following text:

"location": "westeurope"

The resources section in Template1 contains the following text:

```
"type": "Microsoft.Compute/virtualMachines",  
"apiVersion": "2018-10-01",  
"name": "[variables('vmName')]",  
"location": "westeurope",
```

You need to deploy the virtual machine to the West US location by using Template1.

What should you do?

- A. Modify the location in the resources section to westus
- B. Select West US during the deployment
- C. Modify the location in the variables section to westus

Answer: A

Explanation:

You can change the location in resources. Parameters used to define the value of some variables to be able to use in different places in the template resources.

Resources are used only for complicated expressions. In any case, RM will only deploy from resources. In case the value is not mentioned directly, then it will check parameters if it is specified in the resources.

Based on this question, the value of location is defined directly in resources. so you change the resources location value

Question: 266

CertyIQ

You create an App Service plan named Plan1 and an Azure web app named webapp1.

You discover that the option to create a staging slot is unavailable.

You need to create a staging slot for Plan1.

What should you do first?

- A. From Plan1, scale up the App Service plan
- B. From webapp1, modify the Application settings
- C. From webapp1, add a custom domain
- D. From Plan1, scale out the App Service plan

Answer: A

Explanation:

The app must be running in the Standard, Premium, or Isolated tier in order for you to enable multiple deployment slots.

If the app isn't already in the Standard, Premium, or Isolated tier, you receive a message that indicates the supported tiers for enabling staged publishing. At this point, you have the option to select Upgrade and go to the Scale tab of your app before continuing.

Scale up: Get more CPU, memory, disk space, and extra features like dedicated virtual machines (VMs), custom domains and certificates, staging slots, autoscaling, and more.

Incorrect:

Scale out: Increase the number of VM instances that run your app. You can scale out to as many as 30 instances

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/deploy-staging-slots> <https://docs.microsoft.com/en-us/azure/app-service/manage-scale-up>

CertyIQ

Question: 267

You plan to move a distributed on-premises app named App1 to an Azure subscription.

After the planned move, App1 will be hosted on several Azure virtual machines.

You need to ensure that App1 always runs on at least eight virtual machines during planned Azure maintenance. What should you create?

- A. one virtual machine scale set that has 10 virtual machines instances
- B. one Availability Set that has three fault domains and one update domain
- C. one Availability Set that has 10 update domains and one fault domain
- D. one virtual machine scale set that has 12 virtual machines instances

Answer: A

Explanation:

First: in case you created one fault domain, you are limited with one update domain. You can test this.

Second: By default, Azure uses 5 update domains and up to 3 fault domains. So, In case you created 10 vm in scale set. then you will have 2 vm in each update domain. So once one update domain is not available, then you get 4 domains with 8 vms as required.

CertyIQ

Question: 268

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 machine named VM1 that runs Windows Server 2016.

You need to create an alert in Azure when more than two error events are logged to the System event log on VM1 within an hour.

Solution: You create an event subscription on VM1. You create an alert in Azure Monitor and specify VM1 as the source

Does this meet the goal?

- A. Yes
- B. No

Answer: B**Explanation:**

Instead: You create an Azure Log Analytics workspace and configure the data settings. You install the Microsoft Monitoring Agent on VM1. You create an alert in Azure Monitor and specify the Log Analytics workspace as the source.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agents-overview>

CertyIQ**Question: 269**

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 machine named VM1. VM1 was deployed by using a custom Azure Resource Manager template named ARM1.json.

You receive a notification that VM1 will be affected by maintenance.

You need to move VM1 to a different host immediately.

Solution: From the Overview blade, you move the virtual machine to a different subscription.

Does this meet the goal?

- A. Yes
- B. No

Answer: B**Explanation:**

Changing Subscription won't affect the downtime, it will just change the billing. You would need to redeploy the VM. After you redeploy a VM, the temporary disk is lost, and dynamic IP addresses associated with virtual network interface are updated.

From Overview there is no option to move the VM to another hardware to skip the maintenance.

Ideally you need an Availability Set and defining the Update Domains.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/redeploy-to-new-node>

CertyIQ**Question: 270**

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 machine named VM1. VM1 was deployed by using a custom Azure Resource Manager template named ARM1.json.

You receive a notification that VM1 will be affected by maintenance.

You need to move VM1 to a different host immediately.
Solution: From the Redeploy blade, you click Redeploy.
Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

When you redeploy a VM, it moves the VM to a new node within the Azure infrastructure and then powers it back on, retaining all your configuration options and associated resources.

References:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/redeploy-to-new-node>

Question: 271

CertyIQ

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 machine named VM1. VM1 was deployed by using a custom Azure Resource Manager template named ARM1.json.

You receive a notification that VM1 will be affected by maintenance.

You need to move VM1 to a different host immediately.

Solution: From the Update management blade, you click Enable.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

You would need to redeploy the VM.

This action would not make the VM be re-deployed in a new host.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/redeploy-to-new-node>

Question: 272

CertyIQ

You have an Azure subscription that contains a web app named webapp1.

You need to add a custom domain named www.contoso.com to webapp1.

What should you do first?

- A. Create a DNS record
- B. Add a connection string
- C. Upload a certificate.

D. Stop webapp1.

Answer: A

Explanation:

You can use either a CNAME record or an A record to map a custom DNS name to App Service.

Reference:

<https://docs.microsoft.com/en-us/Azure/app-service/app-service-web-tutorial-custom-domain>

Question: 273

CertyIQ

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 subscription that contains the resources shown in the following table.

Name	Type	Region
RG1	Resource group	West US
RG2	Resource group	East Asia
storage1	Storage account	West US
storage2	Storage account	East Asia
VM1	Virtual machine	West US
VNET1	Virtual network	West US
VNET2	Virtual network	East Asia

VM1 connects to VNET1.

You need to connect VM1 to VNET2.

Solution: You move VM1 to RG2, and then you add a new network interface to VM1.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Instead you should delete VM1. You recreate VM1, and then you add the network interface for VM1.

Note: When you create an Azure virtual machine (VM), you must create a virtual network (VNet) or use an existing VNet. You can change the subnet a VM is connected to after it's created, but you cannot change the VNet.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/network-overview>

Question: 274

CertyIQ

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 subscription that contains the resources shown in the following table.

Name	Type	Region
RG1	Resource group	West US
RG2	Resource group	East Asia
storage1	Storage account	West US
storage2	Storage account	East Asia
VM1	Virtual machine	West US
VNET1	Virtual network	West US
VNET2	Virtual network	East Asia

VM1 connects to VNET1.

You need to connect VM1 to VNET2.

Solution: You delete VM1. You recreate VM1, and then you create a new network interface for VM1 and connect it to VNET2.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

You should delete VM1. You recreate VM1, and then you add the network interface for VM1.

Note: When you create an Azure virtual machine (VM), you must create a virtual network (VNet) or use an existing VNet. You can change the subnet a VM is connected to after it's created, but you cannot change the VNet.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/network-overview>

Question: 275

CertyIQ

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 subscription that contains the resources shown in the following table.

Name	Type	Region
RG1	Resource group	West US
RG2	Resource group	East Asia
storage1	Storage account	West US
storage2	Storage account	East Asia
VM1	Virtual machine	West US
VNET1	Virtual network	West US
VNET2	Virtual network	East Asia

VM1 connects to VNET1.

You need to connect VM1 to VNET2.

Solution: You turn off VM1, and then you add a new network interface to VM1.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Instead you should delete VM1. You recreate VM1, and then you add the network interface for VM1.

Note: When you create an Azure virtual machine (VM), you must create a virtual network (VNet) or use an existing VNet. You can change the subnet a VM is connected to after it's created, but you cannot change the VNet.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/network-overview>

Question: 276

CertyIQ

HOTSPOT -

You have an Azure subscription named Subscription1 that contains the quotas shown in the following table.

Quota	Location	Usage
Standard BS Family vCPUs	West US	0 of 20
Standard D Family vCPUs	West US	0 of 20
Total Regional vCPUs	West US	0 of 20

You deploy virtual machines to Subscription1 as shown in the following table.

Name	Size	vCPUs	Location	Status
VM1	Standard_B2ms	2	West US	Running
VM2	Standard_B16ms	16	West US	Stopped (Deallocated)

You plan to deploy the virtual machines shown in the following table.

Name	Size	vCPUs
VM3	Standard_B2ms	1
VM4	Standard_D4s_v3	4
VM5	Standard_B16ms	16

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
You can deploy VM3 to West US.	<input type="radio"/>	<input type="radio"/>
You can deploy VM4 to West US.	<input type="radio"/>	<input type="radio"/>
You can deploy VM5 to West US.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
You can deploy VM3 to West US.	<input checked="" type="radio"/>	<input type="radio"/>
You can deploy VM4 to West US.	<input type="radio"/>	<input checked="" type="radio"/>
You can deploy VM5 to West US.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Total regional vCPUs = 20

2 vCPUs (VM1) + 16 vCPUs (VM20) = 18 vCPUs, which means that only 2 vCPUs left to exceed usage limit.

Box 1: Yes

We can add 1 vCPU. 2 vCPUs (VM1) + 16 vCPUs (VM20) + 1 vCPU (VM3) = 19 vCPUs

Box 2: No

We cannot add 4 vCPUs. 2 vCPUs (VM1) + 16 vCPUs (VM20) + 4 vCPU (VM4) = 22 vCPUs

Box 3: No

We cannot add 16 vCPU. 2 vCPUs (VM1) + 16 vCPUs (VM20) + 16 vCPU (VM5) = 34 vCPUs

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/quota>

CertyIQ

Question: 277

HOTSPOT -

You have an Azure subscription that contains an Azure Availability Set named WEBPROD-AS-USE2 as shown in the following exhibit.

```
PS Azure:\> az vm availability-set list -g RG1
[
  {
    "id": "/subscriptions/8372f433-2dcd-4361-b5ef-5b188fed87d0/resourceGroups/RG1/providers/Microsoft.Compute/availabilitySets/WEBPROD-AS-USE2",
    "location": "eastus2",
    "name": "WEBPROD-AS-USE2",
    "platformFaultDomainCount": 2,
    "platformUpdateDomainCount": 10,
    "proximityPlacementGroup": null,
    "resourceGroup": "RG1",
    "sku": {
      "capacity": null,
      "name": "Aligned",
      "tier": null
    },
    "statuses": null,
    "tags": {},
    "type": "Microsoft.Compute/availabilitySets",
    "virtualMachines": []
  }
]
Azure:/
```

You add 14 virtual machines to WEBPROD-AS-USE2.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

When Microsoft performs planned maintenance in East US 2, the maximum number of unavailable virtual machines will be [answer choice].

2
7
10
14

If the server rack in the Azure datacenter that hosts WEBPROD-AS-USE2 experiences a power failure, the maximum number of unavailable virtual machines will be [answer choice].

2
7
10
14

Answer:

Answer Area

When Microsoft performs planned maintenance in East US 2, the maximum number of unavailable virtual machines will be [answer choice].

2
7
10
14

If the server rack in the Azure datacenter that hosts WEBPROD-AS-USE2 experiences a power failure, the maximum number of unavailable virtual machines will be [answer choice].

2
7
10
14

Explanation:

Box 1: 2 -

There are 10 update domains. The 14 VMs are shared across the 10 update domains so four update domains will have two VMs and six update domains will have one VM. Only one update domain is rebooted at a time. Therefore, a maximum of two VMs will be offline.

Box 2: 7 -

There are 2 fault domains. The 14 VMs are shared across the 2 fault domains, so 7 VMs in each fault domain. A rack failure will affect one fault domain so 7 VMs will be offline.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/manage-availability>

Question: 278

You deploy an Azure Kubernetes Service (AKS) cluster named Cluster1 that uses the IP addresses shown in the

CertyIQ

following table.

IP address	Assigned to
131.107.2.1	Load balancer front end
192.168.10.2	Kubernetes DNS service
172.17.7.1	Docket bridge address
10.0.10.11	Kubernetes cluster node

You need to provide internet users with access to the applications that run in Cluster1.

Which IP address should you include in the DNS record for Cluster1?

- A. 131.107.2.1
- B. 10.0.10.11
- C. 172.17.7.1
- D. 192.168.10.2

Answer: A

Explanation:

A.131.107.2.1.

In Kubernetes when we expose apps we either expose them through Ingress using a single front-end loadbalancer IP, or we expose them using Services like NodePort or LoadBalancer.

Based on the provided scenario we should map the DNS entry to the Load Balancer Front End IP and expose applications using Ingress.

To be able to access applications on Kubernetes, you need an application Load Balancer created by Azure which have public ip.

Question: 279

CertyIQ

You have a deployment template named Template1 that is used to deploy 10 Azure web apps.

You need to identify what to deploy before you deploy Template1. The solution must minimize Azure costs.

What should you identify?

- A. five Azure Application Gateways
- B. one App Service plan
- C. 10 App Service plans
- D. one Azure Traffic Manager
- E. one Azure Application Gateway

Answer: B

Explanation:

Creating one App Service Plan should be your first priority and what type of Plan i.e. Basic, STD, premium, Isolated will depend on needs and once done then you can support up to 10 Web Apps.

You create Azure web apps in an App Service plan.

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/overview-hosting-plans>

CertyIQ

Question: 280

HOTSPOT -

You plan to deploy an Azure container instance by using the following Azure Resource Manager template.

```
{  
  "type": "Microsoft.ContainerInstance/containerGroups",  
  "apiVersion": "2018-10-01",  
  "name": "webprod",  
  "location": "westus",  
  "properties": {  
    "containers": [  
      {  
        "name": "webprod",  
        "properties": {  
          "image": "microsoft/iis:nanoserver",  
          "ports": [  
            {  
              "protocol": "TCP",  
              "port": 80  
            }  
          ],  
          "environmentVariables": [],  
          "resources": {  
            "requests": {  
              "memoryInGB": 1.5,  
              "cpu": 1  
            }  
          }  
        }  
      }  
    ],  
    "restartPolicy": "OnFailure",  
    "ipAddress": {  
      "ports": [  
        {  
          "protocol": "TCP",  
          "port": 80  
        }  
      ],  
      "ip": "[parameters('IPAddress')]",  
      "type": "Public"  
    },  
    "osType": "Windows"  
  }  
}
```

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Internet users [answer choice].

- can connect to the container from any device
- cannot connect to the container
- can only connect to the container from devices that run Windows

If Internet Information Services (IIS) in the container fail, [answer choice].

- the container will restart automatically
- the container will only restart manually
- the container must be redeployed

Answer:

Answer Area

Internet users [answer choice].

- can connect to the container from any device
- cannot connect to the container
- can only connect to the container from devices that run Windows

If Internet Information Services (IIS) in the container fail, [answer choice].

- the container will restart automatically
- the container will only restart manually
- the container must be redeployed

Explanation:

Internet Users Connectivity to the Container

Can connect to the container from any device.

In Azure Container Instances (ACI) or Docker containers running in the cloud, containers are typically exposed using public IP addresses or DNS names.

If networking and firewall rules allow, internet users can connect from any device (Windows, Linux, macOS, mobile, etc.).

The other options ("cannot connect" or "only from Windows devices") are incorrect because:

Containers are platform-independent and do not require a specific OS to access them.

If proper network and firewall configurations are applied, users can connect.

IIS Failure Recovery in the Container

The container will restart automatically.

In Azure Container Instances (ACI), Kubernetes, or Docker, a container restart policy can be set to automatically restart a container if it fails.

By default, Azure Container Instances use a restart policy such as:

Always (default) → Ensures the container restarts if it crashes.

OnFailure → Restarts only if the container exits with a failure code.

Never → The container does not restart.

Since IIS runs inside the container, if it crashes, the container itself is restarted automatically, provided the correct restart policy is configured.

The other options ("only restart manually" or "must be redeployed") are incorrect because:

Containers typically do not require manual intervention for restarts.

Redeployment is not needed unless the container image itself is faulty.

Question: 281

CertyIQ

You have an Azure subscription that contains a virtual machine named VM1. VM1 hosts a line-of-business application that is available 24 hours a day. VM1 has one network interface and one managed disk. VM1 uses the D4s v3 size.

You plan to make the following changes to VM1:

- ⇒ Change the size to D8s v3.
- ⇒ Add a 500-GB managed disk.
- ⇒ Add the Puppet Agent extension.
- ⇒ Enable Desired State Configuration Management.

Which change will cause downtime for VM1?

- A. Enable Desired State Configuration Management
- B. Add a 500-GB managed disk
- C. Change the size to D8s v3
- D. Add the Puppet Agent extension

Answer: C

Explanation:

C. Change the size to D8s v3.

Changing the size of an Azure virtual machine involves a stop and restart of the virtual machine, which will cause downtime for the line-of-business application hosted on VM1. This downtime can be minimized by using Azure Availability Sets or by taking appropriate steps to prepare for the change, such as backing up data or moving the application to another virtual machine.

Adding a managed disk, installing the Puppet Agent extension, or enabling Desired State Configuration Management should not cause downtime for VM1.

While resizing the VM it must be in a stopped state.

Reference:

<https://azure.microsoft.com/en-us/blog/resize-virtual-machines/>

Question: 282

CertyIQ

You have an app named App1 that runs on an Azure web app named webapp1.

The developers at your company upload an update of App1 to a Git repository named Git1.

Webapp1 has the deployment slots shown in the following table.

Name	Function
webapp1-prod	Production
webapp1-test	Staging

You need to ensure that the App1 update is tested before the update is made available to users. Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Swap the slots
- B. Deploy the App1 update to webapp1-prod, and then test the update
- C. Stop webapp1-prod
- D. Deploy the App1 update to webapp1-test, and then test the update
- E. Stop webapp1-test

Answer: AD

Explanation:

- A. Swap the slots.

Once the update is successfully tested in the test slot, you swap the slots.

Swapping the slots promotes the tested version from webapp1-test to webapp1-prod without downtime.

This ensures a smooth transition and minimizes the risk of deploying untested changes.

- D. Deploy the update to webapp1-test, and then test the update.

In Azure App Service, deployment slots allow you to deploy an update to a staging/test slot without affecting the live production environment.

The update should first be deployed to webapp1-test to verify that it works correctly.

Question: 283

CertyIQ

You have an Azure subscription named Subscription1 that has the following providers registered:

- ⇒ Authorization
- ⇒ Automation
- ⇒ Resources
- ⇒ Compute
- ⇒ KeyVault
- ⇒ Network
- ⇒ Storage
- ⇒ Billing
- ⇒ Web

Subscription1 contains an Azure virtual machine named VM1 that has the following configurations:

- ⇒ Private IP address: 10.0.0.4 (dynamic)
- ⇒ Network security group (NSG): NSG1
- ⇒ Public IP address: None
- ⇒ Availability set: AVSet
- ⇒ Subnet: 10.0.0.0/24
- ⇒ Managed disks: No
- ⇒ Location: East US

You need to record all the successful and failed connection attempts to VM1.

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

NOTE: Each correct selection is worth one point.

- A. Enable Azure Network Watcher in the East US Azure region.
- B. Add an Azure Network Watcher connection monitor.
- C. Register the MicrosoftLogAnalytics provider.
- D. Create an Azure Storage account.
- E. Register the Microsoft.Insights resource provider.
- F. Enable Azure Network Watcher flow logs.

Answer: DEF

Explanation:

When you create or update a virtual network in your subscription, Network Watcher will be enabled automatically in your Virtual Network's region. There is no impact to your resources or associated charge for automatically enabling Network Watcher. For more information, see Network Watcher create.

Create a VM with a network security group

Enable Network Watcher (done by default with the vnet/subnet creation)

-- and register the Microsoft.Insights provider -----todo

Enable a traffic flow log for an NSG, using Network Watcher's NSG flow log capability --todo BUT !

NSG flow log data is written to an Azure Storage account. Complete the following steps to create a storage account for the log data.

So you need to create a storage account before enable the NSG flow

Download logged data

View logged data

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview>

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-portal>

Question: 284

CertyIQ

You need to deploy an Azure virtual machine scale set that contains five instances as quickly as possible. What should you do?

- A. Deploy five virtual machines. Modify the Availability Zones settings for each virtual machine.
- B. Deploy five virtual machines. Modify the Size setting for each virtual machine.
- C. Deploy one virtual machine scale set that is set to VM (virtual machines) orchestration mode.
- D. Deploy one virtual machine scale set that is set to ScaleSetVM orchestration mode.

Answer: D

Explanation:

D. Deploy one virtual machine scale set that is set to ScaleSetVM orchestration mode.

To deploy an Azure Virtual Machine Scale Set (VMSS) with five instances as quickly as possible, the best option is to use ScaleSetVM orchestration mode. This mode is specifically designed for scalable and automatically managed virtual machines.

Question: 285

CertyIQ

You plan to create the Azure web apps shown in the following table.

Name	Runtime stack
WebApp1	.NET Core 3.1(LTS)
WebApp2	ASP.NET V4.8
WebApp3	PHP 7.3
WebApp4	Ruby 2.6

What is the minimum number of App Service plans you should create for the web apps?

- A. 1
- B. 2
- C. 3
- D. 4

Answer: B**Explanation:**

.NET Core 3.0: Windows and Linux ASP

.NET V4.7: Windows only

PHP 7.3: Windows and Linux

Ruby 2.6: Linux only

Also, you can't use Windows and Linux Apps in the same App Service Plan, because when you create a new App Service plan you have to choose the OS type. You can't mix Windows and Linux apps in the same App Service plan. So, you need 2 ASPs.

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/overview>

Question: 286

CertyIQ

HOTSPOT -

You have a pay-as-you-go Azure subscription that contains the virtual machines shown in the following table.

Name	Resource group	Daily cost
VM1	RG1	20 euros
VM2	RG2	30 euros

You create the budget shown in the following exhibit.

Budget1

Resource group

Edit budget

Delete budget

CURRENT SPEND
5.93 EUR

Budget

1,000.00 EUR

BUDGET SUMMARY

Name	Budget1
Scope	RG1 (Resource group)
Filters	-
Ammount	1,000.00 EUR
Budget period	Resets billing month
Start date	6/20/2019
End date	6/19/2021

BUDGET ALERTS

Alert conditions	% OF BUDGET	AMOUNT	ACTION GROUP	ACTION GROUP
	50%	€500	AG1	1 Email
	70%	€700	AG2	1 SMS
	100%	€1,000	AG3	1 Azure app
Alert recipients (email)	User1@Contoso.com			

The AG1 action group contains a user named only.

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

Hot Area:

Answer Area

When the maximum amount in Budget1 is reached, [answer choice].

- VM1 and VM2 are turned off
- VM1 and VM2 continue to run
- VM1 is turned off, and VM2 continues to run

Based on the current usage costs of the virtual machines, [answer choice].

- no email notifications will be sent each month
- one email notification will be sent each month
- two email notifications will be sent each month
- three email notifications will be sent each month

Answer:

Answer Area

When the maximum amount in Budget1 is reached, [answer choice].

- VM1 and VM2 are turned off
- VM1 and VM2 continue to run
- VM1 is turned off, and VM2 continues to run

Based on the current usage costs of the virtual machines, [answer choice].

- no email notifications will be sent each month
- one email notification will be sent each month
- two email notifications will be sent each month
- three email notifications will be sent each month

Explanation:

Box 1: VM1 and VM2 continue to run

The budget alerts are for Resource Group RG1, which include VM1, but not VM2. However, when the budget thresholds you've created are exceeded, only notifications are triggered. None of your resources are affected and your consumption isn't stopped.

Box 2: one email notification will be sent each month.

Budget alerts for Resource Group RG1, which include VM1, but not VM2. VM1 consumes 20 Euro/day. The 50%, 500 Euro limit, will be reached in 25 days, and an email will be sent.

The 70% and 100% alert conditions will not be reached within a month, and they don't trigger email actions anyway.

Credit alerts: Credit alerts are generated automatically at 90% and at 100% of your Azure credit balance.

Whenever an alert is generated, it's reflected in cost alerts and in the email sent to the account owners. 90% and 100% will not be reached though.

Reference:

<https://docs.microsoft.com/en-us/azure/cost-management-billing/costs/cost-mgt-alerts-monitor-usage-spending> <https://docs.microsoft.com/en-gb/azure/cost-management-billing/costs/tutorial-acm-create-budgets>

Question: 287

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 subscription named Subscription1. Subscription1 contains a resource group named RG1. RG1 contains resources that were deployed by using templates.

You need to view the date and time when the resources were created in RG1.

Solution: From the Subscriptions blade, you select the subscription, and then click Programmatic deployment.
Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

From the RG1 blade, click Deployments. You see a history of deployment for the resource group.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/template-tutorial-create-first-template?tabs=azure-powershell>

Question: 288

CertyIQ

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 subscription that contains the resources shown in the following table.

Name	Type	Region
RG1	Resource group	West US
RG2	Resource group	East Asia
storage1	Storage account	West US
storage2	Storage account	East Asia
VM1	Virtual machine	West US
VNET1	Virtual network	West US
VNET2	Virtual network	East Asia

VM1 connects to VNET1.

You need to connect VM1 to VNET2.

Solution: You create a new network interface, and then you add the network interface to VM1.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

You should delete VM1. You recreate VM1, and then you add the network interface for VM1.

Note: When you create an Azure virtual machine (VM), you must create a virtual network (VNet) or use an existing VNet. You can change the subnet a VM is connected to after it's created, but you cannot change the VNet.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/network-overview>

CertyIQ

Question: 289

You have an Azure Active Directory (Azure AD) tenant named adatum.com that contains the users shown in the following table.

Name	Role
User1	<i>None</i>
User2	Global administrator
User3	Cloud device administrator
User4	Intune administrator

Adatum.com has the following configurations:

- ⇒ Users may join devices to Azure AD is set to User1.
- ⇒ Additional local administrators on Azure AD joined devices is set to None.

You deploy Windows 10 to a computer named Computer1. User1 joins Computer1 to adatum.com.

You need to identify the local Administrator group membership on Computer1.

Which users are members of the local Administrators group?

- A. User1 only
- B. User2 only
- C. User1 and User2 only
- D. User1, User2, and User3 only
- E. User1, User2, User3, and User4

Answer: C

Explanation:

Users may join devices to Azure AD - This setting enables you to select the users who can register their devices as Azure AD joined devices. The default is All.

Additional local administrators on Azure AD joined devices - You can select the users that are granted local administrator rights on a device. Users added here are added to the Device Administrators role in Azure AD. Global administrators, here User2, in Azure AD and device owners are granted local administrator rights by default.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal>

CertyIQ

Question: 290

HOTSPOT -

You have Azure subscriptions named Subscription1 and Subscription2. Subscription1 has following resource groups:

Name	Region	Lock type
RG1	West Europe	None
RG2	West Europe	Read Only

RG1 includes a web app named App1 in the West Europe location.

Subscription2 contains the following resource groups:

Name	Region	Lock type
RG3	East Europe	Delete
RG4	Central US	none

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
App1 can be moved to RG2	<input type="radio"/>	<input type="radio"/>
App1 can be moved to RG3	<input type="radio"/>	<input type="radio"/>
App1 can be moved to RG4	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
App1 can be moved to RG2	<input type="radio"/>	<input checked="" type="radio"/>
App1 can be moved to RG3	<input checked="" type="radio"/>	<input type="radio"/>
App1 can be moved to RG4	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Box 1: No -

RG2 is read only. ReadOnly means authorized users can read a resource, but they cannot delete or update the resource.

Box 2: Yes -

Box 3: Yes -

Note:

App Service resources are region-specific and cannot be moved directly across regions. You can move the App Service resource by creating a copy of your existing App Service resource in the target region, then move your content over to the new app. You can then delete the source app and App Service plan. To make copying your app easier, you can clone an individual App Service app into an App Service plan in another region.

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/manage-move-across-regions> <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/move-limitations/app-service-move-limitations>

Question: 291

CertyIQ

HOTSPOT -

You have an Azure subscription named Subscription1 that contains the following resource group:

- ⇒ Name: RG1
- ⇒ Region: West US
- ⇒ Tag: `tag1`: `value1`

You assign an Azure policy named Policy1 to Subscription1 by using the following configurations:

- ⇒ Exclusions: None
- ⇒ Policy definition: Append a tag and its value to resources
- ⇒ Assignment name: Policy1
- ⇒ Parameters:
- ⇒ Tag name: tag2

Tag value: value2 -

After Policy1 is assigned, you create a storage account that has the following configuration:

- ⇒ Name: storage1
- ⇒ Location: West US
- ⇒ Resource group: RG1
- ⇒ Tags: `tag3`: `value3`

You need to identify which tags are assigned to each resource.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Tags assigned to RG1:

"tag1": "value1" only
"tag2": "value2" only
"tag1": "value1" and "tag2": "value2"

Tags assigned to storage1:

"tag3": "value3" only
"tag1": "value1" and "tag3": "value3" only
"tag2": "value2" and "tag3": "value3" only
"tag1": "value1", "tag2": "value2", and "tag3": "value3"

Answer:

Answer Area

Tags assigned to RG1:

"tag1": "value1" only
"tag2": "value2" only
"tag1": "value1" and "tag2": "value2"

Tags assigned to storage1:

"tag3": "value3" only
"tag1": "value1" and "tag3": "value3" only
"tag2": "value2" and "tag3": "value3" only
"tag1": "value1", "tag2": "value2", and "tag3": "value3"

Explanation:

- 1) Tags assigned to RG1: "'tag1': 'value1' only"
- 2) Tags assigned to storage1: "'tag2': 'value2' and 'tag3': 'value3' only"

The Resource Group already existed before the Policy was created. And the policy is for resources only not resource groups.

The storage account was created with tag3 and then gets appended the tag2 because the policy.

Question: 292

CertyIQ

HOTSPOT -

You have an Azure subscription named Subscription1.

In Subscription1, you create an alert rule named Alert1.

The Alert1 action group is configured as shown in the following exhibit.

```
ResourceGroupName : default-activitylogalerts
GroupShortName   : AG1
Enabled          : True
EmailReceivers   : {Action1_ "EmailAction"}
SmsReceivers     : {Action1_ "SMSAction"}
WebhookReceivers : {}
Id              : /subscriptions/a4fde29b-d56a-4f6c-8298-
6c53cd0b720c/resourceGroups/
default-activitylogalerts/providers/microsoft.insights/actionGroups/ActionGroup1
Name            : ActionGroup1
Type            : Microsoft.Insights/ActionGroups
Location        : Global
Tags            : {}
```

Alert1 alert criteria triggered every minute.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

The number of email messages that Alert1 will send in an hour is

0
4
6
12
60

The number of SMS messages that Alert2 will send in an hour is

0
4
6
12
60

Answer:

Answer Area

The number of email messages that Alert1 will send in an hour is

0
4
6
12
60

The number of SMS messages that Alert2 will send in an hour is

0
4
6
12
60

Explanation:

Box 1: 60 -

One alert per minute will trigger one email per minute.

Box 2: 12 -

No more than 1 SMS every 5 minutes can be send, which equals 12 per hour.

Note: Rate limiting is a suspension of notifications that occurs when too many are sent to a particular phone number, email address or device. Rate limiting ensures that alerts are manageable and actionable.

The rate limit thresholds are:

- ⇒ SMS: No more than 1 SMS every 5 minutes.
- ⇒ Voice: No more than 1 Voice call every 5 minutes.
- ⇒ Email: No more than 100 emails in an hour.
- ⇒ Other actions are not rate limited.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-rate-limiting>

CertyIQ**Question: 293**

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

Name	Type	Region	Resource group
RG1	Resource group	West Europe	<i>Not applicable</i>
RG2	Resource group	North Europe	<i>Not applicable</i>
Vault1	Recovery Services vault	West Europe	RG1

You create virtual machines in Subscription1 as shown in the following table.

Name	Resource group	Region	Operating system
VM1	RG1	West Europe	Windows Server 2016
VM2	RG1	North Europe	Windows Server 2016
VM3	RG2	West Europe	Windows Server 2016
VMA	RG1	West Europe	Ubuntu Server 18.04
VMB	RG1	North Europe	Ubuntu Server 18.04
VMC	RG2	West Europe	Ubuntu Server 18.04

You plan to use Vault1 for the backup of as many virtual machines as possible.

Which virtual machines can be backed up to Vault1?

- A. VM1 only
- B. VM3 and VMC only
- C. VM1, VM2, VM3, VMA, VMB, and VMC
- D. VM1, VM3, VMA, and VMC only
- E. VM1 and VM3 only

Answer: D**Explanation:**

To create a vault to protect virtual machines, the vault must be in the same region as the virtual machines. If you have virtual machines in several regions, create a

Recovery Services vault in each region.

Reference:

<https://docs.microsoft.com/bs-cyrl-ba/azure/backup/backup-create-rs-vault>

CertyIQ

Question: 294

You have an Azure Kubernetes Service (AKS) cluster named AKS1.

You need to configure cluster autoscaler for AKS1.

Which two tools should you use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. the kubectl command
- B. the az aks command
- C. the Set-AzVm cmdlet
- D. the Azure portal
- E. the Set-AzAks cmdlet

Answer: BD

Explanation:

B. the az aks command: You can use the Azure Command-Line Interface (CLI) command `az aks update` to configure the cluster autoscaler for an AKS cluster. This command allows you to enable or disable the cluster autoscaler and set parameters like minimum and maximum node counts.

D. the Azure portal: You can also configure the cluster autoscaler for AKS using the Azure portal. Navigate to your AKS cluster in the Azure portal, go to the "Node pools" section, and then configure the autoscaler settings for the specific node pool.

CertyIQ

Question: 295

You create the following resources in an Azure subscription:

- ⇒ An Azure Container Registry instance named Registry1
- ⇒ An Azure Kubernetes Service (AKS) cluster named Cluster1

You create a container image named App1 on your administrative workstation.

You need to deploy App1 to Cluster1.

What should you do first?

- A. Run the docker push command.
- B. Create an App Service plan.
- C. Run the az acr build command.
- D. Run the az aks create command.

Answer: A

Explanation:

A. Run the docker push command.

To deploy your container image named App1 to your AKS cluster, you need to push the image to a container registry where it can be accessed by the cluster. Since you've created the image on your administrative workstation, the next logical step is to push this image to your Azure Container Registry (Registry1).

Question: 296

CertyIQ

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

Name	Type	Resource group	Location
RG1	Resource group	<i>Not applicable</i>	Central US
RG2	Resource group	<i>Not applicable</i>	West US
VMSS1	Virtual machine scale set	RG2	West US
Proximity1	Proximity placement group	RG1	Central US
Proximity2	Proximity placement group	RG2	West US
Proximity3	Proximity placement group	RG1	Central US

You need to configure a proximity placement group for VMSS1.

Which proximity placement groups should you use?

- A. Proximity2 only
- B. Proximity1, Proximity2, and Proximity3
- C. Proximity1 only
- D. Proximity1 and Proximity3 only

Answer: A**Explanation:**

Resource Group location of VMSS1 is the RG2 location, which is West US.

Only Proximity2, which also in RG2, is location in West US

Reference:

<https://azure.microsoft.com/en-us/blog/introducing-proximity-placement-groups/>

Question: 297

CertyIQ

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 subscription named Subscription1. Subscription1 contains a resource group named RG1. RG1 contains resources that were deployed by using templates.

You need to view the date and time when the resources were created in RG1.

Solution: From the Subscriptions blade, you select the subscription, and then click Resource providers.

Does this meet the goal?

- A. Yes
- B. No

Answer: B**Explanation:**

From the RG1 blade, click Deployments. You see a history of deployment for the resource group.

Reference:

Question: 298

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 subscription named Subscription1. Subscription1 contains a resource group named RG1. RG1 contains resources that were deployed by using templates.

You need to view the date and time when the resources were created in RG1.

Solution: From the RG1 blade, you click Automation script.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

From the RG1 blade, click Deployments. You see a history of deployment for the resource group.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/template-tutorial-create-first-template?tabs=azure-powershell>

Question: 299

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 subscription named Subscription1. Subscription1 contains a resource group named RG1. RG1 contains resources that were deployed by using templates.

You need to view the date and time when the resources were created in RG1.

Solution: From the RG1 blade, you click Deployments.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

From the RG1 blade, click Deployments. You see a history of deployment for the resource group.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/template-tutorial-create-first-template?tabs=azure-powershell>

Question: 300

CertyIQ

You have an Azure subscription named Subscription1.
You deploy a Linux virtual machine named VM1 to Subscription1.
You need to monitor the metrics and the logs of VM1.
What should you use?

- A. Azure HDInsight
- B. Linux Diagnostic Extension (LAD) 3.0
- C. the AzurePerformanceDiagnostics extension
- D. Azure Analysis Services

Answer: B

Explanation:

The Linux Diagnostic Extension should be used which downloads the Diagnostic Extension (LAD) agent on Linux server.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/diagnostics-linux>

Question: 301

CertyIQ

HOTSPOT -

You have an Azure subscription named Subscription1. Subscription1 contains a virtual machine named VM1. You install and configure a web server and a DNS server on VM1. VM1 has the effective network security rules shown in the following exhibit:

Network Interface: vm1441		Effective security rules		Topology	
		Virtual network/subnet: VNET1/default	NIC Public IP: 52.160.123.200	NIC Private IP: 10.0.6.4	Accelerated networking: Disabled
Inbound port rules		Outbound port rules	Application security groups		Load balancing
🛡️ Network security group VM1-nsg (attached to network interface: vm1441) Impacts 0 subnets, 1 network interfaces				Add inbound port rule	
Priority	Name	Port	Protocol	Source	Destination
100	Rule2	50-60	Any	Any	Any
300	⚠️ RDP	3389	TCP	Any	Any
400	Rule1	50-500	Any	Any	Any
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any
65500	DenyAllInBound	Any	Any	Any	Any

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Internet users [answer choice].

- can connect to only the DNS server on VM1
- can connect to only the web server on VM1
- can connect to the web server and the DNS server on VM1
- cannot connect to the web server and the DNS server on VM1

If you delete Rule2, Internet users [answer choice].

- can connect to only the DNS server on VM1
- can connect to only the web server on VM1
- can connect to the web server and the DNS server on VM1
- cannot connect to the web server and the DNS server on VM1

Answer:

Answer Area

Internet users [answer choice].

- can connect to only the DNS server on VM1
- can connect to only the web server on VM1
- can connect to the web server and the DNS server on VM1
- cannot connect to the web server and the DNS server on VM1

If you delete Rule2, Internet users [answer choice].

- can connect to only the DNS server on VM1
- can connect to only the web server on VM1
- can connect to the web server and the DNS server on VM1
- cannot connect to the web server and the DNS server on VM1

Explanation:

Box 1: Can connect to only the web server on VM 1.

Rule2 blocks ports 50-60, which includes port 53, the DNS port. Internet users can reach to the Web server, since it uses port 80.

Box 2: Can connect to the web server and the DNS Server on VM 1.

If Rule2 is removed internet users can reach the DNS server as well.

Note: Rules are processed in priority order, with lower numbers processed before higher numbers, because lower numbers have higher priority. Once traffic matches a rule, processing stops. As a result, any rules that exist with lower priorities (higher numbers) that have the same attributes as rules with higher priorities are not processed.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/security-overview>

Question: 302

CertyIQ

You plan to deploy three Azure virtual machines named VM1, VM2, and VM3. The virtual machines will host a web app named App1.

You need to ensure that at least two virtual machines are available if a single Azure datacenter becomes unavailable.

What should you deploy?

- A. all three virtual machines in a single Availability Zone
- B. all virtual machines in a single Availability Set
- C. each virtual machine in a separate Availability Zone
- D. each virtual machine in a separate Availability Set

Answer: C

Explanation:

Use availability zones to protect from datacenter level failures.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/manage-availability>

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/tutorial-availability-sets>

Question: 303

CertyIQ

You have an Azure virtual machine named VM1 that runs Windows Server 2019.

You save VM1 as a template named Template1 to the Azure Resource Manager library.

You plan to deploy a virtual machine named VM2 from Template1.

What can you configure during the deployment of VM2?

- A. operating system
- B. administrator username
- C. virtual machine size
- D. resource group

Answer: D

Explanation:

When you deploy a template, you specify a resource group that will contain the resources. Before running the deployment command, create the resource group or during deployment also we can create the resource group. If you try to deploy your own template in the portal, there are 3 available options - "Subscription", "Resource Group", "Location". Resource group is the only one of the three options available in this list of answers.

Resource group: During deployment, you can choose the resource group where the new VM (VM2) will be created. This allows you to organize resources logically.

Question: 304

CertyIQ

You have an Azure subscription that contains an Azure virtual machine named VM1. VM1 runs a financial reporting app named App1 that does not support multiple active instances.

At the end of each month, CPU usage for VM1 peaks when App1 runs.

You need to create a scheduled runbook to increase the processor performance of VM1 at the end of each month.

What task should you include in the runbook?

- A. Add the Azure Performance Diagnostics agent to VM1.

- B. Modify the VM size property of VM1.
- C. Add VM1 to a scale set.
- D. Increase the vCPU quota for the subscription.
- E. Add a Desired State Configuration (DSC) extension to VM1.

Answer: B

Explanation:

Modify the VM size property of VM1: This option allows you to resize the virtual machine to a larger size with more vCPUs and potentially more memory, which directly increases the processing power available to VM1. This can help accommodate the increased CPU usage at the end of each month.

Question: 305

CertyIQ

You plan to deploy several Azure virtual machines that will run Windows Server 2019 in a virtual machine scale set by using an Azure Resource Manager template.

You need to ensure that NGINX is available on all the virtual machines after they are deployed. What should you use?

- A. Deployment Center in Azure App Service
- B. A Desired State Configuration (DSC) extension
- C. the New-AzConfigurationAssignment cmdlet
- D. a Microsoft Intune device configuration profile

Answer: B

Explanation:

Azure virtual machine extensions are small packages that run post-deployment configuration and automation on Azure virtual machines.

In the following example, the Azure CLI is used to deploy a custom script extension to an existing virtual machine, which installs a Nginx webserver.

```
az vm extension set \
--resource-group myResourceGroup \
--vm-name myVM --name customScript \
--publisher Microsoft.Azure.Extensions \
--settings 'commandToExecute': "apt-get install -y nginx"
```

Note:

There are several versions of this question in the exam. The question has two correct answers:

1. a Desired State Configuration (DSC) extension
2. Azure Custom Script Extension

The question can have other incorrect answer options, including the following:

- ⇒ the Publish-AzVMDscConfiguration cmdlet
- ⇒ Azure Application Insights

Reference:

<https://docs.microsoft.com/en-us/azure/architecture/framework/devops/automation-configuration>

Question: 306

CertyIQ

HOTSPOT -

You deploy an Azure Kubernetes Service (AKS) cluster that has the network profile shown in the following exhibit.

Network profile

Type (plugin)	Basic (Kubnet)
Pod CIDR	10.244.0.0/16
Service CIDR	10.0.0.0/16
DNS service IP	10.0.0.10
Docker bridge CIDR	172.17.0.1/16

Network options

HTTP application routing

Enabled

Disabled

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Containers will be assigned an IP address in the [answer choice] subnet.

▼
10.244.0.0/16
10.0.0.0/16
172.17.0.1/16

Services in the AKS cluster will be assigned an IP address in the [answer choice] subnet.

▼
10.244.0.0/16
10.0.0.0/16
172.17.0.1/16

Answer:

Answer Area

Containers will be assigned an IP address in the [answer choice] subnet.

10.244.0.0/16
10.0.0.0/16
172.17.0.1/16

Services in the AKS cluster will be assigned an IP address in the [answer choice] subnet.

10.244.0.0/16
10.0.0.0/16
172.17.0.1/16

Explanation:

Box 1: 10.244.0.0/16 -

The Pod CIDR.

Note: The --pod-cidr should be a large address space that isn't in use elsewhere in your network environment. This range includes any on-premises network ranges if you connect, or plan to connect, your Azure virtual networks using Express Route or a Site-to-Site VPN connection.

This address range must be large enough to accommodate the number of nodes that you expect to scale up to. You can't change this address range once the cluster is deployed if you need more addresses for additional nodes.

Box 2: 10.0.0.0/16 -

The --service-cidr is used to assign internal services in the AKS cluster an IP address.

Reference:

<https://docs.microsoft.com/en-us/azure/aks/configure-kubenet>

Question: 307

CertyIQ

HOTSPOT -

You have the App Service plan shown in the following exhibit.

Default Auto created scale condition



Delete warning ⓘ The very last or default recurrence rule cannot be deleted. Instead, you can disable autoscale to turn off autoscale.

Scale mode Scale based on a metric Scale to a specific instance count

Scale out

When homepage (Maximum) CpuPercentage > 85 Increase count by 1

Rules

Scale in

When homepage (Average) CpuPercentage < 30 Decrease count by 1

[+ Add a rule](#)

Minimum

Maximum

Default

Instance limits

1

5

1

Schedule

This scale condition is executed when none of the other scale condition(s) match

The scale-in settings for the App Service plan are configured as shown in the following exhibit.

Operator *	Metric threshold to trigger scale action * ⓘ
<input type="text" value="Less than"/>	<input type="text" value="30"/> %
Duration (in minutes) * ⓘ	
<input type="text" value="5"/> ✓	
Time grain (in mins) ⓘ	Time grain statistic * ⓘ
1	<input type="text" value="Average"/> ✓
Action	
Operation *	
<input type="text" value="Decrease count by"/>	
Instance count *	Cool down (minutes) * ⓘ
<input type="text" value="1"/> ✓	<input type="text" value="5"/>

The scale out rule is configured with the same duration and cool down tile as the scale in rule.

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

NOTE: Each correct selection is worth one point.

Hot Area:

If after deployment CPU usage is 70 percent for one hour and then reaches 90 percent for five minutes, at that time the total number of instances will be [answer choice].

1
2
3
4
5

If after deployment the CPU maintains constant usage of 90 percent for one hour, and then the average CPU usage is below 25 percent for nine minutes, at that point the number of instances will be [answer choice].

1
2
3
4
5

Answer:

If after deployment CPU usage is 70 percent for one hour and then reaches 90 percent for five minutes, at that time the total number of instances will be [answer choice].

1
2
3
4
5

If after deployment the CPU maintains constant usage of 90 percent for one hour, and then the average CPU usage is below 25 percent for nine minutes, at that point the number of instances will be [answer choice].

1
2
3
4
5

Explanation:

Box 1: 2

70% for 1h, and then 90% for 5 minutes. So, from the default of 1 it will scale out 1 more. So, 2 in total.

Box 2: 4

90% for 1h and then 25% for 9minutes. So, from the default of 1 it will scale in to the max 5 ($60/5 = 12$, which means 6 times scale out, because we have 5 minutes period of cool down). Then when it drops to 25% for 9 minutes and it will scale in once after 5 mins (since the average of the last 5 minutes is under 30%), so it will decrease by 1, so 4 in total. Then it will have a cooldown of 5 minutes before scaling in again, but since only 4 minutes left from 9 minutes ($9-5 = 4$), it won't scale in again. So, 4 in total.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/learn/tutorial-autoscale-performance-schedule>

<https://docs.microsoft.com/en-us/azure/azure-monitor/autoscale/autoscale-understanding-settings>

CertyIQ

Question: 308

You have an Azure virtual machine named VM1 that runs Windows Server 2019. The VM was deployed using default drive settings.

You sign in to VM1 as a user named User1 and perform the following actions:

- ⇒ Create files on drive C.
- ⇒ Create files on drive D.
- ⇒ Modify the screen saver timeout.
- ⇒ Change the desktop background.

You plan to redeploy VM1.

Which changes will be lost after you redeploy VM1?

- A. the modified screen saver timeout
- B. the new desktop background
- C. the new files on drive D
- D. the new files on drive C

Answer: C

Explanation:

For Windows Server, the temporary disk is mounted as “D:\”.

For Linux based VM's the temporary disk is mounted as “/dev/sdb1”.

Reference:

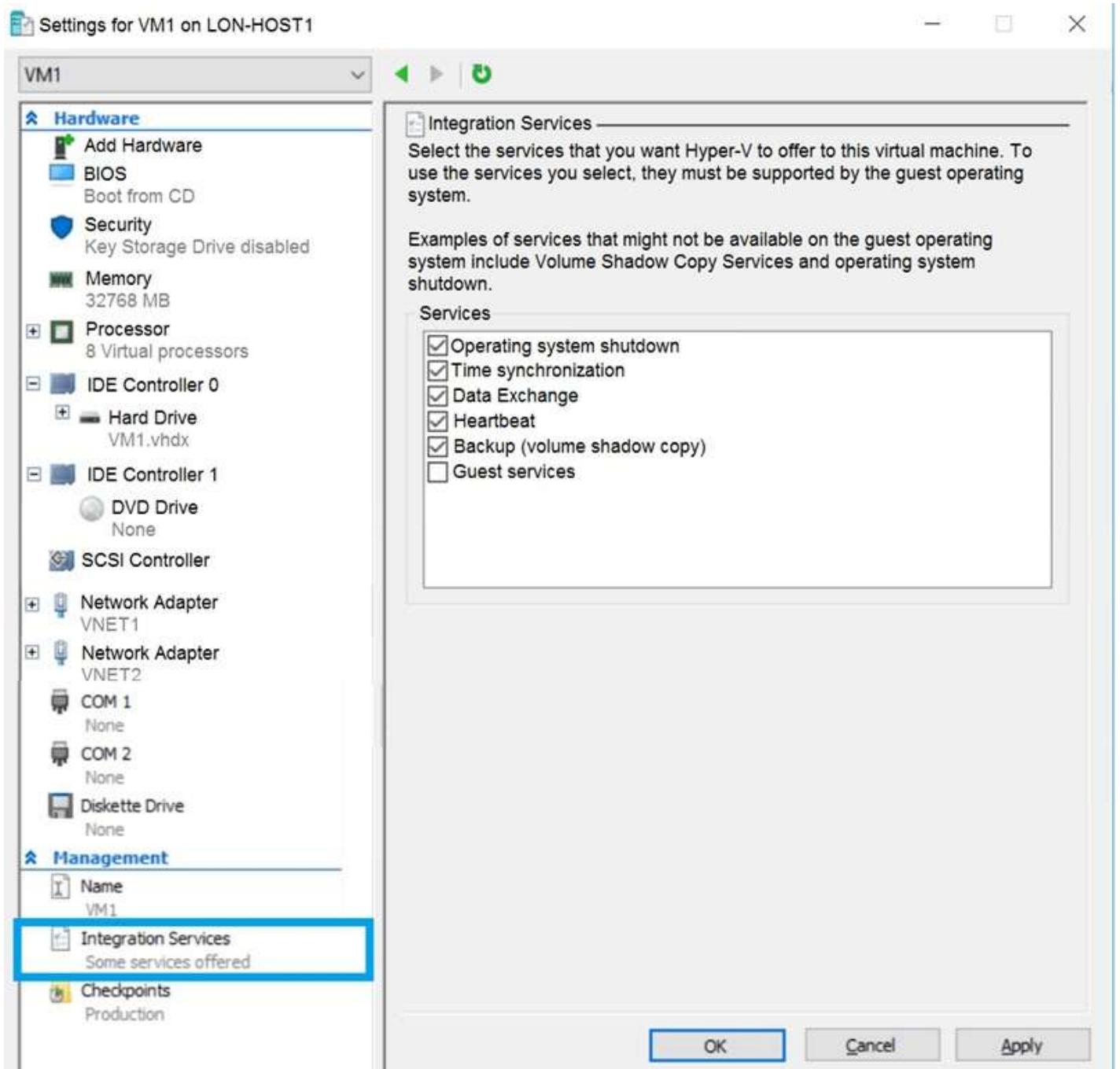
<https://www.cloudelicious.net/azure-vms-and-their-temporary-storage>

CertyIQ

Question: 309

You have an Azure subscription.

You have an on-premises virtual machine named VM1. The settings for VM1 are shown in the exhibit. (Click the Exhibit tab.)



You need to ensure that you can use the disks attached to VM1 as a template for Azure virtual machines. What should you modify on VM1?

- A. the memory
- B. the network adapters
- C. the hard drive
- D. the processor
- E. Integration Services

Answer: C

Explanation:

From the exhibit we see that the disk is in the VHDX format.

Before you upload a Windows virtual machine (VM) from on-premises to Microsoft Azure, you must prepare the virtual hard disk (VHD or VHDX). Azure supports only generation 1 VMs that are in the VHD file format and have a fixed sized disk. The maximum size allowed for the VHD is 1,023 GB. You can convert a generation 1 VM from the VHDX file system to VHD and from a dynamically expanding disk to fixed-sized.

Reference:

Question: 310

HOTSPOT -

You have an Azure subscription that contains a virtual machine scale set. The scale set contains four instances that have the following configurations:

- ⇒ Operating system: Windows Server 2016
- ⇒ Size: Standard_D1_v2

You run the get-azvmss cmdlet as shown in the following exhibit:

```
PS Azure:> (Get-AzVmss -Name WebProd -ResourceGroupName RG1).VirtualMachineProfile.OsProfile.WindowsConfiguration  
  
ProvisionVMAgent : True  
EnableAutomaticUpdates : False  
TimeZone :  
AdditionalUnattendContent :  
WinRM :  
  
Azure:/  
PS Azure:> Get-AzVmss -Name WebProd -ResourceGroupName RG1 | Select -ExpandProperty UpgradePolicy  
  
Mode RollingUpgradePolicy AutomaticOSUpgradePolicy  
-----  
Automatic Microsoft.Azure.Management.Compute.Models.AutomaticOSUpgradePolicy  
  
Azure:/  
PS Azure:> []
```

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

When an administrator changes the virtual machine size, the size will be changed on up to [answer choice] virtual machines simultaneously.

▼	
0	
1	
2	
4	

When a new build of the Windows Server 2016 image is released, the new build will be deployed to up to [answer choice] virtual machines simultaneously.

▼	
0	
1	
2	
4	

Answer:

Answer Area

When an administrator changes the virtual machine size, the size will be changed on up to [answer choice] virtual machines simultaneously.

▼
0
1
2
4

When a new build of the Windows Server 2016 image is released, the new build will be deployed to up to [answer choice] virtual machines simultaneously.

▼
0
1
2
4

Explanation:

Box 1: 4

If you resize the Scale Set all the VMs get resized at once, thus 4 is the correct answer.

Box 2: 1

Automatic OS updates update 20% of the VMs at once, with a minimum of 1 VM instance at a time. Also 20% of 4 = 0.8.

Reference:

<https://docs.microsoft.com/en-us/learn/modules/build-app-with-scale-sets/2-features-benefits-virtual-machine-scale-sets>

<https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-automatic-upgrade>

<https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-upgrade-scale-set>

Question: 311

CertyIQ

You have an Azure subscription named Subscription1 that is used by several departments at your company. Subscription1 contains the resources in the following table:

Name	Type
storage1	Storage account
RG1	Resource group
container1	Blob container
share1	File share

Another administrator deploys a virtual machine named VM1 and an Azure Storage account named storage2 by using a single Azure Resource Manager template.

You need to view the template used for the deployment.

From which blade can you view the template that was used for the deployment?

- A. VM1
- B. RG1
- C. storage2
- D. container1

Answer: B

Explanation:

View template from deployment history

1. Go to the resource group for your new resource group. Notice that the portal shows the result of the last deployment. Select this link.

The screenshot shows the 'Resource group' blade for a resource group named 'exportsite'. On the left, there's a navigation bar with 'Overview' selected. In the center, there's a summary card for 'Subscription name (change)' showing 'Microsoft Azure Consumption' and 'Subscription ID'. To the right, a 'Deployments' section is shown with a red box around the text '1 Succeeded'. Below this, there's a table with columns for 'DEPLOYMENT NAME' and 'STATUS'.

DEPLOYMENT NAME	STATUS
Microsoft.WebSiteSQLDatabased1...	Succeeded

2. You see a history of deployments for the group. In your case, the portal probably lists only one deployment. Select this deployment.

The screenshot shows the 'Deployment details' blade for the deployment 'Microsoft.WebSiteSQLDatabased1...'. At the top, there are buttons for 'Delete', 'Cancel', 'Redeploy', and 'View template'. Below this is a search bar. The main area displays the deployment details table, with the 'DEPLOYMENT NAME' row highlighted by a red box. The 'STATUS' column shows 'Succeeded' with a green checkmark icon.

DEPLOYMENT NAME	STATUS
Microsoft.WebSiteSQLDatabased1...	Succeeded

3. The portal displays a summary of the deployment. The summary includes the status of the deployment and its operations and the values that you provided for parameters. To see the template that you used for the deployment, select View template.

Microsoft.WebSiteSQLDatabase13386b0-9908
Deployment

Actions: Delete Cancel Refresh Redeploy View template

Summary:

- DEPLOYMENT DATE: 7/5/2017 4:01:15 PM
- STATUS: Succeeded
- DURATION: 1 minute 30 seconds
- RESOURCE GROUP: exportsite
- RELATED: Events

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-export-template>

Question: 312

CertyIQ

You have an Azure web app named App1. App1 has the deployment slots shown in the following table:

Name	Function
webapp1-prod	Production
webapp1-test	Staging

In webapp1-test, you test several changes to App1.

You back up App1.

You swap webapp1-test for webapp1-prod and discover that App1 is experiencing performance issues.

You need to revert to the previous version of App1 as quickly as possible.

What should you do?

- A. Redeploy App1
- B. Swap the slots
- C. Clone App1
- D. Restore the backup of App1

Answer: B

Explanation:

When you swap deployment slots, Azure swaps the Virtual IP addresses of the source and destination slots,

thereby swapping the URLs of the slots. We can easily revert the deployment by swapping back.

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/deploy-staging-slots>

CertyIQ

Question: 313

HOTSPOT -

You have an Azure subscription named Subscription1. Subscription1 contains two Azure virtual machines VM1 and VM2. VM1 and VM2 run Windows Server 2016.

VM1 is backed up daily by Azure Backup without using the Azure Backup agent.

VM1 is affected by ransomware that encrypts data.

You need to restore the latest backup of VM1.

To which location can you restore the backup? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

You can perform a file recovery of VM1 to:

- VM1 only
- VM1 or a new Azure virtual machine only
- VM1 and VM2 only
- A new Azure virtual machine only
- Any Windows computer that has Internet connectivity

You can restore VM1 to:

- VM1 only
- VM1 or a new Azure virtual machine only
- VM1 and VM2 only
- Any Windows computer that has Internet connectivity

Answer:

Answer Area

You can perform a file recovery of VM1 to:

VM1 only
VM1 or a new Azure virtual machine only
VM1 and VM2 only
A new Azure virtual machine only
Any Windows computer that has Internet connectivity

You can restore VM1 to:

VM1 only
VM1 or a new Azure virtual machine only
VM1 and VM2 only
Any Windows computer that has Internet connectivity

Explanation:

Box 1: Any Windows computer that has Internet connectivity

For files recovery, you download and run a windows executable to map a network drive. It can only run when the OS meets the requirements. Any computer running Windows Server 2016 or Windows 10 is suitable. File recovery can be done from any machine on the Internet.

Note: There might be compatibility issues with any Windows computer, so consider VM1 and VM2 only as an answer.

Box 2: VM1 or a new Azure virtual machine only

For restoring a VM, you can choose 'Create new' or 'Replace existing'.

Reference:

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-restore-files-from-vm>

<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/backup/backup-azure-restore-files-from-vm.md#for-windows-os>

Question: 314

CertyIQ

You plan to back up an Azure virtual machine named VM1.

You discover that the Backup Pre-Check status displays a status of Warning.

What is a possible cause of the Warning status?

- A. VM1 is stopped.
- B. VM1 does not have the latest version of the Azure VM Agent (WaAppAgent.exe) installed.
- C. VM1 has an unmanaged disk.
- D. A Recovery Services vault is unavailable.

Answer: B**Explanation:**

The Warning state indicates one or more issues in VM's configuration that might lead to backup failures and provides recommended steps to ensure successful backups. Not having the latest VM Agent installed, for example, can cause backups to fail intermittently and falls in this class of issues.

Reference:

<https://azure.microsoft.com/en-us/blog/azure-vm-backup-pre-checks/>

CertyIQ**Question: 315**

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 machine named VM1. VM1 was deployed by using a custom Azure Resource Manager template named ARM1.json.

You receive a notification that VM1 will be affected by maintenance.

You need to move VM1 to a different host immediately.

Solution: From the Overview blade, you move the virtual machine to a different resource group.

Does this meet the goal?

- A. Yes
- B. No

Answer: B**Explanation:**

You would need to redeploy the VM.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/redeploy-to-new-node>

CertyIQ**Question: 316****HOTSPOT -**

You have an Azure subscription.

You plan to use Azure Resource Manager templates to deploy 50 Azure virtual machines that will be part of the same availability set.

You need to ensure that as many virtual machines as possible are available if the fabric fails or during servicing.

How should you configure the template? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
{  
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",  
    "contentVersion": "1.0.0.0",  
    "parameters": {},  
    "resources": [  
        {  
            "type": "Microsoft.Compute/availabilitySets",  
            "name": "ha",  
            "apiVersion": "2017-12-01",  
            "location": "eastus",  
            "properties": {  
                "platformFaultDomainCount":  ,  
                "platformUpdateDomainCount":   
            }  
        }  
    ]  
}
```

Answer:

Answer Area

```
{  
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",  
    "contentVersion": "1.0.0.0",  
    "parameters": {},  
    "resources": [  
        {  
            "type": "Microsoft.Compute/availabilitySets",  
            "name": "ha",  
            "apiVersion": "2017-12-01",  
            "location": "eastus",  
            "properties": {  
                "platformFaultDomainCount":  ,  
                "platformUpdateDomainCount":   
            }  
        }  
    ]  
}
```

Explanation:

Box 1: 3 -

you can create 3 fault domains (max) in eastus, so the answer is 3 and 20, because the update domain max is 20.

Box 2: 20 -

Use 20 for platformUpdateDomainCount

Increasing the update domain (platformUpdateDomainCount) helps with capacity and availability planning when the platform reboots nodes. A higher number for the pool (20 is max) means that fewer of their nodes in any given availability set would be rebooted at once.

Reference:

<https://www.itprotoday.com/microsoft-azure/check-if-azure-region-supports-2-or-3-fault-domains-managed-disks> <https://github.com/Azure/acs-engine/issues/1030>

CertyIQ

Question: 317

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 machine named VM1 that runs Windows Server 2016.

You need to create an alert in Azure when more than two error events are logged to the System event log on VM1 within an hour.

Solution: You create an Azure Log Analytics workspace and configure the Agent configuration settings. You install the Microsoft Monitoring Agent on VM1. You create an alert in Azure Monitor and specify the Log Analytics workspace as the source.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Alerts in Azure Monitor can identify important information in your Log Analytics repository. They are created by alert rules that automatically run log searches at regular intervals, and if results of the log search match particular criteria, then an alert record is created and it can be configured to perform an automated response.

The Log Analytics agent collects monitoring data from the guest operating system and workloads of virtual machines in Azure, other cloud providers, and on-premises. It collects data into a Log Analytics workspace.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/learn/tutorial-response> <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agents-overview>

CertyIQ

Question: 318

HOTSPOT -

You have an Azure subscription.

You deploy a virtual machine scale set that is configured as shown in the following exhibit.

Create a virtual machine scale set

Basics Disks Networking Scaling Management Health Advanced

An Azure virtual machine scale set can automatically increase or decrease the number of VM instances that run your application. This automated and elastic behavior reduces the management overhead to monitor and optimize the performance of your application. [Learn more about VMSS scaling](#)

Instance

Initial instance count *



Scaling

Scaling policy

Manual

Custom

Minimum number of VMs *



Maximum number of VMs *



Scale out

CPU threshold (%) *



Duration in minutes *



Number of VMs to increase by *



Scale in

CPU threshold (%) *



Number of VMs to decrease by *



Diagnostic logs

Collect diagnostic logs from Autoscale Disabled Enabled

Scale-In policy

Configure the order in which virtual machines are selected for deletion during a scale-in operation.
[Learn more about scale-in policies.](#)

Scale-in policy

Default - balance across availability zones and fault domains, then delete V...

Use the drop-down menus to select the answer choice that answers each question based on the information presented in the graphic

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

At 9:00 AM, the scale set starts and CPU utilization is 90 percent for 15 minutes. How many virtual machine instances will be running at 9:15 AM?

	▼
2	
3	
4	
5	

At 10:00 AM, the scale set has five virtual machine instances running and CPU utilization falls to less than 15 percent for 60 minutes. How many virtual machine instances will be running at 11:00 AM?

	▼
1	
2	
3	
4	

Answer:

Answer Area

At 9:00 AM, the scale set starts and CPU utilization is 90 percent for 15 minutes. How many virtual machine instances will be running at 9:15 AM?

	▼
2	
3	
4	
5	

At 10:00 AM, the scale set has five virtual machine instances running and CPU utilization falls to less than 15 percent for 60 minutes. How many virtual machine instances will be running at 11:00 AM?

	▼
1	
2	
3	
4	

Explanation:

Box-1: 3

Initial starts 2 VM's 15 minutes have passed. at 10 minutes 1 VM was added we now have 3 VM's. Cool down is 5 Minutes before another 10 minute wait cycle starts so the answer is 3.

Box-2:1

Initial 5 VM's 60 minutes Pass. 1 VM removed every 15 minute cycle. 10 minutes wait timer plus 5 minute cool down equals 15 minutes cycle. Four 15 minute cycles pass equaling 60 minutes removing 4 VM's. We have 1 VM left.

Default Scale in and Out Default Durations are 10 minutes with 5 minute cool down.

The default scale set settings in Azure are:

- Minimum number of instances 1
- Maximum number of instances 10
- Scale out CPU threshold (%) 75
- Duration in minutes 10
- Number of instances to increase by 1
- Scale in CPU threshold (%) 25
- Number of instances to decrease by -1

Reference:

<https://learn.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-autoscale-portal#create-a-rule-to-automatically-scale-in>

Question: 319

CertyIQ

You have web apps in the West US, Central US and East US Azure regions.
You have the App Service plans shown in the following table.

Name	Operating system	Location	SKU and size
ASP1	Windows	West US	Standard S1
ASP2	Linux	Central US	Premium V2 P1v2
ASP3	Linux	East US	Premium V2 P1v2
ASP4	Linux	East US	Premium V2 P1v2

You plan to create an additional App Service plan named ASP5 that will use the Linux operating system.
You need to identify in which of the currently used locations you can deploy ASP5.
What should you recommend?

- A. West US, Central US, or East US
- B. Central US only
- C. East US only
- D. West US only

Answer: A

Explanation:

A. West US, Central US, or East US

Azure supports Linux App Service plans in a variety of regions, and West US, Central US, and East US are among those regions that commonly support Linux-based App Service plans. You can deploy ASP5 in any of these three locations.

CertyIQ

Question: 320

You plan to deploy several Azure virtual machines that will run Windows Server 2019 in a virtual machine scale set by using an Azure Resource Manager template.

You need to ensure that NGINX is available on all the virtual machines after they are deployed.

What should you use?

- A. the New-AzConfigurationAssignment cmdlet
- B. a Desired State Configuration (DSC) extension
- C. Azure Active Directory (Azure AD) Application Proxy
- D. Azure Application Insights

Answer: B

Explanation:

There are several versions of this question in the exam. The question has two correct answers:

1. a Desired State Configuration (DSC) extension
2. Azure Custom Script Extension

The question can have other incorrect answer options, including the following:

- ⇒ the Publish-AzVMDscConfiguration cmdlet
- ⇒ Azure Application Insights

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-overview>

CertyIQ

Question: 321

HOTSPOT -

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

Name	Type
ManagementGroup1	Management group
RG1	Resource group
9c8bc1cd-7655-4c66-b3ea-a8ee101d8f75	Subscription ID
Tag1	Tag

In Azure Cloud Shell, you need to create a virtual machine by using an Azure Resource Manager (ARM) template. How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

```
$adminPassword = Read-Host -Prompt "Enter the administrator password" -AsSecureString
```

New-AzVm
New-AzResource
New-AzTemplateSpec
New-AzResourceGroupDeployment

-Tag Tag1'
-ResourceGroupName RG1'
-GroupName ManagementGroup1'
-Subscription 9c8bc1cd-7655-4c66-b3ea-a8ee101d8f75

```
- TemplateUri "https://raw.githubusercontent.com/Azure/azure-quickstart-templates/master/101-vm-simple-windows/azuredeploy.json" `
```

```
- adminUsername LocalAdministrator -adminPassword $adminPassword -dnsLabelPrefix ContosoVM1
```

Answer:

```
$adminPassword = Read-Host -Prompt "Enter the administrator password" -AsSecureString
```

New-AzVm
New-AzResource
New-AzTemplateSpec
New-AzResourceGroupDeployment

-Tag Tag1'
-ResourceGroupName RG1'
-GroupName ManagementGroup1'
-Subscription 9c8bc1cd-7655-4c66-b3ea-a8ee101d8f75

```
- TemplateUri "https://raw.githubusercontent.com/Azure/azure-quickstart-templates/master/101-vm-simple-windows/azuredeploy.json" `
```

```
- adminUsername LocalAdministrator -adminPassword $adminPassword -dnsLabelPrefix ContosoVM1
```

Explanation:

Box 1: New-AzResourceGroupDeployment.

This cmdlet allows you to use a custom ARM template file to deploy resources to a resource group. For example:

```
New-AzResourceGroup -Name $resourceGroupName -Location "$location"
```

```
New-AzResourceGroupDeployment `
```

```
-ResourceGroupName $resourceGroupName `
```

```
-TemplateUri "https://raw.githubusercontent.com/Azure/azure-quickstart-templates/master/quickstarts/microsoft.compute/vm-simple-windows/azuredeploy.json" `
```

```
-adminUsername $adminUsername `
```

```
-adminPassword $adminPassword `
```

```
-dnsLabelPrefix $dnsLabelPrefix
```

Box 2: -ResourceGroupName RG1.

It's one of parameters of New-AzResourceGroupDeployment to specify to which resource group you want to deploy resources.

You could use New-AzVm to create a VM, but it doesn't use a template. You would need to provide all parameters in the command line.

Reference: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/ps-template>

<https://docs.microsoft.com/en-us/powershell/module/az.compute/new-azvm?view=azps-7.0.0>

<https://docs.microsoft.com/en-us/powershell/module/az.resources/new-azresourcegroupdeployment?view=azps-6.6.0>

Question: 322

CertyIQ

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 deploy an Azure Kubernetes Service (AKS) cluster named AKS1.

You need to deploy a YAML file to AKS1.

Solution: From Azure Cloud Shell, you run az aks.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

To deploy a YAML file, the command is:

kubectl apply -f <file_name>.yaml

Reference:

<https://docs.microsoft.com/en-us/azure/aks/kubernetes-walkthrough>

Question: 323

CertyIQ

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 machine named VM1 that runs Windows Server 2016.

You need to create an alert in Azure when more than two error events are logged to the System event log on VM1 within an hour.

Solution: You create an Azure Log Analytics workspace and configure the data settings. You add the Microsoft Monitoring Agent VM extension to VM1. You create an alert in Azure Monitor and specify the Log Analytics workspace as the source.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

You add the Microsoft Monitoring Agent VM extension to VM1 > This is WRONG

You Install the Microsoft Monitoring Agent VM agent to VM1 > This is Correct

1. Log analytics agent - Install in VM.
 2. Log analytics workspace - collect the log files from Log Analytics Agent.
 3. Azure Monitor - Create alert based on logs read from Log Analytics Workspace.
- Reference: <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agents-overview>

Question: 324

CertyIQ

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 machine named VM1 that runs Windows Server 2016.

You need to create an alert in Azure when more than two error events are logged to the System event log on VM1 within an hour.

Solution: You create an Azure Log Analytics workspace and configure the data settings. You install the Microsoft Monitoring Agent on VM1. You create an alert in

Azure Monitor and specify the Log Analytics workspace as the source.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Alerts in Azure Monitor can identify important information in your Log Analytics repository. They are created by alert rules that automatically run log searches at regular intervals, and if results of the log search match particular criteria, then an alert record is created and it can be configured to perform an automated response.

The Log Analytics agent collects monitoring data from the guest operating system and workloads of virtual machines in Azure, other cloud providers, and on-premises. It collects data into a Log Analytics workspace.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/learn/tutorial-response> <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agents-overview>

Question: 325

CertyIQ

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

Name	Type	Resource group	Location
Vault1	Recovery services vault	RG1	East US
VM1	Virtual machine	RG1	East US
VM2	Virtual machine	RG1	West US

All virtual machines run Windows Server 2016.

On VM1, you back up a folder named Folder1 as shown in the following exhibit.



Specify Backup Schedule (Files and Folders)

Getting started
Select Items to Backup
Specify Backup Schedu...
Select Retention Policy...
Choose Initial Backup T...
Confirmation
Modify Backup Progress

Define a schedule when you want to create a backup copy for selected files and folders

Schedule a backup every

Day Week

At following times (Maximum allowed is three times a day)

6:00 AM ▾

10:00 PM ▾

None ▾

You plan to restore the backup to a different virtual machine.

You need to restore the backup to VM2.

What should you do first?

- A. From VM1, install the Windows Server Backup feature.
- B. From VM2, install the Microsoft Azure Recovery Services Agent.
- C. From VM1, install the Microsoft Azure Recovery Services Agent.
- D. From VM2, install the Windows Server Backup feature.

Answer: B

Explanation:

From VM2, install the Microsoft Azure Recovery Services Agent: This is the correct step to take first because the Recovery Services Agent allows VM2 to interact with Azure Backup and restore the backup from Azure.

Reference:

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-restore-windows-server>

CertyIQ

Question: 326

HOTSPOT -

You have an Azure subscription.

You need to use an Azure Resource Manager (ARM) template to create a virtual machine that will have multiple data disks.

How should you complete the template? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
{  
  "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",  
  "parameters": {  
    "numberOfDataDisks": {  
      "type": "int",  
      "metadata": {  
        "description": "The number of dataDisks to create."  
      }  
    },  
    ...  
  },  
  "resources": [  
    {  
      "type": "Microsoft.Compute/virtualMachines",  
      "apiVersion": "2017-03-30",  
      ...  
      "properties": {  
        "storageProfile": {  
          ...  


|                |   |
|----------------|---|
| "copy": [      | ▼ |
| "copyIndex": [ | ▼ |
| "dependsOn": [ | ▼ |

  
          { "name": "dataDisks",  
            "count": "[parameters('numberOfDataDisks')]",  
            "input": {  
              "diskSizeGB": 1023,  
              "lun": 

|             |   |
|-------------|---|
| "[copy      | ▼ |
| "[copyIndex | ▼ |
| "[dependsOn | ▼ |

 ('dataDisks'))]  
            }  
          }  
        }  
      }  
      "createOption": "Empty"  
    }  
  ]  
}
```

Answer:

Answer Area

```
{  
  "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",  
  "parameters": {  
    "numberOfDataDisks": {  
      "type": "int",  
      "metadata": {  
        "description": "The number of dataDisks to create."  
      }  
    },  
    ...  
  },  
  "resources": [  
    {  
      "type": "Microsoft.Compute/virtualMachines",  
      "apiVersion": "2017-03-30",  
      ...  
      "properties": {  
        "storageProfile": {  
          ...  
  
          "copy": [  
            "copyIndex": [  
              "dependsOn": [  
  
                { "name": "dataDisks",  
                  "count": "[parameters('numberOfDataDisks')]",  
                  "input": {  
                    "diskSizeGB": 1023,  
                    "lun": [copy  
                            "[copyIndex  
                            "[dependsOn  
  
                    "createOption": "Empty"  
                  ...  
                }  
              ]  
            ]  
          ]  
        }  
      }  
    }  
  ]  
}
```

Explanation:

1. copy

2. copyIndex

<https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/copy-properties#syntax>

Add the copy element to the resources section of your template to set the number of items for a property. The copy element has the following general format:

- The count property specifies the number of iterations you want for the property

<https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/copy-properties#property-iteration>

Use the length function on the array to specify the count for iterations, and copyIndex to retrieve the current index in the array.

Question: 327

CertyIQ

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 subscription named Subscription1 that contains the resources shown in the following table.

Name	Type	Location	Resource group
RG1	Resource group	East US	<i>Not applicable</i>
RG2	Resource group	West Europe	<i>Not applicable</i>
RG3	Resource group	North Europe	<i>Not applicable</i>
VNET1	Virtual network	Central US	RG1
VM1	Virtual machine	West US	RG2

Subscription1 also includes a virtual network named VNET2. VM1 connects to a virtual network named VNET2 by using a network interface named NIC1.

You need to create a new network interface named NIC2 for VM1.

Solution: You create NIC2 in RG1 and West US.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

The virtual machine you attach a network interface to and the virtual network you connect it to must exist in the same location, here West US, also referred to as a region.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface>

Question: 328

CertyIQ

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 subscription named Subscription1 that contains the resources shown in the following table.

Name	Type	Location	Resource group
RG1	Resource group	East US	<i>Not applicable</i>
RG2	Resource group	West Europe	<i>Not applicable</i>
RG3	Resource group	North Europe	<i>Not applicable</i>
VNET1	Virtual network	Central US	RG1
VM1	Virtual machine	West US	RG2

Subscription1 also includes a virtual network named VNET2. VM1 connects to a virtual network named VNET2 by using a network interface named NIC1.

You need to create a new network interface named NIC2 for VM1.

Solution: You create NIC2 in RG2 and Central US.

Does this meet the goal?

A. Yes

B. No

Answer: B**Explanation:**

The virtual machine you attach a network interface to and the virtual network you connect it to must exist in the same location, here West US, also referred to as a region.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface>

Question: 329**CertyIQ**

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 subscription named Subscription1 that contains the resources shown in the following table.

Name	Type	Location	Resource group
RG1	Resource group	East US	<i>Not applicable</i>
RG2	Resource group	West Europe	<i>Not applicable</i>
RG3	Resource group	North Europe	<i>Not applicable</i>
VNET1	Virtual network	Central US	RG1
VM1	Virtual machine	West US	RG2

Subscription1 also includes a virtual network named VNET2. VM1 connects to a virtual network named VNET2 by using a network interface named NIC1.

You need to create a new network interface named NIC2 for VM1.

Solution: You create NIC2 in RG2 and West US.

Does this meet the goal?

A. Yes

B. No

Answer: A**Explanation:**

The virtual machine you attach a network interface to and the virtual network you connect it to must exist in the same location, here West US, also referred to as a region.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface>

Question: 330**CertyIQ**

You develop the following Azure Resource Manager (ARM) template to create a resource group and deploy an Azure Storage account to the resource group.

```

{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "resources": [
        {
            "type": "Microsoft.Resources/resourceGroups",
            "apiVersion": "2018-05-01",
            "location": "eastus",
            "name": "RG1"
        },
        {
            "type": "Microsoft.Resources/deployments",
            "apiVersion": "2017-05-10",
            "name": "storageDeployment",
            "resourceGroup": "RG1",
            "dependsOn": [
                "[resourceId('Microsoft.Resources/resourceGroups/', 'RG1')]"
            ],
            "properties": {
                "mode": "Incremental",
                "template": {
                    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
                    "contentVersion": "1.0.0.0",
                    "resources": [
                        {
                            "type": "Microsoft.Storage/storageAccounts",
                            "apiVersion": "2017-10-01",
                            "name": "storage1",
                            "location": "eastus",
                            "kind": "StorageV2",
                            "sku": {
                                "name": "Standard_LRS"
                            }
                        }
                    ]
                }
            }
        }
    ]
}

```

Which cmdlet should you run to deploy the template?

- A. New-AzResource
- B. New-AzResourceGroupDeployment
- C. New-AzTenantDeployment
- D. New-AzDeployment

Answer: D

Explanation:

Answer D: New-AzDeployment.

To add resources to a resource group, use the New-AzResourceGroupDeployment which creates a deployment at a resource group. The New-AzDeployment cmdlet creates a deployment at the current subscription scope, which deploys subscription level resources.

Reference:

<https://learn.microsoft.com/en-us/powershell/module/az.resources/new-azdeployment?view=azps-9.7.0>

Question: 331

CertyIQ

HOTSPOT -

You have an Azure App Service app named WebApp1 that contains two folders named Folder1 and Folder2. You need to configure a daily backup of WebApp1. The solution must ensure that Folder2 is excluded from the backup.

What should you create first, and what should you use to exclude Folder2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

First create:

- An Azure Storage account
- A Backup vault
- A Recovery Services vault
- A resource group

To exclude Folder2, use:

- A _backup.filter file
- A backup policy
- A lock
- A WebJob

Answer:

Answer Area

First create:

- An Azure Storage account
- A Backup vault
- A Recovery Services vault
- A resource group

To exclude Folder2, use:

- A _backup.filter file
- A backup policy
- A lock
- A WebJob

Explanation:

Box 1: An Azure Storage account -

App Service can back up the following information to an Azure storage account and container that you have configured your app to use.

App configuration -

File content -

Database connected to your app -

Note: Choose your backup destination by selecting a Storage Account and Container. The storage account must belong to the same subscription as the app you want to back up. If you wish, you can create a new storage account or a new container in the respective pages.

Box 2: A _backup.filter file -

Exclude files from your backup.

Suppose you have an app that contains log files and static images that have been backup once and are not going to change. In such cases, you can exclude those folders and files from being stored in your future backups. To exclude files and folders from your backups, create a _backup.filter file in the D:\home\site\wwwroot folder of your app. Specify the list of files and folders you want to exclude in this file.

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/manage-backup>

CertyIQ**Question: 332**

You plan to deploy several Azure virtual machines that will run Windows Server 2019 in a virtual machine scale set by using an Azure Resource Manager template.

You need to ensure that NGINX is available on all the virtual machines after they are deployed.

What should you use?

- A. the Publish-AzVMDscConfiguration cmdlet
- B. Azure Application Insights
- C. Azure Custom Script Extension
- D. a Microsoft Endpoint Manager device configuration profile

Answer: C**Explanation:**

Use Azure Resource Manager templates to install applications into virtual machine scale sets with the Custom Script Extension.

Note: The Custom Script Extension downloads and executes scripts on Azure VMs. This extension is useful for post deployment configuration, software installation, or any other configuration / management task.

To see the Custom Script Extension in action, create a scale set that installs the NGINX web server and outputs the hostname of the scale set VM instance.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/tutorial-install-apps-template>

CertyIQ**Question: 333**

HOTSPOT -

You have an Azure subscription. The subscription contains a virtual machine that runs Windows 10.

You need to join the virtual machine to an Active Directory domain.

How should you complete the Azure Resource Manager (ARM) template? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
{  
    "apiVersion": "2017-03-30",  
    "type": "Microsoft.Compute/VirtualMachines",  
    "name": "[concat(parameters('VName'), '/joindomain')]",  
    "location": "[parameter('location')]",  
    "properties": {  
        "publisher": "Microsoft.Compute",  
        "type": "JsonADDomainExtension",  
        "typeHandlerVersion": "1.3",  
        "autoUpgradeMinorVersion": true,  
        "settings": {  
            "Name": "[parameters('domainName')]",  
            "User": "[parameters('domainusername')]",  
            "Restart": "true",  
            "Options": "3"  
        },  
        "ProtectedSettings": {  
            "Settings": {},  
            "Statuses": {}  
        },  
        "Password": "[parameters('domainPassword')]"  
    }  
}
```

Answer:

Answer Area

```
{  
    "apiVersion": "2017-03-30",  
    "type": "Microsoft.Compute/VirtualMachines",  
    "name": "[concat(parameters('VName'), '/joindomain')]",  
    "location": "[parameter('location')]",  
    "properties": {  
        "publisher": "Microsoft.Compute",  
        "type": "JsonADDomainExtension",  
        "typeHandlerVersion": "1.3",  
        "autoUpgradeMinorVersion": true,  
        "settings": {  
            "Name": "[parameters('domainName')]",  
            "User": "[parameters('domainusername')]",  
            "Restart": "true",  
            "Options": "3"  
        },  
        "ProtectedSettings": {  
            "Settings": {},  
            "Statuses": {}  
        }  
    }  
}
```

Explanation:

Box 1: "Microsoft.Compute/VirtualMachines/extensions",

The following JSON example uses the Microsoft.Compute/virtualMachines/extensions resource type to install the Active Directory domain join extension.

Parameters are used that you specify at deployment time. When the extension is deployed, the VM is joined to the specified managed domain.

Box 2: "ProtectedSettings":

Example:

```
"apiVersion": "2015-06-15",  
"type": "Microsoft.Compute/virtualMachines/extensions",  
"name": "[concat(parameters('dnsLabelPrefix'), '/joindomain')]",  
"location": "[parameters('location')]",  
"dependsOn": [  
    "[concat('Microsoft.Compute/virtualMachines/', parameters('dnsLabelPrefix'))]"
```

```

],
"properties":
"publisher": "Microsoft.Compute",
"type": "JsonADDomainExtension",
"typeHandlerVersion": "1.3",
"autoUpgradeMinorVersion": true,
"settings":
"Name": "[parameters('domainToJoin')]",
"OUPath": "[parameters('ouPath')]",
"User": "[concat(parameters('domainToJoin'), '\\\\', parameters('domainUsername'))]",
"Restart": "true",
"Options": "[parameters('domainJoinOptions')]"
,
"protectedSettings":
"Password": "[parameters('domainPassword')]"

```

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/join-windows-vm-template>

Question: 334

CertyIQ

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

Name	Type	Resource group	Location
RG1	Resource group	<i>Not applicable</i>	Central US
RG2	Resource group	<i>Not applicable</i>	West US
VMSS1	Virtual machine scale set	RG2	West US
Proximity1	Proximity placement group	RG1	West US
Proximity2	Proximity placement group	RG2	Central US
Proximity3	Proximity placement group	RG1	Central US

You need to configure a proximity placement group for VMSS1.

Which proximity placement groups should you use?

- A. Proximity2 only
- B. Proximity1, Proximity2, and Proximity3
- C. Proximity1 only
- D. Proximity1 and Proximity3 only

Answer: A

Explanation:

- A. Proximity2 only.

Using a single proximity placement group (Proximity2) for VMSS1 ensures that all instances of VMSS1 are placed as close to each other as possible, which reduces network latency and increases performance.

HOTSPOT

You are creating an Azure Kubernetes Services (AKS) cluster as shown in the following exhibit.

Create Kubernetes cluster

...



Validation passed

Basics

Subscription	Visual Studio Premium with MSDN
Resource group	RG1
Region	West Europe
Kubernetes cluster name	AKS1
Kubernetes version	1.20.9

Node pools

Node pools	1
Enable virtual nodes	Disabled
Enable virtual machine scale sets	Enabled

Authentication

Authentication method	Service principal
Role-based access control (RBAC)	Enabled
AKS-managed Azure Active Directory	Disabled
Encryption type	(Default) Encryption at-rest with a platform-managed key

Networking

Network configuration	Kubenet
DNS name prefix	AKS1-dns
Load balancer	Standard
Private cluster	Disabled
Authorized IP ranges	Disabled
Network policy	None
HTTP application routing	No

[Create](#)[< Previous](#)[Next >](#)[Download a template for automation](#)

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

NOTE: Each correct selection is worth one point.

Answer Area

To ensure that you can create Windows containers in AKS1, you must [answer choice].

enable virtual nodes
increase the number of node pools
modify the Kubernetes version setting
modify the Network configuration setting

To ensure that you can integrate AKS1 with an Azure container registry, you must modify the [answer choice] setting.

AKS-managed Azure Active Directory
Authentication method
Authorized IP ranges
Kubernetes version
Network configuration

Answer:

Answer Area

To ensure that you can create Windows containers in AKS1, you must [answer choice].

enable virtual nodes
increase the number of node pools
modify the Kubernetes version setting
modify the Network configuration setting

To ensure that you can integrate AKS1 with an Azure container registry, you must modify the [answer choice] setting.

AKS-managed Azure Active Directory
Authentication method
Authorized IP ranges
Kubernetes version
Network configuration

Explanation:

1) Modify the Network configuration setting

"To run an AKS cluster that supports node pools for Windows Server containers, your cluster needs to use a network policy that uses Azure CNI (advanced) network plugin."

2) AKS-Managed Azure Active Directory

Reference:

<https://learn.microsoft.com/en-us/azure/aks/cluster-container-registry-integration?tabs=azure-cli>

<https://learn.microsoft.com/en-us/azure/aks/learn/quick-windows-container-deploy-cli>

HOTSPOT

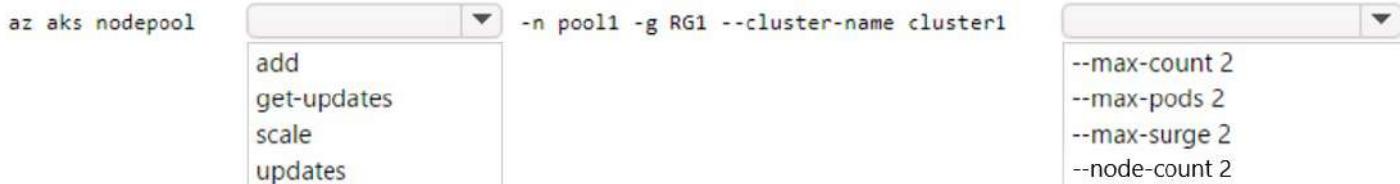
You have an Azure subscription that contains an Azure Kubernetes Service (AKS) cluster named Cluster1. Cluster1 hosts a node pool named Pool1 that has four nodes.

You need to perform a coordinated upgrade of Cluster1. The solution must meet the following requirements:

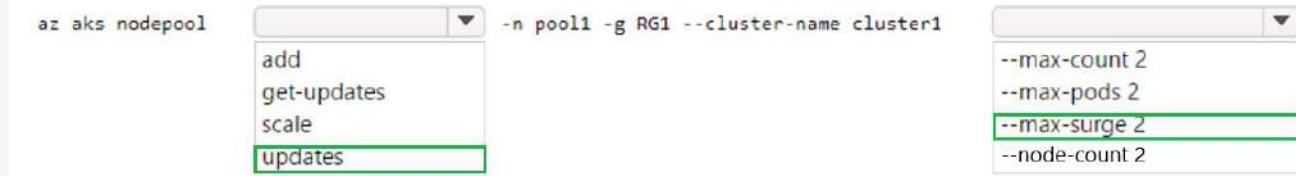
- Deploy two new nodes to perform the upgrade.
- Minimize costs.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



Explanation:

1. updates
2. --max-surge 2

<https://learn.microsoft.com/en-us/cli/azure/aks/nodepool?view=azure-cli-latest#az-aks-nodepool-update>

Update a node pool properties.

<https://learn.microsoft.com/en-us/cli/azure/aks/nodepool?view=azure-cli-latest#az-aks-nodepool-update-optional-parameters>

max-surge

- Extra nodes used to speed upgrade. When specified, it represents the number or percent used, eg. 5 or 33%.

Question: 337

HOTSPOT

You have an Azure subscription.

You create the following file named Deploy.json.

```
{  
    "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",  
    "contentVersion": "1.0.0.0",  
    "parameters": {  
        "location": {  
            "type": "string",  
            "defaultValue": "westus"  
        }  
    },  
    "resources": [  
        {  
            "apiVersion": "2019-04-01",  
            "type": "Microsoft.Storage/storageAccounts",  
            "name": "[concat(copyIndex(), 'storage', uniqueString(resourceGroup().id))]",  
            "location": "[resourceGroup().location]",  
            "sku": {  
                "name": "Premium_LRS"  
            },  
            "kind": "StorageV2",  
            "properties": {},  
            "copy": {  
                "name": "storagecopy",  
                "count": 3  
            }  
        }  
    ]  
}
```

You connect to the subscription and run the following commands.

```
New-AzResourceGroup -Name RG1 -Location "centralus"  
New-AzResourceGroupDeployment -ResourceGroupName RG1 -TemplateFile "deploy.json"
```

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
The commands will create four new resources.	<input type="radio"/>	<input type="radio"/>
The commands will create storage accounts in the West US Azure region.	<input type="radio"/>	<input type="radio"/>
The first storage account that is created will have a prefix of 0.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements

Yes No

The commands will create four new resources.

The commands will create storage accounts in the West US Azure region.

The first storage account that is created will have a prefix of 0.

Explanation:

Yes : The 4 resources created are the RG1 resource group + the 3 storage accounts

No: the location of the storage accounts is defined by the parameter "location" in the "resources" item that has the value of the Resource Group (stated by the "resourceGroup().location" function that returns the location of the resource group RG1 which is in Central US)

Yes: the names of the storages account have the prefix given by the copyIndex() function in "name": "[concat(copyIndex(),'storage',uniqueString(resourceGroup().id))]", which starts at the position 0

Question: 338

CertyIQ

You plan to deploy several Azure virtual machines that will run Windows Server 2019 in a virtual machine scale set by using an Azure Resource Manager template.

You need to ensure that NGINX is available on all the virtual machines after they are deployed.

What should you use?

- A. Azure Custom Script Extension
- B. Deployment Center in Azure App Service
- C. the Publish-AzVMDscConfiguration cmdlet
- D. the New-AzConfigurationAssignment cmdlet

Answer: A

Explanation:

A. Azure Custom Script Extension.

Azure Custom Script Extension: This extension can be used to download and execute scripts on Azure VMs during their provisioning. You can provide a script to install NGINX on the virtual machines as part of the deployment process.

Question: 339

CertyIQ

HOTSPOT

-

You have an Azure subscription that contains a resource group named RG1.

You plan to use an Azure Resource Manager (ARM) template named template1 to deploy resources. The solution must meet the following requirements:

- Deploy new resources to RG1.
- Remove all the existing resources from RG1 before deploying the new resources.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

```
New-AzResourceGroupDeployment -TemplateUri  
"https://contoso.com/template1" -TemplateParameterfile
```

params.json

RG1 -Mode

- Name
- QueryString
- ResourceGroupName
- Tag

- All
- Complete
- Incremental

Answer:

```
New-AzResourceGroupDeployment -TemplateUri  
"https://contoso.com/template1" -TemplateParameterfile
```

params.json

RG1 -Mode

- Name
- QueryString
- ResourceGroupName**
- Tag

- All
- Complete**
- Incremental

Explanation:

1. -ResourceGroupName

2. Complete

<https://learn.microsoft.com/en-us/powershell/module/az.resources/new-azresourcegroupdeployment?view=azps-9.3.0#-resourcegroupname>

Specifies the name of the resource group to deploy.

<https://learn.microsoft.com/en-us/powershell/module/az.resources/new-azresourcegroupdeployment?view=azps-9.3.0#-mode>

Specifies the deployment mode. The acceptable values for this parameter are:

-Complete: In complete mode, Resource Manager deletes resources that exist in the resource group but are not specified in the template.

- Incremental: In incremental mode, Resource Manager leaves unchanged resources that exist in the resource

group but are not specified in the template.

CertyIQ

Question: 340

HOTSPOT

You have an Azure App Service web app named app1.

You configure autoscaling as shown in following exhibit.

Default* Auto created scale condition 

Delete warning  The very last or default recurrence rule cannot be deleted. Instead, you can disable autoscale to turn off autoscale.

Scale mode  Scale based on a metric Scale to a specific instance count

Rules  It is recommended to have at least one scale in rule. To create new rules, click [Add a rule](#).

Scale out

When  (Average) CpuPercentage > 70 Increase count by 1

[+ Add a rule](#)

Instance limits

Minimum 	Maximum 	Default 
1 	5 	1 

Schedule  This scale condition is executed when none of the other scale condition(s) match

You configure the autoscale rule criteria as shown in the following exhibit.

Criteria

Time aggregation *

Maximum

Metric namespace *

App Service plans standard metrics

Metric name

CPU Percentage

1 minute time grain

Dimension Name

Operator

Dimension Values

Add

Instance

=

All values

If you select multiple values for a dimension, autoscale will aggregate the metric across the selected values, not evaluate the metric for each values individually.



CpuPercentage (Maximum)

1.67 %

Enable metric divide by instance count

Operator *

Metric threshold to trigger scale action *

Greater than

70

%

Duration (minutes) *

10

Time grain (minutes)

Time grain statistic *

1

Average

Action

Operation *

Cool down (minutes) *

Increase count by

5

Instance count *

1

Use the drop-down menus to select the answer choice that answers each question based on the information

presented in the graphic.

NOTE: Each correct selection is worth one point.

After CPU usage has reached 80 percent for 15 minutes, [answer choice] will be running.

- 1 instance
- 2 instances
- 3 instances
- 4 instances
- 5 instances

Once the first scale-out instance is created, the minimum time before an additional instance is created will be [answer choice].

- 1 minute
- 5 minutes
- 10 minutes
- 15 minutes

Answer:

After CPU usage has reached 80 percent for 15 minutes, [answer choice] will be running.

- 1 instance
- 2 instances
- 3 instances
- 4 instances
- 5 instances

Once the first scale-out instance is created, the minimum time before an additional instance is created will be [answer choice].

- 1 minute
- 5 minutes
- 10 minutes
- 15 minutes

Explanation:

After CPU usage has reached 80 percent for 15 minutes, [answer choice] will be running.

2 instances.

This indicates that autoscaling is enabled, and when CPU utilization exceeds 80% for 15 minutes, the system scales out by adding an additional instance.

If initially only one instance was running, then scaling up will increase the total count to 2 instances.

This is a common threshold-based scaling policy used in cloud environments to optimize performance and availability.

Once the first scale-out instance is created, the minimum time before an additional instance is created will be [answer choice].

15 minutes.

The scale-out cooldown period determines how long the system waits before adding another instance after the first scale-out.

A 15-minute delay ensures the system does not aggressively add new instances too quickly, preventing unnecessary costs and system instability.

This setting is useful in preventing rapid oscillations in scaling activity.

Question: 341

You have an Azure subscription.

You plan to deploy the Azure container instances shown in the following table.

Name	Operating system
Instance1	Nano Server installation of Windows Server 2019
Instance2	Server Core installation of Windows Server 2019
Instance3	Linux
Instance4	Linux

Which instances can you deploy to a container group?

- A. Instance1 only
- B. Instance2 only
- C. Instance1 and Instance2 only
- D. Instance3 and Instance4 only

Answer: D**Explanation:**

Multi-container groups currently support only Linux containers. For Windows containers, Azure Container Instances only supports deployment of a single container instance. While we are working to bring all features to Windows containers, you can find current platform differences in the service

Reference:

<https://learn.microsoft.com/en-us/azure/container-instances/container-instances-container-groups>

Question: 342

You plan to deploy several Azure virtual machines that will run Windows Server 2019 in a virtual machine scale set by using an Azure Resource Manager template.

You need to ensure that NGINX is available on all the virtual machines after they are deployed.

What should you use?

- A. Azure Custom Script Extension
- B. Deployment Center in Azure App Service
- C. the New-AzConfigurationAssignment cmdlet
- D. Azure AD Application Proxy

Answer: A**Explanation:**

The Custom Script Extension downloads and runs scripts on Azure virtual machines (VMs). This extension is useful for post-deployment configuration, software installation, or any other configuration or management task. You can download scripts from Azure Storage or GitHub, or provide them to the Azure portal at extension runtime.

Question: 343

CertyIQ

You have an Azure subscription that has the public IP addresses shown in the following table.

Name	IP version	SKU	Tier	IP address assignment
IP1	IPv4	Standard	Regional	Static
IP2	IPv4	Standard	Global	Static
IP3	IPv4	Basic	Regional	Dynamic
IP4	IPv4	Basic	Regional	Static
IP5	IPv6	Standard	Regional	Static

You plan to deploy an Instance of Azure Firewall Premium named FW1.

Which IP addresses can you use?

- A. IP2 only
- B. IP1 and IP2 only
- C. IP1, IP2, and IP5 only
- D. IP1, IP2, IP4, and IP5 only

Answer: B

Explanation:

Azure Firewall

- Dynamic IPv4: No
- Static IPv4: Yes
- Dynamic IPv6: No
- Static IPv6: No

Azure Firewall is a cloud-based network security service that protects your Azure Virtual Network resources. Azure Firewall requires at least one public static IP address to be configured. This IP or set of IPs are used as the external connection point to the firewall. Azure Firewall supports standard SKU public IP addresses. Basic SKU public IP address and public IP prefixes aren't supported.

Reference:

<https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-addresses#at-a-glance>

Azure Firewall

- Dynamic IPv4: No

- Static IPv4: Yes
- Dynamic IPv6: No
- Static IPv6: No

<https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/configure-public-ip-firewall>

Azure Firewall is a cloud-based network security service that protects your Azure Virtual Network resources. Azure Firewall requires at least one public static IP address to be configured. This IP or set of IPs are used as the external connection point to the firewall. Azure Firewall supports standard SKU public IP addresses. Basic SKU public IP address and public IP prefixes aren't supported.

Reference:

<https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/configure-public-ip-firewall>

<https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-addresses#at-a-glance>

Azure Firewall

Question: 344

CertyIQ

HOTSPOT

-

You have an Azure subscription.

You need to deploy a virtual machine by using an Azure Resource Manager (ARM) template.

How should you complete the template? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

```
{  
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",  
    ...  
    "type": "Microsoft.Compute/virtualMachines",  
    ...  
    "dependsOn": [  
        "[  
            reference  
            resourceId  
            Union  
        ]",  
        "properties": {  
            "storageProfile": {  
                "  
                    [  
                        Array  
                        Image  
                        ImageReference  
                        vhd  
                    ]": {  
                        "publisher": "MicrosoftWindowsServer",  
                        "Offer": "WindowsServer",  
                        "sku": "2019-Datacenter",  
                        "version": "latest"  
                    }  
            }  
        }  
    }  
}
```

Answer:

Answer Area

```
{  
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",  
    ...  
    "type": "Microsoft.Compute/virtualMachines",  
    ...  
    "dependsOn": [  
        "[  
            reference  
            resourceId  
            Union  
        ]",  
        "properties": {  
            "storageProfile": {  
                "  
                    [  
                        Array  
                        Image  
                        ImageReference  
                        vhd  
                    ]": {  
                        "publisher": "MicrosoftWindowsServer",  
                        "Offer": "WindowsServer",  
                        "sku": "2019-Datacenter",  
                        "version": "latest"  
                    }  
            }  
        }  
    }  
}
```

Explanation:

resourceId.

resourceId is used to dynamically retrieve the ID of an existing resource.

Ensures the VM references the correct network interface (NIC).

resourceId dynamically retrieves the ID of an existing network interface (NIC).

imageReference.

imageReference defines the OS image for the VM.

imageReference ensures the VM uses the correct Windows Server 2019 OS image.

Question: 345**CertyIQ**

HOTSPOT

-

You need to configure a new Azure App Service app named WebApp1. The solution must meet the following requirements:

- WebApp1 must be able to verify a custom domain name of app.contoso.com.
- WebApp1 must be able to automatically scale up to eight instances.
- Costs and administrative effort must be minimized.

Which pricing plan should you choose, and which type of record should you use to verify the domain? To answer, select the appropriate options in the answer area.

NOTE: Each correct answer is worth one point.

Answer Area

Pricing plan:

- Basic
- Free
- Shared
- Standard

Record type:

- A
- AAAA
- PTR
- TXT

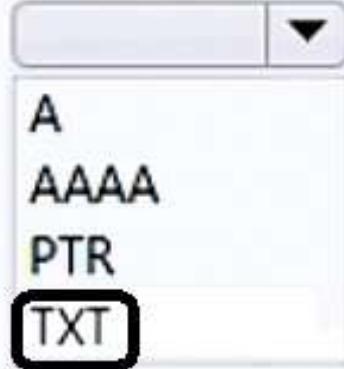
Answer:

Answer Area

Pricing plan:



Record type:



Explanation:

Pricing Plan: Standard.

Record Type: TXT.

WebApp1 must be able to verify a custom domain name of app.contoso.com. All paid tiers (Basic, Standard, Premium, Isolated) allow for custom domains.

WebApp1 must be able to automatically scale up to eight instances. Auto-scaling is a feature that is available in the Standard, Premium, and Isolated tiers. It is not available in the Basic tier, which allows you to manually scale up to 3 instances.

Costs and administrative effort must be minimized.

Pricing Plan: Given these requirements, the best option is the "Standard" tier. It offers both auto-scaling and custom domains, while being less expensive than the Premium or Isolated tiers. The Basic tier does not support auto-scaling, and the Free and Shared tiers do not support custom domains or auto-scaling.

For verifying a custom domain, Azure uses a CNAME or TXT record. The A record cannot be used for domain verification

Question: 346

HOTSPOT

-

You have an Azure subscription that contains the virtual machines shown in the following table.

CertyIQ

Name	Location	vCPUs	Generation
VM1	West Europe	8	2
VM2	East US	2	1
VM3	West US	12	1

You create an Azure Compute Gallery named ComputeGallery1 as shown in the Azure Compute Gallery exhibit.
(Click the Azure Compute Gallery tab.)

Create Azure compute gallery



Basics Sharing Tags Review + create

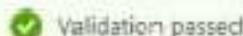
Basics

Subscription	Azure Pass - Sponsorship
Resource group	RG1
Region	West Europe
Name	ComputeGallery1
Description	None

In ComputeGallery1, you create a virtual machine image definition named Image1 as shown in the image definition exhibit.
(Click the Image Definition tab.)

Create a VM image definition

...



Basics Version Publishing options Tags Review + create

Basics

Subscription	Azure Pass - Sponsorship
Resource group	RG1
Region	East US
Target Azure compute gallery	ComputeGallery1
VM image definition name	Image1
OS type	Windows
Security type	Standard
VM generation	V1
OS state	Specialized
Publisher	Contoso
Offer	WindowsServer2022
SKU	Datacenter

Publishing options

Product name	None
License terms link	None
Description	None
Release notes URI	None
Privacy terms URI	None
Purchase plan name	None
Purchase plan publisher name	None
Recommended VM vCPUs	4-16
Recommended VM memory	1-32 GB
Excluded disk types	None
VM image definition end of life date	None

For each of the following statements, select Yes if the statement is true. Otherwise, select No,

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
The operating system disk of VM1 can be used as a source for a version of Image1.	<input type="radio"/>	<input type="radio"/>
The operating system disk of VM2 can be used as a source for a version of Image1.	<input type="radio"/>	<input type="radio"/>
The operating system disk of VM3 can be used as a source for a version of Image1.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
The operating system disk of VM1 can be used as a source for a version of Image1.	<input type="radio"/>	<input checked="" type="checkbox"/>
The operating system disk of VM2 can be used as a source for a version of Image1.	<input checked="" type="checkbox"/>	<input type="radio"/>
The operating system disk of VM3 can be used as a source for a version of Image1.	<input type="radio"/>	<input checked="" type="checkbox"/>

Explanation:

Box 1- NO

VM gen 2 is not directly supported for image definition with v1. Image & VM source regions doesn't match.

Box 2 - YES

VM generations matches, along with image & VM source region.

Box 3 - NO

VM generations matches, but image & VM source region doesn't.

Reference:

<https://learn.microsoft.com/en-us/azure/virtual-machines/shared-image-galleries?tabs=azure-cli#how-do-i-specify-the-source-region-while-creating-the-image-version>

Question: 347

CertyIQ

You plan to create the Azure web apps shown in the following table.

Name	Runtime stack
WebApp1	.NET 6 (LTS)
WebApp2	ASP.NET V4.8
WebApp3	PHP 8.1
WebApp4	Python 3.11

What is the minimum number of App Service plans you should create for the web apps?

- A.1
- B.2
- C.3
- D.4

Answer: B

Explanation:

Correct Answer: B.NET: Windows and Linux ASP.NET: Windows only PHP: Windows and Linux Python: Windows and Linux Also, you can't use Windows and Linux Apps in the same App Service Plan, because when you create a new App Service plan you have to choose the OS type. You can't mix Windows and Linux apps in the same App Service plan. So, you need 2 ASPs.

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/overview>

Question: 348

CertyIQ

HOTSPOT

-

You have an Azure subscription that contains the resource groups shown in the following table.

Name	Location
RG1	East US
RG2	West US

You create the following Azure Resource Manager (ARM) template named deploy.json.

```
{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {},
  "variables": {},
  "resources": [
    {
      "type": "Microsoft.Resources/resourceGroups",
      "apiVersion": "2018-05-01",
      "location": "eastus",
      "name": "[concat('RG', copyIndex())]",
      "copy": {
        "name": "copy",
        "count": 4
      }
    }
  ],
  "outputs": {}
}
```

You deploy the template by running the following cmdlet.

```
New-AzSubscriptionDeployment -Location westus -TemplateFile deploy.json
```

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
The template creates a resource group named RG0 in the East US Azure region.	<input type="radio"/>	<input type="radio"/>
The template creates four new resource groups.	<input type="radio"/>	<input type="radio"/>
The template creates a resource group named RG3 in the West US Azure region.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
The template creates a resource group named RG0 in the East US Azure region.	<input checked="" type="checkbox"/>	<input type="radio"/>
The template creates four new resource groups.	<input type="radio"/>	<input checked="" type="checkbox"/>
The template creates a resource group named RG3 in the West US Azure region.	<input type="radio"/>	<input checked="" type="checkbox"/>

Explanation:

1. Yes. RG0 will be created with location from template file. For subscription level deployments, you must provide a location for the deployment. The location of the deployment is separate from the location of the resources you deploy. The deployment location specifies where to store deployment data.
2. No. Only RG0 and RG3 will be created, RG1 and RG2 already exist and can't be created.
3. No. RG3 will be created in east region.

<https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/deploy-to-subscription?tabs=azure-cli#deployment-location-and-name>

Question: 349

CertyIQ

You have an Azure App Service app named App1 that contains two running instances.

You have an autoscale rule configured as shown in the following exhibit.

Criteria

Metric namespace *

Standard metrics

Metric name

Memory Percentage

1 minute time grain

Dimension Name

Operator

Dimension Values

Add

Instance

=

All values



If you select multiple values for a dimension, autoscale will aggregate the metric across the selected values, not evaluate the metric for each value individually.



MemoryPercentage (Average)

39.28 %

Enable metric divide by instance count

Operator *

Metric threshold to trigger scale action *

Greater than

70

%

Duration (minutes) *

Time grain (minutes)

15

1

Time grain statistic *

Time aggregation *

Average

Average

Action

Operation *

Cool down (minutes) *

Increase count by

5

instance count *

1

For the Instance limits scale condition setting, you set Maximum to 5.

During a 30-minute period, App1 uses 80 percent of the available memory.

What is the maximum number of instances for App1 during the 30-minute period?

- A.2
- B.3
- C.4
- D.5

Answer: D

Explanation:

Start at 2 instances, after 15 min, > 70%, then +1 instance

Cooling 5 mins, still >70%, then +1 instance

Cooling 5 mins, still > 70%, then +1 instance

Cooling 5 mins, still >70%, since max 5 instances, keep 5 instances only.

Question: 350**CertyIQ**

HOTSPOT

You have an Azure subscription that contains the container images shown in the following table.

Name	Operating system
Image1	Windows Server
Image2	Linux

You plan to use the following services:

- Azure Container Instances
- Azure Container Apps
- Azure App Service

In which services can you run the images? To answer, select the options in the answer area.

NOTE: Each correct answer is worth one point.

Answer Area

Image1:

- Azure Container Instances only
- Azure Container Apps only
- Azure Container Instances and App Services only
- Azure Container Apps and App Services only
- Azure Container Instances, Azure Container Apps, and App Services

Image2:

- Azure Container Instances only
- Azure Container Apps only
- Azure Container Instances and App Services only
- Azure Container Apps and App Services only
- Azure Container Instances, Azure Container Apps, and App Services

Answer:

Answer Area

Image1:

- Azure Container Instances only
- Azure Container Apps only
- Azure Container Instances and App Services only
- Azure Container Apps and App Services only
- Azure Container Instances, Azure Container Apps, and App Services

Image2:

- Azure Container Instances only
- Azure Container Apps only
- Azure Container Instances and App Services only
- Azure Container Apps and App Services only
- Azure Container Instances, Azure Container Apps, and App Services

Explanation:

Azure Container Instances only.

ACI is a serverless container service that allows you to run containers without managing the underlying infrastructure.

It is ideal for short-lived tasks or scenarios where you need to quickly deploy containers.

Azure Container Apps only.

ACA is a fully managed serverless platform for running containerized applications.

It is designed for microservices and modern applications, offering features like auto-scaling and integration with Dapr (Distributed Application Runtime).

Question: 351

CertyIQ

You have an Azure AD tenant named contoso.com.

You have an Azure subscription that contains an Azure App Service web app named App1 and an Azure key vault named KV1. KV1 contains a wildcard certificate for contoso.com.

You have a user named use[(#)] that is assigned the Owner role for App1 and KV1.

You need to configure App1 to use the wildcard certificate of KV1.

What should you do first?

- A.Create an access policy for KV1 and assign the Microsoft Azure App Service principal to the policy.
- B.Assign a managed user identity to App1.
- C.Configure KV1 to use the role-based access control (RBAC) authorization system.
- D.Create an access policy for KV1 and assign the policy to User1.

Answer: A

Explanation:

 = user1@contoso.com

In order to read secrets from a key vault, you need to have a vault created and give your app permission to access it. Create a key vault by following the Key Vault quick start. Create a managed identity for your application. Key vault references use the app's system-assigned identity by default, but you can specify a user-assigned identity. Authorize read access to secrets your key vault for the managed identity you created earlier. How you do it depends on the permissions model of your key vault: Azure role-based access control: Assign the Key Vault Secrets User role to the managed identity. For instructions, see Provide access to Key Vault keys, certificates, and secrets with an Azure role-based access control. Vault access policy: Assign the Get secrets permission to the managed identity. For instructions, see Assign a Key Vault access policy.

<https://learn.microsoft.com/en-us/azure/app-service/app-service-key-vault-references?tabs=azure-cli>

CertyIQ**Question: 352**

You have an Azure subscription.

You plan to deploy the resources shown in the following table.

Name	Type
IP1	Microsoft.Network/publicIPAddresses
NSG1	Microsoft.Network/networkSecurityGroups
VNET1	Microsoft.Network/virtualNetworks
NIC1	Microsoft.Network/networkInterfaces
VM1	Microsoft.Compute/virtualMachines

You need to create a single Azure Resource Manager (ARM) template that will be used to deploy the resources.

Which resource should be added to the dependsOn section for VM1?

- A.VNET1
- B.NIC1
- C.IP1
- D.NSG1

Answer: B**Explanation:**

B. The NIC acts as the bridge between the VM and the other network resources like the virtual network, public IP, and network security group. Hence, it's essential to ensure that NIC1 is deployed before VM1.

<https://learn.microsoft.com/en-us/azure/templates/microsoft.compute/virtualmachines?pivots=deployment-language-arm-template>

<https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/resource-dependency>

<https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/template-tutorial-create-templates-with-dependent-resources?tabs=CLI>

You have an Azure subscription.

You create the following Azure Resource Manager (ARM) template named Template.json.

```
{  
  "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",  
  "contentVersion": "1.0.0.0",  
  "parameters": {},  
  "variables": {},  
  "resources": [  
    {  
      "type": "Microsoft.Resources/resourceGroups",  
      "apiVersion": "2022-12-01",  
      "location": "eastus",  
      "name": "Marketing"  
    }  
  ],  
  "outputs": {}  
}
```

You need to deploy Template.json.

Which PowerShell cmdlet should you run from Azure Cloud Shell?

- A.New-AzSubscriptionDeployment
- B.New-AzManagementGroupDeployment
- C.New-AzResourceGroupDeployment
- D.New-AzTenantDeployment

Answer: A**Explanation:**

New-Az Subscription Deployment is the correct answer, as the New-Az Resource Deployment is used to deploy in an existing resource group. You can use New-Az Subscription Deployment(which is an alias for New-Az Deployment) to deploy resources at subscription level. "The New-Az Resource Group Deployment cmdlet adds a deployment to an existing resource group

<https://learn.microsoft.com/en-us/powershell/module/az.resources/new-azresourcegroupdeployment?view=azps-10.4.1>

<https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/deploy-to-subscription?tabs=azure-powershell>

You have an Azure subscription that contains a resource group named RG1.

You plan to create a storage account named storage1.

You have a Bicep file named File1.

You need to modify File1 so that it can be used to automate the deployment of storage1 to RG1.

Which property should you modify?

- A.kind
- B.scope
- C.sku
- D.location

Answer: D

Explanation:

D (location) is the only logical answer. Here's the rationale. Kind, sku and location are three required properties. Scope (function) is not. Since we already 'have a Bicep file named File1' and need 'to automate the deployment of storage1 to RG1' the only variable required updating is the location, as we can leave other two (kind & sku) as-is. Location is required property which must be modified.

Question: 355

CertyIQ

HOTSPOT

Your company purchases a new Azure subscription.

You create a file named Deploy.json as shown in the following exhibit.

```
1  {
2      "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
3      "contentVersion": "1.0.0.0",
4      "parameters": {},
5      "variables": {},
6      "resources": [
7          {
8              "type": "Microsoft.Resources/resourceGroups",
9              "apiVersion": "2018-05-01",
10             "location": "eastus",
11             "name": "[concat('RG', copyIndex())]",
12             "copy": {
13                 "name": "copy",
14                 "count": 3
15             }
16         },
17         {
18             "type": "Microsoft.Resources/deployments",
19             "apiVersion": "2021-04-01",
20             "name": "lockDeployment",
21             "resourceGroup": "RG1",
22             "dependsOn": "[[resourceId('Microsoft.Resources/resourceGroups/', 'RG1')]]",
23             "properties": {
24                 "mode": "Incremental",
25                 "template": {
26                     "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
27                     "contentVersion": "1.0.0.0",
28                     "parameters": {},
29                     "variables": {},
30                     "resources": [
31                         {
32                             "type": "Microsoft.Authorization/locks",
33                             "apiVersion": "2016-09-01",
34                             "name": "rgLock",
35                             "properties": {
36                                 "level": "CanNotDelete"
37                             }
38                         }
39                     ]
40                 }
41             }
42         }
43     ]
44 }
```

```

37     }
38   ]
39 }
40 }
41 },
42 },
43 {
44   "type": "Microsoft.Resources/deployments",
45   "apiVersion": "2021-04-01",
46   "name": "lockDeployment",
47   "resourceGroup": "RG2",
48   "dependsOn": "[[resourceId('Microsoft.Resources/resourceGroups/', 'RG2')]]",
49   "properties": {
50     "mode": "Incremental",
51     "template": {
52       "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
53       "contentVersion": "1.0.0.0",
54       "parameters": {},
55       "variables": {},
56       "resources": [
57         {
58           "type": "Microsoft.Authorization/locks",
59           "apiVersion": "2016-09-01",
60           "name": "rgLock",
61           "properties": {
62             "level": "ReadOnly"
63           }
64         }
65       ]
66     }
67   }
68 },
69 ],
70   "outputs": {}
71 }

```

You connect to the subscription and run the following cmdlet.

New-AzDeployment -Location westus -TemplateFile "deploy.json"

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
You can deploy a virtual machine to RG1.	<input type="radio"/>	<input type="radio"/>
You can deploy a virtual machine to RG2.	<input type="radio"/>	<input type="radio"/>
You can manually create a resource group named RG3.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
You can deploy a virtual machine to RG1.	<input checked="" type="radio"/>	<input type="radio"/>
You can deploy a virtual machine to RG2.	<input type="radio"/>	<input checked="" type="radio"/>
You can manually create a resource group named RG3.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Yes

No

Yes

The deployment creates 3 RGs called RG0, RG1, RG2 as the index is 0-based.

You can deploy to RG1 as the lock is delete.

You can't deploy to RG2 as the lock is read-only, hence it can't be modified.

CertyIQ

Question: 356

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

Name	Type	Resource group	Location
RG1	Resource group	<i>Not applicable</i>	Central US
RG2	Resource group	<i>Not applicable</i>	West US
VMSS1	Virtual machine scale set	RG2	West US
Proximity1	Proximity placement group	RG1	West US
Proximity2	Proximity placement group	RG2	Central US
Proximity3	Proximity placement group	RG1	Central US

You need to configure a proximity placement group for VMSS1.

Which proximity placement groups should you use?

- A.Proximity2 only
- B.Proximity1, Proximity2, and Proximity3
- C.Proximity1 only
- D.Proximity1 and Proximity3 only

Answer: C

Explanation:

C. Proximity1 only.

Proximity1 is chosen because it ensures that the VMs in VMSS1 are co-located physically, maximizing performance and minimizing latency. Using multiple PPGs (options B and D) would spread the VMs across different physical locations, increasing latency and reducing the benefits of proximity placement.

Question: 357

CertyIQ

HOTSPOT

You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Subnet	Subnet-associated network security group (NSG)	Peered with
VNet1	Subnet1	NSG1	VNet2
VNet2	Subnet2	NSG2	VNet1

The subscription contains the virtual machines shown in the following table.

Name	Connected to
VM1	Subnet1
VM2	Subnet2

The subscription contains the Azure App Service web apps shown in the following table.

Name	Description
WebApp1	Uses the Premium pricing tier and has virtual network integration with VNet1
WebApp2	Uses the Isolated pricing tier and is deployed to Subnet2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
WebApp1 can communicate with VM2.	<input type="radio"/>	<input type="radio"/>
NSG1 controls inbound traffic to WebApp1.	<input type="radio"/>	<input type="radio"/>
WebApp2 can communicate with VM1.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
WebApp1 can communicate with VM2.	<input checked="" type="radio"/>	<input type="radio"/>
NSG1 controls inbound traffic to WebApp1.	<input type="radio"/>	<input checked="" type="radio"/>
WebApp2 can communicate with VM1.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

webapp1 can communicate with vm2: Yes

webapp1 is integrated with vnet1 and vnet1 is peered with vnet2, which vm2 is connected to. So, webapp1 can communicate with vm2.

nsg1 controls inbound traffic to webapp1: No

nsg1 is associated with subnet1, not directly with webapp1. It controls the inbound traffic to the subnet1, not to the webapp1.

webapp2 can communicate with vm1: Yes

webapp2 is deployed to subnet2 and subnet2 is in vnet2. vnet2 is peered with vnet1, which vm1 is connected to. So, webapp2 can communicate with vm1.

Question: 358

CertyIQ

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

Name	Type	Region	Resource group
RG1	Resource group	West Europe	<i>Not applicable</i>
RG2	Resource group	North Europe	<i>Not applicable</i>
Vault1	Recovery Services vault	West Europe	RG1

You create virtual machines in Subscription1 as shown in the following table.

Name	Resource group	Region	Operating system
VM1	RG1	West Europe	Windows Server 2022
VM2	RG1	North Europe	Windows Server 2022
VM3	RG2	West Europe	Windows Server 2022
VMA	RG1	West Europe	Ubuntu Server 20.04
VMB	RG1	North Europe	Ubuntu Server 20.04
VMC	RG2	West Europe	Ubuntu Server 20.04

You plan to use Vault1 for the backup of as many virtual machines as possible.

Which virtual machines can be backed up to Vault1?

- A.VM1 only
- B.VM3 and VMC only
- C.VM1, VM2, VM3, VMA, VMB, and VMC
- D.VM1, VM3, VMA, and VMC only
- E.VM1 and VM3 only

Answer: D

Explanation:

D: VM1, VM3, VMA, and VMC only the West Europe VMs: You need a vault in every Azure region that contains VMs you want to back up. You can't back up to a different region. Azure Backup supports application-consistent backups for both Windows and Linux VMs. There is no restriction that prevents backups from being performed on a Recovery Services Vault located in another resource Group

Reference:

<https://learn.microsoft.com/en-us/azure/virtual-machines/backup-recovery>

Question: 359

CertyIQ

You have an Azure subscription that contains an Azure container registry named ContReg1.

You enable the Admin user for ContReg1.

Which username can you use to sign in to ContReg1?

- A.root
- B.admin
- C.administrator
- D.ContReg1

Answer: D

Explanation:

D. ContReg1.

For Azure Container Registry, when the Admin user is enabled, the username is the name of the registry itself.

In this case, the username would be "ContReg1." This allows you to sign in using "ContReg1" as the username, along with the corresponding password generated or set for the Admin user.

Question: 360

CertyIQ

You have an Azure subscription.

You plan to create an Azure container registry named ContReg1.

You need to ensure that you can push and pull signed images for ContReg1.

What should you do for ContReg1?

- A. Enable encryption by using a customer-managed key.
- B. Create a connected registry.
- C. Add a token.
- D. Enable content trust.

Answer: D

Explanation:

D. Enable content trust.

Enabling content trust in Azure Container Registry ensures that all images are signed before they are pushed to the registry and verifies the signatures when images are pulled. This helps maintain the integrity and authenticity of the container images, ensuring that only signed and trusted images are used.

Question: 361

CertyIQ

HOTSPOT

-

You have an Azure subscription that has the Azure container registries shown in the following table.

Name	Service tier
ContReg1	Premium
ContReg2	Standard
ContReg3	Basic

You plan to use ACR Tasks and configure private endpoint connections.

Which container registries support ACR Tasks and private endpoints? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

ACR Tasks:

- ContReg1 only
- ContReg1 and ContReg2 only
- ContReg1, ContReg2, and ContReg3

Private endpoints:

- ContReg1 only
- ContReg1 and ContReg2 only
- ContReg1, ContReg2, and ContReg3

Answer:

Answer Area

ACR Tasks:

- ContReg1 only
- ContReg1 and ContReg2 only
- ContReg1, ContReg2, and ContReg3

Private endpoints:

- ContReg1 only
- ContReg1 and ContReg2 only
- ContReg1, ContReg2, and ContReg3

Explanation:

ContReg1, ContReg2, and ContReg3.

This option indicates that ACR Tasks are applicable to all three container registries.

ContReg1 only.

This option suggests that private endpoints are configured only for ContReg1.

Question: 362

CertyIQ

You plan to deploy several Azure virtual machines that will run Windows Server 2022 in a virtual machine scale set by using an Azure Resource Manager template.

You need to ensure that NGINX is available on all the virtual machines after they are deployed.

What should you use?

A.Azure Custom Script Extension

- B.Deployment Center in Azure App Service
- C.Microsoft Entra Application Proxy
- D.the Publish-AzVMDscConfiguration cmdlet

Answer: A

Explanation:

- A. Azure Custom Script Extension.

The Azure Custom Script Extension allows you to run scripts (PowerShell, Bash, etc.) on Azure VMs after deployment.

CertyIQ

Question: 363

You have an Azure subscription that contains a container group named Group1. Group1 contains two Azure container instances as shown in the following table.

Name	Resource request	Resource limit
container1	2 CPUs	2 CPUs
container2	3 CPUs	4 CPUs

You need to ensure that container2 can use CPU resources without negatively affecting container1.

What should you do?

- A.Increase the resource limit of container1 to three CPUs.
- B.Increase the resource limit of container2 to six CPUs.
- C.Remove the resource limit for both containers.
- D.Decrease the resource limit of container2 to two CPUs.

Answer: C

Explanation:

Answer is C.

The resources allocated to Group1 is 5 CPUs

Option D must be wrong. It is because the resource limit of a container instance must be greater than or equal to the mandatory resource request property. The resource limit of container 2 must be 3 or greater.

Option B is wrong as well. The maximum resource limit you can set for a container instance is the total resources allocated to the group. Thus, maximum request limit of container2 is 5. Also, Resource limit of container2 is 4. Container2 could use up to 4 CPUs that will negatively impact container1. Increase it 6 CPUs will make the situation even worse.

Option A can not stop container2 use up to 4 CPUs.

CertyIQ

Question: 364

You have an Azure subscription.

You plan to deploy a container.

You need to recommend which Azure services can scale the container automatically.

What should you recommend?

- A.Azure Container Apps only
- B.Azure Container Instances only
- C.Azure Container Apps or Azure App Service only
- D.Azure Container Instances or Azure App Service only
- E.Azure Container Apps, Azure Container Instances, or Azure App Service

Answer: C

Explanation:

To scale containers automatically, the following Azure services support this feature:

Azure Container Apps: Supports automatic horizontal scaling through declarative scaling rules1.

Azure App Service: Supports automatic scaling for web apps, including those deployed as containers

Question: 365

CertyIQ

HOTSPOT

-

You have an Azure subscription that uses Azure Container Instances.

You have a computer that has Azure Command-Line Interface (CLI) and Docker installed.

You create a container image named image1.

You need to provision a new Azure container registry and add image1 to the registry.

Which command should you run for each requirement? To answer, select the options in the answer area.

NOTE: Each correct answer is worth one point.

Answer Area

Provision a new container registry:

- az acr build
- az acr create
- az container create
- docker create

Add image1 to the registry:

- az acr create
- az container create
- docker pull
- docker push

Answer:

Answer Area

Provision a new container registry:

- az acr build
- az acr create**
- az container create
- docker create

Add image1 to the registry:

- az acr create
- az container create
- docker pull
- docker push**

Explanation:

Provision a new container registry: **az.acr create**.

This is the correct command to create a new Azure Container Registry.

Add image1 to the registry: **docker push**.

This is the correct command to push a Docker image to a registry.

Question: 366

CertyIQ

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 container registry named Registry1 that contains an image named image1.

You receive an error message when you attempt to deploy a container instance by using image1.

You need to be able to deploy a container instance by using image1.

Solution: You assign the AcrPull role to ACR-Tasks-Network for Registry1.

Does this meet the goal?

- A.Yes
- B.No

Answer: B

Explanation:

No Acr Pull role assigned to ACR-Tasks-Network does not meet the goal. This role should be assigned to the identity that is performing the container deployment.

Question: 367

CertyIQ

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 container registry named Registry1 that contains an image named image1.

You receive an error message when you attempt to deploy a container instance by using image1.

You need to be able to deploy a container instance by using image1.

Solution: You select Use dedicated data endpoint for Registry1.

Does this meet the goal?

- A.Yes
- B.No

Answer: B

Explanation:

No, selecting “Use dedicated data endpoint” for Registry1 does not directly address the issue of deploying a container instance using image1. The error message you received likely indicates that the image is inaccessible. This can happen due to several reasons, such as incorrect credentials or firewall rules blocking

access12. To resolve this issue, you should ensure that: The credentials used to access the Azure Container Registry are correct. The Azure Container Registry allows access from the Azure Container Instances service. You can achieve this by enabling the “Allow trusted services” option or using a managed identity12.

CertyIQ

Question: 368

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 container registry named Registry1 that contains an image named image1.

You receive an error message when you attempt to deploy a container instance by using image1.

You need to be able to deploy a container instance by using image1.

Solution: You create a private endpoint connection for Registry1.

Does this meet the goal?

- A.Yes
- B.No

Answer: B

Explanation:

B. No Creating a private endpoint connection for Registry1 alone will not resolve the issue of deploying a container instance using image1. The error could be due to various reasons such as authentication issues, image not being found, or network restrictions. To troubleshoot, you might need to:- Ensure the container instance has the necessary permissions to access the registry.- Verify the image name and tag are correct.- Check network settings and firewall rules.- Confirm that the container instance can resolve the registry's DNS name.

Question: 369

CertyIQ

You have a Standard Azure App Service plan named Plan1.

You need to ensure that Plan1 will scale automatically when the CPU usage of the web app exceeds 80 percent.

What should you select for Plan1?

- A.Automatic in the Scale out method settings
- B.Rules Based in the Scale out method settings
- C.Premium P1 in the Scale up (App Service plan) settings
- D.Standard S1 in the Scale up (App Service plan) settings
- E.Manual in the Scale out method settings

Answer: B

Explanation:

In Azure Monitor, rules-based scaling in the scale-out method settings use metrics and schedules to determine when to add or remove resources to run an application. These rules include minimum and maximum resource levels, and when the conditions are met, one or more autoscale actions are triggered. For example, you can scale out an application by adding VMs when the average CPU usage per VM is above a certain percentage, or scale it back by removing VMs when CPU usage drops below a certain percentage.

Question: 370

CertyIQ

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

ADatum Corporation is consulting firm that has a main office in Montreal and branch offices in Seattle and New York.

Existing Environment -

Azure Environment -

ADatum has an Azure subscription that contains three resource groups named RG1, RG2, and RG3.

The subscription contains the storage accounts shown in the following table.

Name	Kind	Location	Hierarchical namespace	Container	File share
storage1	StorageV2	West US	Yes	cont1	share1
storage2	StorageV2	West US	No	cont2	share2

The subscription contains the virtual machines shown in the following table.

Name	Size	Operating system	Description
VM1	A	Red Hat Enterprise Linux (RHEL)	Uses ephemeral OS disks
VM2	D	Windows Server 2022	Has a basic volume
VM3	B	Red Hat Enterprise Linux (RHEL)	Uses a standard SSDs
VM4	M	Windows Server 2022	Uses Write Accelerator disks
VM5	E	Windows Server 2022	Has a dynamic volume

The subscription has an Azure container registry that contains the images shown in the following table.

Name	Operating system
Image1	Windows Server
Image2	Linux

The subscription contains the resources shown in the following table.

Name	Description	In resource group
Workspace1	Log Analytics workspace	RG1
WebApp1	Azure App Service web app	RG1
VNet1	Virtual network	RG2
zone1.com	Azure Private DNS zone	RG3

Azure Key Vault -

The subscription contains an Azure key vault named Vault1.

Vault1 contains the certificates shown in the following table.

Name	Content type	Key type	Key size
Cert1	PKCS#12	RSA	2048
Cert2	PKCS#12	RSA	4096
Cert3	PEM	RSA	2048
Cert4	PEM	RSA	4096

Vault1 contains the keys shown in the following table.

Name	Type	Description
Key1	RSA	Has a key size of 4096
Key2	EC	Has Elliptic curve name set to P-256

Microsoft Entra Environment -

ADatum has a Microsoft Entra tenant named adatum.com that is linked to the Azure subscription and contains the users shown in the following table.

Name	Microsoft Entra role	Azure role
Admin1	Global Administrator	None
Admin2	Attribute Definition Administrator	None
Admin3	Attribute Assignment Administrator	None
User1	None	Reader for RG2 and RG3

The tenant contains the groups shown in the following table.

Name	Type
Group1	Security group
Group2	Microsoft 365 group

The adatum.com tenant has a custom security attribute named Attribute1.

Planned Changes -

ADatum plans to implement the following changes:

- Configure a data collection rule (DCR) named DCR1 to collect only system events that have an event ID of 4648 from VM2 and VM4.
- In storage1, create a new container named cont2 that has the following access policies: oThree stored access policies named Stored1, Stored2, and Stored3 oA legal hold for immutable blob storage
- Whenever possible, use directories to organize storage account content.
- Grant User1 the permissions required to link Zone1 to VNet1.
- Assign Attribute1 to supported adatum.com resources.
- In storage2, create an encryption scope named Scope1.
- Deploy new containers by using Image1 or Image2.

Technical Requirements -

ADatum must meet the following technical requirements:

- Use TLS for WebApp1.
- Follow the principle of least privilege.
- Grant permissions at the required scope only.
- Ensure that Scope1 is used to encrypt storage services.
- Use Azure Backup to back up cont1 and share1 as frequently as possible.
- Whenever possible, use Azure Disk Encryption and a key encryption key (KEK) to encrypt the virtual machines.

You need to configure WebApp1 to meet the technical requirements.

Which certificate can you use from Vault1?

- A.Cert1 only
- B.Cert1 or Cert2 only
- C.Cert1 or Cert3 only
- D.Cert3 or Cert4 only
- E.Cert1, Cert2 Cert3, or Cert4

Answer: D

Explanation:

D.Cert3 or Cert4 only.

Cert3 and Cert4 likely meet the specific technical requirements for WebApp1, such as being issued by a trusted CA, having valid expiration dates, and being configured for the appropriate domain.

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 machine named VM1. VM1 was deployed by using a custom Azure Resource Manager template named ARM1.json.

You receive a notification that VM1 will be affected by maintenance.

You need to move VM1 to a different host immediately.

Solution: From the resource group blade, move VM1 to another subscription.

Does this meet the goal?

A.Yes

B.No

Answer: B

Explanation:

B. No

Moving a VM to another subscription does not immediately move it to a different host. Instead, it involves a complex process that may require recreating the VM in the target subscription.

Question: 372

CertyIQ

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 machine named VM1. VM1 was deployed by using a custom Azure Resource Manager template named ARM1.json.

You receive a notification that VM1 will be affected by maintenance.

You need to move VM1 to a different host immediately.

Solution: From the VM1 Redeploy + reapply blade, you select Redeploy.

Does this meet the goal?

A.Yes

B.No

Answer: A

Explanation:

A. Yes

Selecting Redeploy from the Redeploy + reapply blade will move VM1 to a new Azure host immediately. This action shuts down the VM, moves it to a different physical server, and then powers it back on, which meets the

goal of moving the VM to a different host.

Redeploy forces the VM to be placed on a new host in Azure while retaining all configurations.

This is useful for resolving host-related issues or maintenance scenarios.

Question: 373

CertyIQ

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 machine named VM1. VM1 was deployed by using a custom Azure Resource Manager template named ARM1.json.

You receive a notification that VM1 will be affected by maintenance.

You need to move VM1 to a different host immediately.

Solution: From the VM1 Updates blade, select One-time update.

Does this meet the goal?

A.Yes

B.No

Answer: B

Explanation:

B. No

Selecting One-time update from the Updates blade is related to applying updates to the VM (such as Windows or Linux updates) but does not move the VM to a different host.

To move VM1 to a different host immediately, you should use the Redeploy option under Redeploy + reapply, which forces the VM to migrate to a new Azure host.

Question: 374

CertyIQ

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

ADatum Corporation is consulting firm that has a main office in Montreal and branch offices in Seattle and New York.

Existing Environment -

Azure Environment -

ADatum has an Azure subscription that contains three resource groups named RG1, RG2, and RG3.

The subscription contains the storage accounts shown in the following table.

Name	Kind	Location	Hierarchical namespace	Container	File share
storage1	StorageV2	West US	Yes	cont1	share1
storage2	StorageV2	West US	No	cont2	share2

The subscription contains the virtual machines shown in the following table.

Name	Size	Operating system	Description
VM1	A	Red Hat Enterprise Linux (RHEL)	Uses ephemeral OS disks
VM2	D	Windows Server 2022	Has a basic volume
VM3	B	Red Hat Enterprise Linux (RHEL)	Uses a standard SSDs
VM4	M	Windows Server 2022	Uses Write Accelerator disks
VM5	E	Windows Server 2022	Has a dynamic volume

The subscription has an Azure container registry that contains the images shown in the following table.

Name	Operating system
Image1	Windows Server
Image2	Linux

The subscription contains the resources shown in the following table.

Name	Description	In resource group
Workspace1	Log Analytics workspace	RG1
WebApp1	Azure App Service web app	RG1
VNet1	Virtual network	RG2
zone1.com	Azure Private DNS zone	RG3

Azure Key Vault -

The subscription contains an Azure key vault named Vault1.

Vault1 contains the certificates shown in the following table.

Name	Content type	Key type	Key size
Cert1	PKCS#12	RSA	2048
Cert2	PKCS#12	RSA	4096
Cert3	PEM	RSA	2048
Cert4	PEM	RSA	4096

Vault1 contains the keys shown in the following table.

Name	Type	Description
Key1	RSA	Has a key size of 4096
Key2	EC	Has Elliptic curve name set to P-256

Microsoft Entra Environment -

ADatum has a Microsoft Entra tenant named adatum.com that is linked to the Azure subscription and contains the users shown in the following table.

Name	Microsoft Entra role	Azure role
Admin1	Global Administrator	<i>None</i>
Admin2	Attribute Definition Administrator	<i>None</i>
Admin3	Attribute Assignment Administrator	<i>None</i>
User1	<i>None</i>	Reader for RG2 and RG3

The tenant contains the groups shown in the following table.

Name	Type
Group1	Security group
Group2	Microsoft 365 group

The adatum.com tenant has a custom security attribute named Attribute1.

Planned Changes -

ADatum plans to implement the following changes:

- Configure a data collection rule (DCR) named DCR1 to collect only system events that have an event ID of 4648 from VM2 and VM4.
- In storage1, create a new container named cont2 that has the following access policies: oThree stored access policies named Stored1, Stored2, and Stored3 oA legal hold for immutable blob storage
- Whenever possible, use directories to organize storage account content.
- Grant User1 the permissions required to link Zone1 to VNet1.
- Assign Attribute1 to supported adatum.com resources.
- In storage2, create an encryption scope named Scope1.
- Deploy new containers by using Image1 or Image2.

Technical Requirements -

ADatum must meet the following technical requirements:

- Use TLS for WebApp1.
- Follow the principle of least privilege.
- Grant permissions at the required scope only.

- Ensure that Scope1 is used to encrypt storage services.
- Use Azure Backup to back up cont1 and share1 as frequently as possible.
- Whenever possible, use Azure Disk Encryption and a key encryption key (KEK) to encrypt the virtual machines.

You need to meet the technical requirements for the KEK.

Which PowerShell cmdlet and key should you use?

- A. Set-AzVMDiskEncryptionExtension and Key2.
- B. Set-AzDiskEncryptionKey and Key2.
- C. Set-AzDiskDiskEncryptionKey and Key1.
- D. Set-AzVMDiskEncryptionExtension and Key1.

Answer: D

Explanation:

D. Set-AzVMDiskEncryptionExtension and Key1.

To meet the technical requirements for the KEK (Key Encryption Key) in Azure VM Disk Encryption, you need to use the Set-AzVMDiskEncryptionExtension cmdlet. This cmdlet enables Azure Disk Encryption (ADE), which supports encrypting both OS and data disks using Azure Key Vault keys.

Set-AzVMDiskEncryptionExtension: This is the correct cmdlet for enabling encryption on a VM using Azure Disk Encryption.

Key1: This likely refers to the Key Encryption Key (KEK), which is used to further protect the encryption keys stored in Azure Key Vault.

Question: 375

CertyIQ

HOTSPOT -

You have an Azure subscription named Sub1.

You plan to deploy a multi-tiered application that will contain the tiers shown in the following table.

Tier	Accessible from the Internet	Number of virtual machines
Front-end web server	Yes	10
Business logic	No	100
Microsoft SQL Server database	No	5

You need to recommend a networking solution to meet the following requirements:

⇒ Ensure that communication between the web servers and the business logic tier spreads equally across the virtual machines.

⇒ Protect the web servers from SQL injection attacks.

Which Azure resource should you recommend for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Ensure that communication between the web servers and the business logic tier spreads equally across the virtual machines:

- an application gateway that uses the Standard tier
- an application gateway that uses the WAF tier
- an internal load balancer
- a network security group (NSG)
- a public load balancer

Protect the web servers from SQL injection attacks:

- an application gateway that uses the Standard tier
- an application gateway that uses the WAF tier
- an internal load balancer
- a network security group (NSG)
- a public load balancer

Answer:

Answer Area

Ensure that communication between the web servers and the business logic tier spreads equally across the virtual machines:

- an application gateway that uses the Standard tier
- an application gateway that uses the WAF tier
- an internal load balancer
- a network security group (NSG)
- a public load balancer

Protect the web servers from SQL injection attacks:

- an application gateway that uses the Standard tier
- an application gateway that uses the WAF tier
- an internal load balancer
- a network security group (NSG)
- a public load balancer

Explanation:

Box 1: an internal load balancer

Azure Internal Load Balancer (ILB) provides network load balancing between virtual machines that reside inside a cloud service or a virtual network with a regional scope.

Box 2: an application gateway that uses the WAF tier

Azure Web Application Firewall (WAF) on Azure Application Gateway provides centralized protection of your web applications from common exploits and vulnerabilities. Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities.

Reference:

<https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/ag-overview>

Question: 376

CertyIQ

Your company has three offices. The offices are located in Miami, Los Angeles, and New York. Each office contains datacenter.

You have an Azure subscription that contains resources in the East US and West US Azure regions. Each region contains a virtual network. The virtual networks are peered.

You need to connect the datacenters to the subscription. The solution must minimize network latency between the

datacenters.

What should you create?

- A. three Azure Application Gateways and one On-premises data gateway
- B. three virtual hubs and one virtual WAN
- C. three virtual WANs and one virtual hub
- D. three On-premises data gateways and one Azure Application Gateway

Answer: C

Explanation:

There can only be one hub per Azure region.

It should be 2 Virtual Hubs and 1 WAN.

Since we have just two regions, it may be impossible to have 3 hubs.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about>

Question: 377

CertyIQ

HOTSPOT -

You plan to deploy five virtual machines to a virtual network subnet.

Each virtual machine will have a public IP address and a private IP address.

Each virtual machine requires the same inbound and outbound security rules.

What is the minimum number of network interfaces and network security groups that you require? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Minimum number of network interfaces:

5
10
15
20

Minimum number of network security groups:

1
2
5
10

Answer:

Answer Area

Minimum number of network interfaces:

5
10
15
20

Minimum number of network security groups:

1
2
5
10

Explanation:

Box 1: 5 -

A public and a private IP address can be assigned to a single network interface.

Box 2: 1 -

You can associate zero, or one, network security group to each virtual network subnet and network interface in a virtual machine. The same network security group can be associated to as many subnets and network interfaces as you choose.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface-addresses>

Question: 378

CertyIQ

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

Name	Type
LB1	Load balancer
VM1	Virtual machine
VM2	Virtual machine

LB1 is configured as shown in the following table.

Name	Type	Value
bepool1	Backend pool	VM1, VM2
LoadBalancerFrontEnd	Frontend IP configuration	Public IP address
hprobe1	Health probe	Protocol: TCP Port: 80 Interval: 5 seconds Unhealthy threshold: 2
rule1	Load balancing rule	IP version: IPv4 Frontend IP address: LoadBalancerFrontEnd Port: 80 Backend Port: 80 Backend pool: bepool1 Health probe: hprobe1

You plan to create new inbound NAT rules that meet the following requirements:

- ⇒ Provide Remote Desktop access to VM1 from the internet by using port 3389.
- ⇒ Provide Remote Desktop access to VM2 from the internet by using port 3389.

What should you create on LB1 before you can create the new inbound NAT rules?

- A. a frontend IP address
- B. a load balancing rule
- C. a health probe
- D. a backend pool

Answer: A

Explanation:

A. a frontend IP address.

Before you can create inbound NAT rules on Azure Load Balancer (LB1), you need to have a frontend IP address. The frontend IP is the public or private IP address that receives incoming traffic before forwarding it based on NAT rules.

Question: 379

CertyIQ

HOTSPOT -

You have Azure virtual machines that run Windows Server 2019 and are configured as shown in the following table.

Name	Private IP address	Public IP address	Virtual network name	DNS suffix configured in Windows Server
VM1	10.1.0.4	52.186.85.63	VNET1	Adatum.com
VM2	10.1.0.5	13.92.168.13	VNET1	Contoso.com

You create a private Azure DNS zone named adatum.com. You configure the adatum.com zone to allow auto registration from VNET1.

Which A records will be added to the adatum.com zone for each virtual machine? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

A records for VM1:

None
Private IP address only
Public IP address only
Private IP address and public IP address

A records for VM2:

None
Private IP address only
Public IP address only
Private IP address and public IP address

Answer:

Answer Area

A records for VM1:

None
Private IP address only
Public IP address only
Private IP address and public IP address

A records for VM2:

None
Private IP address only
Public IP address only
Private IP address and public IP address

Explanation:

The virtual machines are registered (added) to the private zone as A records pointing to their private IP addresses.

Reference:

<https://docs.microsoft.com/en-us/azure/dns/private-dns-overview> <https://docs.microsoft.com/en-us/azure/dns/private-dns-scenarios>

Question: 380

CertyIQ

HOTSPOT -

You have an Azure virtual network named VNet1 that connects to your on-premises network by using a site-to-site VPN. VNet1 contains one subnet named

Sunet1.

Subnet1 is associated to a network security group (NSG) named NSG1. Subnet1 contains a basic internal load balancer named ILB1. ILB1 has three Azure virtual machines in the backend pool.

You need to collect data about the IP addresses that connects to ILB1. You must be able to run interactive queries from the Azure portal against the collected data.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Resource to create:

- An Azure Event Grid
- An Azure Log Analytics workspace
- An Azure Storage account

Resource on which to enable diagnostics:

- ILB1
- NSG1
- The Azure virtual machines

Answer:

Answer Area

Resource to create:

- An Azure Event Grid
- An Azure Log Analytics workspace
- An Azure Storage account

Resource on which to enable diagnostics:

- ILB1
- NSG1
- The Azure virtual machines

Explanation:

Box 1: An Azure Log Analytics workspace

In the Azure portal you can set up a Log Analytics workspace, which is a unique Log Analytics environment with its own data repository, data sources, and solutions.

Box 2: NSG1

NSG flow logs allow viewing information about ingress and egress IP traffic through a Network security group. Through this, the IP addresses that connect to the ILB can be monitored when the diagnostics are enabled on a Network Security Group.

We cannot enable diagnostics on an internal load balancer to check for the IP addresses.

As for Internal LB, it is basic one. Basic can only connect to storage account. Also, Basic LB has only activity logs, which doesn't include the connectivity workflow. So, we need to use NSG to meet the mentioned requirements.

Reference:

<https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-quick-create-workspace>

<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-standard-diagnostics>

Question: 381

CertyIQ

You have the Azure virtual networks shown in the following table.

Name	Address space	Subnet	Resource group Azure region
VNet1	10.11.0.0/16	10.11.0.0/17	West US
VNet2	10.11.0.0/17	10.11.0.0/25	West US
VNet3	10.10.0.0/22	10.10.1.0/24	East US
VNet4	192.168.16.0/22	192.168.16.0/24	North Europe

To which virtual networks can you establish a peering connection from VNet1?

- A. VNet2 and VNet3 only
- B. VNet2 only
- C. VNet3 and VNet4 only
- D. VNet2, VNet3, and VNet4

Answer: C

Explanation:

Address spaces must not overlap to enable VNet Peering.

Incorrect Answers:

A, B, D: The address space for VNet2 overlaps with VNet1. We therefore cannot establish a peering between VNet2 and VNet1.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-connect-virtual-networks-portal> <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-faq#vnet-peering>

Question: 382

CertyIQ

You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains four subnets named Gateway, Perimeter, NVA, and Production.

The NVA subnet contains two network virtual appliances (NVAs) that will perform network traffic inspection between the Perimeter subnet and the Production subnet.

You need to implement an Azure load balancer for the NVAs. The solution must meet the following requirements:

- ⇒ The NVAs must run in an active-active configuration that uses automatic failover.
- ⇒ The load balancer must load balance traffic to two services on the Production subnet. The services have different IP addresses.

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

NOTE: Each correct selection is worth one point.

- A. Deploy a basic load balancer
- B. Deploy a standard load balancer
- C. Add two load balancing rules that have HA Ports and Floating IP enabled
- D. Add two load balancing rules that have HA Ports enabled and Floating IP disabled
- E. Add a frontend IP configuration, a backend pool, and a health probe
- F. Add a frontend IP configuration, two backend pools, and a health probe

Answer: BCF

Explanation:

A standard load balancer is required for the HA ports.

Two backend pools are needed as there are two services with different IP addresses.

Floating IP rule is used where backend ports are reused.

Incorrect Answers:

E: HA Ports are not available for the basic load balancer.

Reference:

<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-standard-overview>

<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-multivip-overview>

CertyIQ

You have an Azure subscription named Subscription1 that contains two Azure virtual networks named VNet1 and VNet2. VNet1 contains a VPN gateway named VPNGW1 that uses static routing. There is a site-to-site VPN connection between your on-premises network and VNet1.

On a computer named Client1 that runs Windows 10, you configure a point-to-site VPN connection to VNet1. You configure virtual network peering between VNet1 and VNet2. You verify that you can connect to VNet2 from the on-premises network. Client1 is unable to connect to VNet2.

You need to ensure that you can connect Client1 to VNet2.

What should you do?

- A. Download and re-install the VPN client configuration package on Client1.
- B. Select Allow gateway transit on VNet1.
- C. Select Allow gateway transit on VNet2.
- D. Enable BGP on VPNGW1

Answer: A

Explanation:

A. Download and re-install the VPN client configuration package on Client1.

Client1 is using a Point-to-Site (P2S) VPN connection to connect to VNet1. However, by default, Point-to-Site VPN clients do not automatically inherit peered network routes (like VNet2).

To fix this issue, you need to download and re-install the VPN client configuration package on Client1 after configuring virtual network peering. This ensures that Client1 gets the updated route table, including routes to VNet2.

HOTSPOT -

You have an Azure subscription. The subscription contains virtual machines that run Windows Server 2016 and are configured as shown in the following table.

Name	Virtual network	DNS suffix configured in Windows Server
VM1	VNET2	Contoso.com
VM2	VNET2	None
VM3	VNET2	Adatum.com

You create a public Azure DNS zone named adatum.com and a private Azure DNS zone named contoso.com.

You create a virtual network link for contoso.com as shown in the following exhibit.

link1
contoso.com

A Save X Discard Delete Access Control (IAM) Tags

Link name
link1

Link state
Completed

Provisioning state
Succeeded

Virtual network details

Virtual network id
`/subscriptions/8372f433-2dcd-4361-b5ef-5b188fed87d0/resourceGroups/RG2/provi...`

Virtual network
VNET2

Configuration
 Enable auto registration (1)

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
When VM1 starts, a record for VM1 is added to the contoso.com DNS zone.	<input type="radio"/>	<input type="radio"/>
When VM2 starts, a record for VM2 is added to the contoso.com DNS zone.	<input type="radio"/>	<input type="radio"/>
When VM3 starts, a record for VM3 is added to the adatum.com DNS zone.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
When VM1 starts, a record for VM1 is added to the contoso.com DNS zone.	<input checked="" type="radio"/>	<input type="radio"/>
When VM2 starts, a record for VM2 is added to the contoso.com DNS zone.	<input checked="" type="radio"/>	<input type="radio"/>
When VM3 starts, a record for VM3 is added to the adatum.com DNS zone.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

All three VMs are in VNET2. Auto registration is enabled for private Azure DNS zone named contoso.com, which is linked to VNET2. So, VM1, VM2 and VM3 will auto-register their host records to contoso.com.

None of the VM will auto-register to the public Azure DNS zone named adatum.com. You cannot register private IPs on the internet (adatum.com)

Box 1: Yes

Auto registration is enabled for private Azure DNS zone named contoso.com.

Box 2: Yes

Auto registration is enabled for private Azure DNS zone named contoso.com.

Box 3: No

None of the VM will auto-register to the public Azure DNS zone named adatum.com

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-name-resolution-for-vms-and-role-instances>

<https://docs.microsoft.com/en-us/azure/dns/private-dns-autoregistration>

<https://docs.microsoft.com/en-us/azure/dns/private-dns-virtual-network-links>

Reference:

Question: 385

CertyIQ

You have an Azure subscription that contains the resources in the following table.

Name	Type	Azure region	Resource group
VNet1	Virtual network	West US	RG2
VNet2	Virtual network	West US	RG1
VNet3	Virtual network	East US	RG1
NSG1	Network security group (NSG)	East US	RG2

To which subnets can you apply NSG1?

- A. the subnets on VNet1 only
- B. the subnets on VNet2 and VNet3 only
- C. the subnets on VNet2 only
- D. the subnets on VNet3 only
- E. the subnets on VNet1, VNet2, and VNet3

Answer: D

Explanation:

All Azure resources are created in an Azure region and subscription. A resource can only be created in a virtual network that exists in the same region and subscription as the resource.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-vnet-plan-design-arm>

Question: 386

CertyIQ

DRAG DROP -

You have an Azure subscription that contains two virtual networks named VNet1 and VNet2. Virtual machines connect to the virtual networks.

The virtual networks have the address spaces and the subnets configured as shown in the following table.

Virtual network	Address space	Subnet	Peering
VNet1	10.1.0.0/16	10.1.0.0/24 10.1.1.0/26	VNet2
VNet2	10.2.0.0/16	10.2.0.0/24	VNet1

You need to add the address space of 10.33.0.0/16 to VNet1. The solution must ensure that the hosts on VNet1 and VNet2 can communicate.

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

Answer Area

Remove VNet1.

Add the 10.33.0.0/16 address space to VNet1.

Create a new virtual network named VNet1.

On the peering connection in VNet2, allow gateway transit.

Recreate peering between VNet1 and VNet2.

On the peering connection in VNet1, allow gateway transit.

Remove peering between VNet1 and VNet2.



Answer:

Actions

Answer Area

Remove VNet1.

Remove peering between VNet1 and VNet2.

Add the 10.33.0.0/16 address space to VNet1.

Add the 10.33.0.0/16 address space to VNet1.

Create a new virtual network named VNet1.

Recreate peering between VNet1 and VNet2.



On the peering connection in VNet2, allow gateway transit.

Recreate peering between VNet1 and VNet2.

On the peering connection in VNet1, allow gateway transit.

Remove peering between VNet1 and VNet2.

Explanation:

Step 1: Remove peering between VNet1 and VNet2.

You can't add address ranges to, or delete address ranges from a virtual network's address space once a virtual network is peered with another virtual network.

To add or remove address ranges, delete the peering, add or remove the address ranges, then re-create the peering.

Step 2: Add the 10.33.0.0/16 address space to VNet1.

Step 3: Recreate peering between VNet1 and VNet2

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering>

CertyIQ

Question: 387

HOTSPOT -

You have an Azure subscription that contains the resource groups shown in the following table.

Name	Location
RG1	West US
RG2	East US

RG1 contains the resources shown in the following table.

Name	Type	Location
storage1	Storage account	West US
VNet1	Virtual network	West US
NIC1	Network interface	West US
Disk1	Disk	West US
VM1	Virtual machine	West US

VM1 is running and connects to NIC1 and Disk1. NIC1 connects to VNET1.

RG2 contains a public IP address named IP2 that is in the East US location. IP2 is not assigned to a virtual machine.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
You can move storage1 to RG2.	<input type="radio"/>	<input type="radio"/>
You can move NIC1 to RG2.	<input type="radio"/>	<input type="radio"/>
If you move IP2 to RG1, the location of IP2 will change.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
You can move storage1 to RG2.	<input checked="" type="radio"/>	<input type="radio"/>
You can move NIC1 to RG2.	<input checked="" type="radio"/>	<input type="radio"/>
If you move IP2 to RG1, the location of IP2 will change.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Box 1: Yes

You can move the Storage Account to RG2, however it stayed in the West US region. You cannot change the Region, you need to recreate the Storage Account.

Box 2: Yes

You can move move NIC1 to RG2 which was associated with VM1 and VNET1 subnet1, however it stayed in the West US region. You can move a NIC to a different RG or Subscription by selecting (change) next to the RG or Subscription name. If you move the NIC to a new Subscription, you must move all resources related to the NIC with it. If the network interface is attached to a virtual machine, for example, you must also move the virtual machine, and other virtual machine-related resources.

Box 3: No

You can move IP2 to RG1, as it isn't associated with any other resource, however it stayed in the East US region. The location will not change.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/move-support-resources>
<https://docs.microsoft.com/en-us/azure/virtual-network/move-across-regions-publicip-powershell>

Question: 388

CertyIQ

You have an Azure web app named webapp1.
You have a virtual network named VNET1 and an Azure virtual machine named VM1 that hosts a MySQL database. VM1 connects to VNET1.
You need to ensure that webapp1 can access the data hosted on VM1.
What should you do?

- A. Deploy an internal load balancer
- B. Peer VNET1 to another virtual network
- C. Connect webapp1 to VNET1

D. Deploy an Azure Application Gateway

Answer: C

Explanation:

C. Connect webapp1 to VNET1.

By connecting the web app to the virtual network, you can enable access from the web app to resources on the virtual network, including the MySQL database hosted on VM1. This can be done by enabling VNet Integration for the web app and then selecting VNET1 as the virtual network to integrate with. Once the integration is set up, the web app will be able to communicate with VM1 on VNET1 as if it were on the same network.

Option A, deploying an internal load balancer, is not necessary in this scenario, as load balancing is not required.

Option B, peering VNET1 to another virtual network, is also not necessary for this scenario, as it does not address the requirement to enable communication between the web app and the MySQL database hosted on VM1.

Option D, deploying an Azure Application Gateway, is not necessary for this scenario, as it is primarily used for load balancing and routing of HTTP/HTTPS traffic. It does not address the requirement to enable communication between the web app and the MySQL database hosted on VM1.

Question: 389

CertyIQ

You create an Azure VM named VM1 that runs Windows Server 2019. VM1 is configured as shown in the exhibit. (Click the Exhibit tab.)

VM1

Virtual machine

Search (Ctrl+ /) <

Connect Start Restart Stop Capture Delete Refresh

Resource group (change): RG1
Status: Stopped (deallocated)
Location: West Europe
Subscription (change): Azure Pass – Sponsorship
Subscription ID: 80f9d59c-629e-4346-b577-8b7e1ef1316a

Computer name: (start VM to view)
Operating system: Windows
Size: Standard DS2 v2 (2 vcpus, 7 GiB memory)
Ephemeral OS disk: N/A
Public IP address: VM1-ip
Private IP address: 10.0.0.4
Virtual network/subnet: VNET1/default
DNS name: Configure

Tags (change): Click here to add tags

Show data for last: 1 hour 6 hours 12 hours 1 day 7 days 30 days

CPU (average)

Percentage-CPU (Avg)
vm1 --

Network (total)

608

You need to enable Desired State Configuration for VM1.

What should you do first?

- A. Connect to VM1.
- B. Start VM1.
- C. Capture a snapshot of VM1.
- D. Configure a DNS name for VM1.

Answer: B

Explanation:

Status is Stopped (Deallocated).

The DSC extension for Windows requires that the target virtual machine is able to communicate with Azure.

The VM needs to be started.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-windows>

Question: 390

CertyIQ

You have five Azure virtual machines that run Windows Server 2016. The virtual machines are configured as web servers.

You have an Azure load balancer named LB1 that provides load balancing services for the virtual machines.

You need to ensure that visitors are serviced by the same web server for each request.

What should you configure?

- A. Floating IP (direct server return) to Disabled
- B. Session persistence to None
- C. Floating IP (direct server return) to Enabled
- D. Session persistence to Client IP

Answer: D

Explanation:

With Sticky Sessions when a client starts a session on one of your web servers, session stays on that specific server. To configure An Azure Load-Balancer For

Sticky Sessions set Session persistence to Client IP or to Client IP and protocol.

On the following image you can see sticky session configuration:

Note:

- ⇒ Client IP and protocol specifies that successive requests from the same client IP address and protocol combination will be handled by the same virtual machine.
- ⇒ Client IP specifies that successive requests from the same client IP address will be handled by the same virtual machine.

Reference:

<https://cloudopszone.com/configure-azure-load-balancer-for-sticky-sessions/>

Question: 391

CertyIQ

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 subscription that contains the following resources:

- ⇒ A virtual network that has a subnet named Subnet1
- ⇒ Two network security groups (NSGs) named NSG-VM1 and NSG-Subnet1
- ⇒ A virtual machine named VM1 that has the required Windows Server configurations to allow Remote Desktop connections

NSG-Subnet1 has the default inbound security rules only.

NSG-VM1 has the default inbound security rules and the following custom inbound security rule:

- ⇒ Priority: 100
- ⇒ Source: Any
- ⇒ Source port range: *
- ⇒ Destination: *
- ⇒ Destination port range: 3389
- ⇒ Protocol: UDP
- ⇒ Action: Allow

VM1 has a public IP address and is connected to Subnet1. NSG-VM1 is associated to the network interface of VM1. NSG-Subnet1 is associated to Subnet1.

You need to be able to establish Remote Desktop connections from the internet to VM1.

Solution: You add an inbound security rule to NSG-Subnet1 that allows connections from the Any source to the *destination for port range 3389 and uses the TCP protocol. You remove NSG-VM1 from the network interface of VM1.

Does this meet the goal?

- A. Yes
- B. No

Answer: A**Explanation:**

The answer is Yes. The main point I miss was that NSG-Subnet1 is correctly modified with TCP 3389 and NSG-VM1 is removed. In this case you should be able to connect. - "Solution: You add an inbound security rule to NSG-Subnet1 that allows connections from the Any source to the *destination for port range 3389 and uses the TCP protocol. You remove NSG-VM1 from the network interface of VM1."

Question: 392**CertyIQ**

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 subscription that contains the following resources:

- ⇒ A virtual network that has a subnet named Subnet1
- ⇒ Two network security groups (NSGs) named NSG-VM1 and NSG-Subnet1
- ⇒ A virtual machine named VM1 that has the required Windows Server configurations to allow Remote Desktop connections

NSG-Subnet1 has the default inbound security rules only.

NSG-VM1 has the default inbound security rules and the following custom inbound security rule:

- ⇒ Priority: 100
- ⇒ Source: Any
- ⇒ Source port range: *
- ⇒ Destination: *
- ⇒ Destination port range: 3389

Protocol: UDP -

■

- ⇒ Action: Allow

VM1 has a public IP address and is connected to Subnet1. NSG-VM1 is associated to the network interface of VM1. NSG-Subnet1 is associated to Subnet1.

You need to be able to establish Remote Desktop connections from the internet to VM1.

Solution: You add an inbound security rule to NSG-Subnet1 that allows connections from the internet source to the VirtualNetwork destination for port range 3389 and uses the UDP protocol.

Does this meet the goal?

- A. Yes
- B. No

Answer: B**Explanation:**

The default port for RDP is TCP port 3389. A rule to permit RDP traffic must be created automatically when you create your VM.

Note on NSG-Subnet1: Azure routes network traffic between all subnets in a virtual network, by default.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-rdp-connection>

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 subscription that contains the following resources:

- ⇒ A virtual network that has a subnet named Subnet1
- ⇒ Two network security groups (NSGs) named NSG-VM1 and NSG-Subnet1
- ⇒ A virtual machine named VM1 that has the required Windows Server configurations to allow Remote Desktop connections

NSG-Subnet1 has the default inbound security rules only.

NSG-VM1 has the default inbound security rules and the following custom inbound security rule:

- ⇒ Priority: 100
- ⇒ Source: Any
- ⇒ Source port range: *
- ⇒ Destination: *
- ⇒ Destination port range: 3389
- ⇒ Protocol: UDP
- ⇒ Action: Allow

VM1 has a public IP address and is connected to Subnet1. NSG-VM1 is associated to the network interface of VM1. NSG-Subnet1 is associated to Subnet1.

You need to be able to establish Remote Desktop connections from the internet to VM1.

Solution: You add an inbound security rule to NSG-Subnet1 and NSG-VM1 that allows connections from the internet source to the VirtualNetwork destination for port range 3389 and uses the TCP protocol.

Does this meet the goal?

- A. Yes
- B. No

Answer: A**Explanation:**

To enable RDP, you need to add "Allow" rule for 3389 port on TCP protocol. this is matches the given suggested solution.

For the existing custom rule, priority doesn't matter if it is 100 or not. As "Network security group security rules are evaluated by priority using the 5-tuple information (source, source port, destination, destination port, and protocol) to allow or deny the traffic." So Azure checks the first rule, it finds that it has UDP. then It will check the second rule, it will find allow TCP on port 3389. So it will allow. Since the protocols are different, so those are totally different rules.

<https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview>

HOTSPOT -

You have a virtual network named VNet1 that has the configuration shown in the following exhibit.

```
Name          : VNet1
ResourceGroupName : Production
Location       : westus
Id            : /subscriptions/14d26092-8e42-4ea7-b770-
9dcef70fb1ea/resourceGroups/Production/providers/Microsoft.Network/virtualNetworks/VNet1
Etag          : W/"76f7edd6-d022-455b-aeae-376059318e5d"
ResourceGuid   : 562696cc-b2ba-4cc5-9619-0a735d6c34c7
ProvisioningState : Succeeded
Tags          :
AddressSpace  : {
    "AddressPrefixes": [
        "10.2.0.0/16"
    ]
}
DhcpOptions   : {}
Subnets       : [
    {
        "Name": "default",
        "Etag": "W/\\"76f7edd6-d022-455b-aeae-376059318e5d\\\"",
        "Id": "/subscriptions/14d26092-8e42-4ea7-b770-
9dcef70fb1ea/resourceGroups/Production/providers/Microsoft.Network/
virtualNetworks/VNet1/subnets/default",
        "AddressPrefix": "10.2.0.0/24",
        "IpConfigurations": [],
        "ResourceNavigationLinks": [],
        "ServiceEndpoints": [],
        "ProvisioningState": "Succeeded"
    }
]
VirtualNetworkPeerings : []
EnableDDoSProtection : false
EnableVmProtection   : false
```

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Before a virtual machine on VNet1 can receive an IP address from 192.168.1.0/24, you must first

add a network interface
add a subnet
add an address space
delete a subnet
delete an address space

Before a virtual machine on VNet1 can receive an IP address from 10.2.1.0/24, you must first

add a network interface
add a subnet
add an address space
delete a subnet
delete an address space

Answer:

Answer Area

Before a virtual machine on VNet1 can receive an IP address from 192.168.1.0/24, you must first

- add a network interface
- add a subnet
- add an address space**
- delete a subnet
- delete an address space

Before a virtual machine on VNet1 can receive an IP address from 10.2.1.0/24, you must first

- add a network interface
- add a subnet**
- add an address space
- delete a subnet
- delete an address space

Explanation:

Box 1: add an address space –

Your IaaS virtual machines (VMs) and PaaS role instances in a virtual network automatically receive a private IP address from a range that you specify, based on the address space of the subnet they are connected to. We need to add the 192.168.1.0/24 address space.

Box 2: add a subnet –

The 10.2.1.0/24 network exists. We need to add a network interface.

Reference:

<https://docs.microsoft.com/en-us/office365/enterprise/designing-networking-for-microsoft-azure-iaas>

Question: 395

CertyIQ

You have an Azure subscription that contains a virtual network named VNET1. VNET1 contains the subnets shown in the following table.

Name	Connected virtual machines
Subnet1	VM1, VM2
Subnet2	VM3, VM4
Subnet3	VM5, VM6

Each virtual machine uses a static IP address.

You need to create network security groups (NSGs) to meet following requirements:

⇒ Allow web requests from the internet to VM3, VM4, VM5, and VM6.

- Allow all connections between VM1 and VM2.
 - Allow Remote Desktop connections to VM1.
 - Prevent all other network traffic to VNET1.
- What is the minimum number of NSGs you should create?

- 1
- 3
- 4
- 12

Answer: A

Explanation:

NSGs can be associated to subnets, individual VMs (classic), or individual network interfaces (NIC) attached to VMs (Resource Manager). You can associate zero, or one, NSG(s) to each VNet subnet and NIC in a virtual machine. The same NSG can be associated to as many subnets and NICs as you choose. So, you can create 1 NSG and associate it with all 3 Subnets. - Allow web requests from internet to VM3, VM4, VM5 and VM 6: You need to add an inbound rule to allow Internet TCP 80 to VM3, VM4, VM5 and VM6 static IP addresses. - Allow all connections between VM1 & VM2: You do not need an NSG as communication in the same VNet is allowed by default, without even configuring NSG. - Allow remote desktop to VM1: You need to add an inbound rule to allow RDP 3389 in VM1's static IP address . - Prevent all other network traffic to VNET1: You do not need to configure any NSG as there is explicit deny rule (DenyAllInbound) in every NSG.

Question: 396

CertyIQ

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

Name	Type	Resource group
VNET1	Virtual network	RG1
VM1	Virtual machine	RG1

The Not allowed resource types Azure policy that has policy enforcement enabled is assigned to RG1 and uses the following parameters:

Microsoft.Network/virtualNetworks
Microsoft.Compute/virtualMachines

In RG1, you need to create a new virtual machine named VM2, and then connect VM2 to VNET1.

What should you do first?

- Remove Microsoft.Compute/virtualMachines from the policy.
- Create an Azure Resource Manager template
- Add a subnet to VNET1.
- Remove Microsoft.Network/virtualNetworks from the policy.

Answer: A

Explanation:

The Not allowed resource types Azure policy prohibits the deployment of specified resource types. You specify an array of the resource types to block.

Virtual Networks and Virtual Machines are prohibited.

Reference:

Question: 397

Your company has an Azure subscription named Subscription1.

The company also has two on-premises servers named Server1 and Server2 that run Windows Server 2016. Server1 is configured as a DNS server that has a primary DNS zone named adatum.com. Adatum.com contains 1,000 DNS records.

You manage Server1 and Subscription1 from Server2. Server2 has the following tools installed:

- ⇒ The DNS Manager console
- ⇒ Azure PowerShell
- ⇒ Azure CLI 2.0

You need to move the adatum.com zone to an Azure DNS zone in Subscription1. The solution must minimize administrative effort.

What should you use?

- A. Azure CLI
- B. Azure PowerShell
- C. the Azure portal
- D. the DNS Manager console

Answer: A

Explanation:

Azure CLI.

Azure DNS supports importing and exporting zone files by using the Azure command-line interface (CLI). Zone file import is not currently supported via Azure PowerShell or the Azure portal.

PrivateDNSMigrationScript is for migrating legacy Azure DNS private zones to the new Azure DNS private zone resource.

<https://docs.microsoft.com/en-us/azure/dns/dns-import-export>

Question: 398

You have a public load balancer that balances ports 80 and 443 across three virtual machines named VM1, VM2, and VM3.

You need to direct all the Remote Desktop Protocol (RDP) connections to VM3 only.

What should you configure?

- A. an inbound NAT rule
- B. a new public load balancer for VM3
- C. a frontend IP configuration
- D. a load balancing rule

Answer: A

Explanation:

An inbound NAT rule forwards incoming traffic to a specific virtual machine

Service: RDP

Protocol: TCP

Port: 3389

Target VM =VM3

Reference:

<https://docs.microsoft.com/en-us/azure/load-balancer/tutorial-load-balancer-port-forwarding-portal>

<https://pixelrobots.co.uk/2017/08/azure-load-balancer-for-rds/>

CertyIQ

Question: 399

HOTSPOT -

You have an Azure subscription named Subscription1 that contains the virtual networks in the following table.

Name	Subnets
VNet1	Subnet11, Subnet12
VNet2	Subnet13

Subscription1 contains the virtual machines in the following table.

Name	Subnet	Availability set
VM1	Subnet11	AS1
VM2	Subnet11	AS1
VM3	Subnet11	<i>Not applicable</i>
VM4	Subnet11	<i>Not applicable</i>
VM5	Subnet12	<i>Not applicable</i>
VM6	Subnet12	<i>Not applicable</i>

In Subscription1, you create a load balancer that has the following configurations:

- ⇒ Name: LB1
- ⇒ SKU: Basic
- ⇒ Type: Internal
- ⇒ Subnet: Subnet12
- ⇒ Virtual network: VNET1

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
LB1 can balance the traffic between VM1 and VM2.	<input type="radio"/>	<input type="radio"/>
LB1 can balance the traffic between VM3 and VM4.	<input type="radio"/>	<input type="radio"/>
LB1 can balance the traffic between VM5 and VM6.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
LB1 can balance the traffic between VM1 and VM2.	<input checked="" type="radio"/>	<input type="radio"/>
LB1 can balance the traffic between VM3 and VM4.	<input type="radio"/>	<input checked="" type="radio"/>
LB1 can balance the traffic between VM5 and VM6.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Basic Load Balancer: Backend pool endpoints for Virtual machines in a single availability set or virtual machine scale set.

Subnet12 association will be used to assign an IP for the internal load balancer, not to load balance the VMs in the Subnet.

Box 1: Yes

VM1 and VM are in the Availability Set.

Box 2: No

Both VMs are not part of any Availability Set or Scale Set.

Box 3: No

Both VMs are not part of any Availability Set or Scale Set.

Reference:

<https://docs.microsoft.com/en-us/azure/load-balancer/skus>

<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-standard-overview>

Question: 400

CertyIQ

HOTSPOT -

You have an Azure virtual machine that runs Windows Server 2019 and has the following configurations:

- ⇒ Name: VM1
- ⇒ Location: West US
- ⇒ Connected to: VNET1
- ⇒ Private IP address: 10.1.0.4
- ⇒ Public IP addresses: 52.186.85.63
- ⇒ DNS suffix in Windows Server: Adatum.com

You create the Azure DNS zones shown in the following table.

Name	Type	Location
Adatum.pri	Private	West Europe
Contoso.pri	Private	Central US
Adatum.com	Public	West Europe
Contoso.com	Public	North Europe

You need to identify which DNS zones you can link to VNET1 and the DNS zones to which VM1 can automatically register.

Which zones should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

DNS zones that you can link to VNET1:

- Adatum.com only
- Adatum.pri and adatum.com only
- The private zones only
- The public zones only

DNS zones to which VM1 can automatically register:

- Adatum.com only
- Adatum.pri and adatum.com only
- The private zones only
- The public zones only

Answer:

Answer Area

DNS zones that you can link to VNET1:

- Adatum.com only
- Adatum.pri and adatum.com only
- The private zones only
- The public zones only

DNS zones to which VM1 can automatically register:

- Adatum.com only
- Adatum.pri and adatum.com only
- The private zones only
- The public zones only

Explanation:

Box 1: The Private Zones only.

Box 2: The Private Zones only.

You can only link VNETs to private DNS zones only and accordingly auto register a VNET only to a private DNS zones. Private DNS zones can be linked with VNETs (not public ones). And VM can auto-register to any private DNS zone linked with the Vnet and with auto-registration option set.

To resolve the records of a private DNS zone from your virtual network, you must link the virtual network with the zone. Linked virtual networks have full access and can resolve all DNS records published in the private zone.

Reference:

<https://docs.microsoft.com/en-us/azure/dns/private-dns-overview>

Question: 401

CertyIQ

DRAG DROP -

You have an on-premises network that you plan to connect to Azure by using a site-to-site VPN. In Azure, you have an Azure virtual network named VNet1 that uses an address space of 10.0.0.0/16 VNet1 contains a subnet named Subnet1 that uses an address space of 10.0.0.0/24.

You need to create a site-to-site VPN to Azure.

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 choice is correct. You will receive credit for any of the correct orders you select.

Select and Place:

Actions

Create a local gateway.

Create a VPN gateway.

Create a gateway subnet.

Create a custom DNS server.

Create a VPN connection.

Create an Azure Content Delivery Network (CDN) profile.

Answer Area



Answer:

Actions

Answer Area

Create a local gateway.

Create a gateway subnet.

Create a VPN gateway.

Create a VPN gateway.

Create a gateway subnet.



Create a local gateway.



Create a custom DNS server.

Create a VPN connection.

Create a VPN connection.

Create an Azure Content Delivery Network (CDN) profile.

Explanation:

1 - Create a Gateway subnet. You need the subnet in place first before you can associate a VPN gateway with it, which is what is created next.

2 - Create a VPN gateway. Associate the VPN gateway with the gateway subnet you created (there are other steps but for the sake of what is available for answers, the prem side is now configured)

Now for the premice side.

3. Create a local gateway. You need the local gateway in order to complete the tunnel,
4. then you can create a VPN connection

Question: 402

CertyIQ

You have an Azure subscription that contains the resources in the following table.

Name	Type	Details
VNet1	Virtual network	<i>Not applicable</i>
Subnet1	Subnet	Hosted on VNet1
VM1	Virtual machine	On Subnet1
VM2	Virtual machine	On Subnet1

VM1 and VM2 are deployed from the same template and host line-of-business applications. You configure the network security group (NSG) shown in the exhibit. (Click the Exhibit tab.)

[Move](#) [Delete](#) [Refresh](#)

Resource group (change) : RG1lod9053488
Location : East US
Subscription (change) : Microsoft AZ
Subscription ID : ac344a74-f85a-4b2e-8057-642088faaf20

Custom security rules : 1 inbound, 1 outbound
Associated with : 0 subnets, 0 network interfaces

Tags (change) : [Click here to add tags](#)

Inbound security rules

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	Port_80	80	TCP	Internet	Any	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Allow AzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Outbound security rules

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	⚠ DenyWebSites	80	TCP	Any	Internet	Deny
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

You need to prevent users of VM1 and VM2 from accessing websites on the Internet over TCP port 80.
What should you do?

- A. Disassociate the NSG from a network interface
- B. Change the Port_80 inbound security rule.
- C. Associate the NSG to Subnet1.
- D. Change the DenyWebSites outbound security rule.

Answer: C

Explanation:

You can associate or dissociate a network security group from a network interface or subnet.

The NSG has the appropriate rule to block users from accessing the Internet. We just need to associate it with Subnet1.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/manage-network-security-group>

Question: 403

CertyIQ

You have two subscriptions named Subscription1 and Subscription2. Each subscription is associated to a different Azure AD tenant.

Subscription1 contains a virtual network named VNet1. VNet1 contains an Azure virtual machine named VM1 and has an IP address space of 10.0.0.0/16.

Subscription2 contains a virtual network named VNet2. VNet2 contains an Azure virtual machine named VM2 and has an IP address space of 10.10.0.0/24.

You need to connect VNet1 to VNet2.

What should you do first?

- A. Move VM1 to Subscription2.
- B. Move VNet1 to Subscription2.

- C. Modify the IP address space of VNet2.
- D. Provision virtual network gateways.

Answer: D

Explanation:

The virtual networks can be in the same or different regions, and from the same or different subscriptions. When connecting VNets from different subscriptions, the subscriptions do not need to be associated with the same Active Directory tenant.

Configuring a VNet-to-VNet connection is a good way to easily connect VNets. Connecting a virtual network to another virtual network using the VNet-to-VNet connection type (VNet2VNet) is similar to creating a Site-to-Site IPsec connection to an on-premises location. Both connectivity types use a VPN gateway to provide a secure tunnel using IPsec/IKE, and both function the same way when communicating.

The local network gateway for each VNet treats the other VNet as a local site. This lets you specify additional address space for the local network gateway in order to route traffic.

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-vnet-vnet-resource-manager-portal>

Question: 404

CertyIQ

You plan to create an Azure virtual machine named VM1 that will be configured as shown in the following exhibit.

Create a virtual machine

⚠ Changing Basic options may reset selections you have made. Review all options prior to creating the virtual machine.

[Basics](#) [Disks](#) [Networking](#) [Management](#) [Advanced](#) [Tags](#) [Review + create](#)

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image.

Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization.

Looking for classic VMs? [Create VM from Azure Marketplace](#)

PROJECT DETAILS

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

* Subscription ?	<input type="text" value="MyDev-Test Subscription"/>	▼
* Resource group ?	<input type="text" value="RG1"/>	▼
	Create new	

INSTANCE DETAILS

* Virtual machine name ?	<input type="text" value="VM1"/>	▼
* Region ?	<input type="text" value="(US) West US 2"/>	▼
Availability options ?	<input type="text" value="No infrastructure redundancy required"/>	▼
* Image ?	<input type="text" value="Windows Server 2016 Datacenter"/>	▼
	Browse all public and private images	
Azure Spot instance ?	<input type="radio"/> Yes <input checked="" type="radio"/> No	

* Size ?

Standard DS1 v2

1 vcpu, 3.5 GiB memory (ZAR 632.47/month)

[Change size](#)

The planned disk configurations for VM1 are shown in the following exhibit.

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

Disk options

* OS disk type [?](#)

Standard HDD

The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.

Enable Ultra Disk compatibility (Preview) [?](#) Yes No

Ultra Disks are only available when using Managed Disks.

Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

 Adding unmanaged data disks is currently not supported at the time of VM creation. You can add them after the VM is created.

Advanced

Use managed disks [?](#)

No Yes

* Storage account [?](#)

(new) rg1 disks799



[Create new](#)

You need to ensure that VM1 can be created in an Availability Zone.

Which two settings should you modify? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

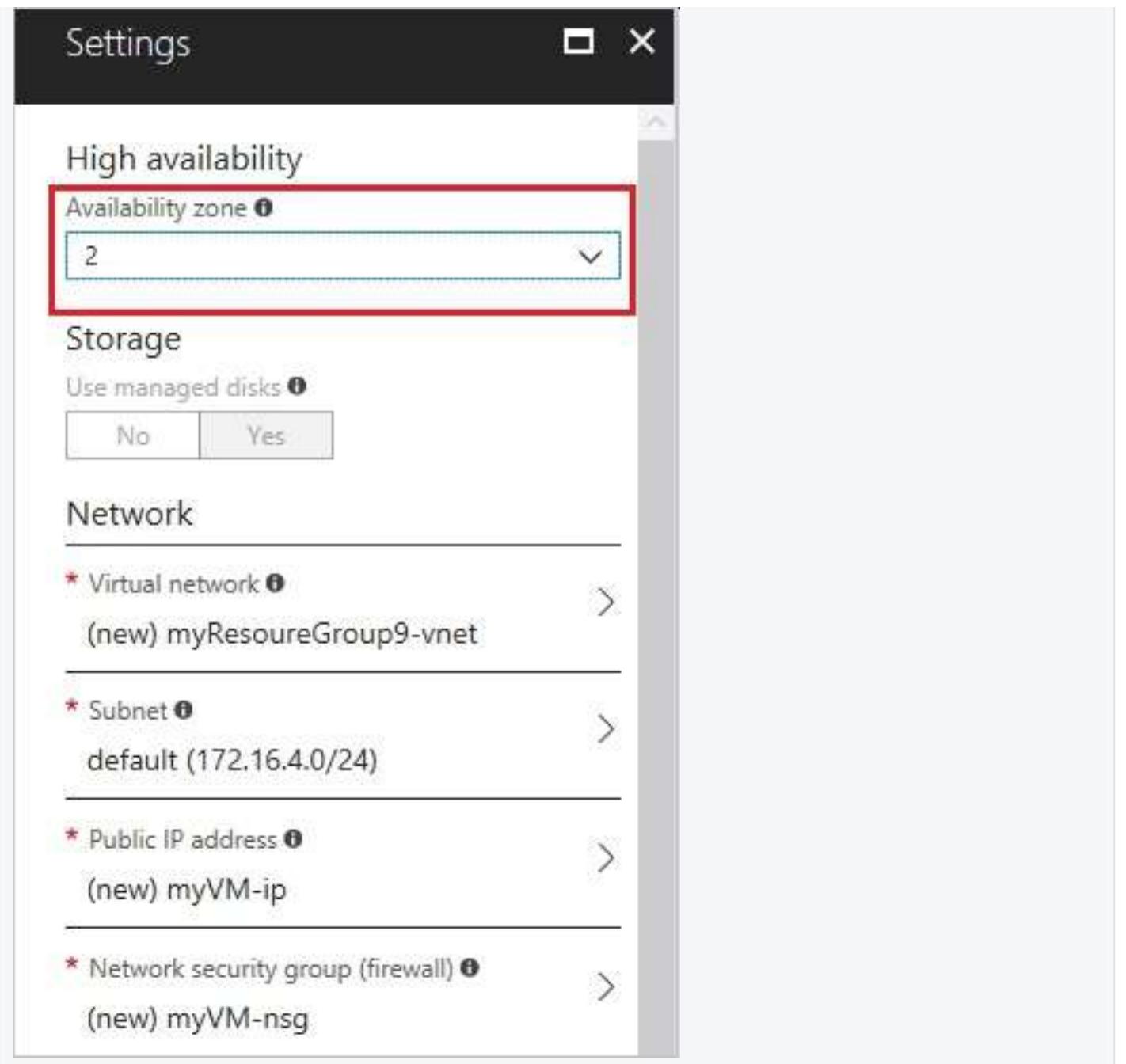
- A. Use managed disks
- B. OS disk type
- C. Availability options
- D. Size
- E. Image

Answer: AC

Explanation:

A: Your VMs should use managed disks if you want to move them to an Availability Zone by using Site Recovery.

C: When you create a VM for an Availability Zone, Under Settings > High availability, select one of the numbered zones from the Availability zone dropdown.



Reference:

<https://docs.microsoft.com/en-us/azure/site-recovery/move-azure-vms-avset-azone> <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/create-portal-availability-zone>

Question: 405

CertyIQ

HOTSPOT -

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

Name	Type	Resource group	Location
RG1	Resource group	<i>Not applicable</i>	Central US
RG2	Resource group	<i>Not applicable</i>	West US
RG3	Resource group	<i>Not applicable</i>	East US
VMSS1	Virtual machine scale set	RG1	West US

VMSS1 is set to VM (virtual machines) orchestration mode.

You need to deploy a new Azure virtual machine named VM1, and then add VM1 to VMSS1.

Which resource group and location should you use to deploy VM1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Resource group:

RG1 only
RG2 only
RG1 or RG2 only
RG1, RG2, or RG3

Location:

West US only
Central US only
Central US or West US only
East US, Central US, or West US

Answer:

Answer Area

Resource group:

RG1 only
RG2 only
RG1 or RG2 only
RG1, RG2, or RG3

Location:

West US only
Central US only
Central US or West US only
East US, Central US, or West US

Explanation:

Box 1: RG1, RG2, or RG3 -

The resource group stores metadata about the resources. When you specify a location for the resource group, you're specifying where that metadata is stored.

Box 2: West US only -

Note: Virtual machine scale sets will support 2 distinct orchestration modes:

ScaleSetVM " Virtual machine instances added to the scale set are based on the scale set configuration model. The virtual machine instance lifecycle - creation, update, deletion - is managed by the scale set. VM (virtual machines) " Virtual machines created outside of the scale set can be explicitly added to the scaleset.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/overview>

Question: 406

CertyIQ

HOTSPOT -

You have an Azure subscription that contains three virtual networks named VNET1, VNET2, and VNET3. Peering for VNET1 is configured as shown in the following exhibit.

The screenshot shows the 'VNET1 | Peerings' blade. On the left is a navigation menu with links like Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. The main area has a search bar and buttons for 'Add' and 'Refresh'. A table lists two peerings:

NAME	PEERING STATUS	PEER	GATEWAY TRANSIT
Peering1	Connected	VNET2	Disabled
Peering1	Connected	VNET3	Disabled

Peering for VNET2 is configured as shown in the following exhibit.

The screenshot shows the 'VNET2 | Peerings' blade. The left navigation menu is identical to the previous one. The main area shows a search bar, 'Add' button, and 'Refresh' button. A table lists one peering entry:

NAME	PEERING STATUS	PEER	GATEWAY TRANSIT
Peering1	Connected	VNET1	Disabled

Peering for VNET3 is configured as shown in the following exhibit.

The screenshot shows the 'VNET3 | Peerings' blade. The left navigation menu is identical. The main area shows a search bar, 'Add' button, and 'Refresh' button. A table lists one peering entry:

NAME	PEERING STATUS	PEER	GATEWAY TRANSIT
Peering1	Connected	VNET1	Disabled

How can packets be routed between the virtual networks? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Packets from VNET1 can be routed to:

VNET2 only
VNET3 only
VNET2 and VNET3

Packets from VNET2 can be routed to:

VNET1 only
VNET3 only
VNET1 and VNET3

Answer:

Answer Area

Packets from VNET1 can be routed to:

VNET2 only
VNET3 only
VNET2 and VNET3

Packets from VNET2 can be routed to:

VNET1 only
VNET3 only
VNET1 and VNET3

Explanation:

Box 1. VNET2 and VNET3

VNet1 is peered with VNet2 and VNet3. Also Gateway transit is disabled.

Box 2: VNET1 only

Gateway transit is disabled, so it can only communicate with the connected VNET1.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview>

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-peering-gateway-transit>

Question: 407

CertyIQ

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 a computer named Computer1 that has a point-to-site VPN connection to an Azure virtual network named VNet1. The point-to-site connection uses a self-signed certificate.

From Azure, you download and install the VPN client configuration package on a computer named Computer2. You need to ensure that you can establish a point-to-site VPN connection to VNet1 from Computer2.

Solution: You modify the Azure Active Directory (Azure AD) authentication policies.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Instead export the client certificate from Computer1 and install the certificate on Computer2.

Note:

Each client computer that connects to a VNet using Point-to-Site must have a client certificate installed. You generate a client certificate from the self-signed root certificate, and then export and install the client certificate. If the client certificate is not installed, authentication fails.

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-certificates-point-to-site>

Question: 408

CertyIQ

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 a computer named Computer1 that has a point-to-site VPN connection to an Azure virtual network named VNet1. The point-to-site connection uses a self-signed certificate.

From Azure, you download and install the VPN client configuration package on a computer named Computer2.

You need to ensure that you can establish a point-to-site VPN connection to VNet1 from Computer2.

Solution: You join Computer2 to Azure Active Directory (Azure AD).

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

A client computer that connects to a VNet using Point-to-Site must have a client certificate installed. Instead export the client certificate from Computer1 and install the certificate on Computer2.

A Point-to-Site (P2S) VPN gateway connection lets you create a secure connection to your virtual network from an individual client computer. A P2S connection is established by starting it from the client computer. This solution is useful for telecommuters who want to connect to Azure VNets from a remote location, such as from home or a conference. P2S VPN is also a useful solution to use instead of S2S VPN when you have only a few clients that need to connect to a VNet. This article applies to the Resource Manager deployment model.

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-certificates-point-to-site>

Question: 409

CertyIQ

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 subscription that contains 10 virtual networks. The virtual networks are hosted in separate resource groups.

Another administrator plans to create several network security groups (NSGs) in the subscription.

You need to ensure that when an NSG is created, it automatically blocks TCP port 8080 between the virtual networks.

Solution: You create a resource lock, and then you assign the lock to the subscription.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

No

You need to use a custom policy definition, because there is not a built-in policy and Resource Lock is an irrelevant solution.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-policy/policy-definition>

<https://docs.microsoft.com/en-us/azure/governance/policy/samples/built-in-policies>

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json>

Question: 410

CertyIQ

You have an Azure subscription named Subscription1. Subscription1 contains a virtual machine named VM1. You have a computer named Computer1 that runs Windows 10. Computer1 is connected to the Internet. You add a network interface named vm1173 to VM1 as shown in the exhibit. (Click the Exhibit tab.)

 Network Interface: **vm1173**
Virtual network/subnet: **RG1-vnet/default**
networking: **Disabled**

Effective security rules
Public IP: **VM1-ip**

Topology
Private IP: **10.0.0.5** Accelerated

Inbound port rules

Outbound port rules

Application security groups

Load balancing

 Network security group **VM1-nsg** (attached to network interface: **vm1173**)

Impacts 0 subnets, 1 network interfaces

Add inbound port rule

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINA...	ACTION	...
300	 RDP	3389	TCP	Any	Any	 Allow	...
65000	AllowVnetInBound	Any	Any	VirtualN...	VirtualN...	 Allow	...
65001	AllowAzureLoadB...	Any	Any	AzureLo...	Any	 Allow	...
65500	DenyAllInBound	Any	Any	Any	Any	 Deny	...

From Computer1, you attempt to connect to VM1 by using Remote Desktop, but the connection fails. You need to establish a Remote Desktop connection to VM1. What should you do first?

- A. Change the priority of the RDP rule
- B. Attach a network interface
- C. Delete the DenyAllInBound rule
- D. Start VM1

Answer: D

Explanation:

D. Start VM1

If you are unable to connect to VM1 via Remote Desktop Protocol (RDP), the first thing to check is whether VM1 is running. If the VM is stopped or deallocated, it will not accept RDP connections.

Incorrect Answers:

A: Rules are processed in priority order, with lower numbers processed before higher numbers, because lower numbers have higher priority. Once traffic matches a rule, processing stops. RDP already has the lowest number and thus the highest priority.

B: The network interface has already been added to VM.

C: The Outbound rules are fine.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/security-overview>

You have the Azure virtual machines shown in the following table.

Name	IP address	Connected to
VM1	10.1.0.4	VNET1/Subnet1
VM2	10.1.10.4	VNET1/Subnet2
VM3	172.16.0.4	VNET2/SubnetA
VM4	10.2.0.8	VNET3/SubnetB

A DNS service is installed on VM1.

You configure the DNS servers settings for each virtual network as shown in the following exhibit.

The screenshot shows the Azure portal interface for configuring DNS servers. At the top, there are 'Save' and 'Discard' buttons. Below them, the 'DNS servers' section has an 'i' icon. There are two options: 'Default (Azure-provided)' (unchecked) and 'Custom' (checked). A list of DNS servers is shown, starting with '10.1.0.4' followed by three ellipses (...). Below this list is a button labeled 'Add DNS server' with its own set of ellipses (...).

You need to ensure that all the virtual machines can resolve DNS names by using the DNS service on VM1. What should you do?

- A. Configure a conditional forwarder on VM1
- B. Add service endpoints on VNET1
- C. Add service endpoints on VNET2 and VNET3
- D. Configure peering between VNET1, VNET2, and VNET3

Answer: D

Explanation:

Virtual network peering enables you to seamlessly connect networks in Azure Virtual Network. The virtual networks appear as one for connectivity purposes. The traffic between virtual machines uses the Microsoft backbone infrastructure.

Incorrect Answers:

B, C: Virtual Network (VNet) service endpoint provides secure and direct connectivity to Azure services over an optimized route over the Azure backbone network.

Endpoints allow you to secure your critical Azure service resources to only your virtual networks. Service Endpoints enables private IP addresses in the VNet to reach the endpoint of an Azure service without needing a public IP address on the VNet.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview> <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview>

HOTSPOT -

You have an Azure subscription that contains the Azure virtual machines shown in the following table.

Name	Connected to subnet
VM1	172.16.1.0/24
VM2	172.16.2.0/24

You add inbound security rules to a network security group (NSG) named NSG1 as shown in the following table.

Priority	Source	Destination	Protocol	Port	Action
100	172.16.1.0/24	172.16.2.0/24	TCP	Any	Allow
101	Any	172.16.2.0/24	TCP	Any	Deny

You run Azure Network Watcher as shown in the following exhibit.

Resource group *

RG1



Source type *

Virtual machine



* Virtual machine

VM1



Destination

Select a virtual machine Specify manually

Resource group *

RG1



Virtual machine *

VM2



Probe Settings

Protocol

TCP ICMP

Destination port *

8080



Advanced settings

Check

Status

Unreachable

Agent extension version

1.4

Source virtual machine

VM1

You run Network Watcher again as shown in the following exhibit.

Source type *

Virtual machine



★ Virtual machine

VM1

**Destination** Select a virtual machine Specify manually**Resource group ***

RG1



Virtual machine *

VM2

**Probe Settings**

Protocol

 TCP ICMP**Check****Status** ReachableAgent extension version
1.4**Source virtual machine**

VM1

Grid view**Topology view****Hops**

NAME	IP ADDRESS	STATUS	NEXT HOP IP ADDRESS	RTT FROM SOURCE [...]
VM1	172.16.1.4		172.16.2.4	0
VM2	172.16.2.4		-	-

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
NSG1 limits VM1 traffic	<input type="radio"/>	<input type="radio"/>
NSG1 applies to VM2	<input type="radio"/>	<input type="radio"/>
VM1 and VM2 connect to the same virtual network	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
NSG1 limits VM1 traffic	<input type="radio"/>	<input checked="" type="radio"/>
NSG1 applies to VM2	<input checked="" type="radio"/>	<input type="radio"/>
VM1 and VM2 connect to the same virtual network	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Box 1: No

NSG1 limits the traffic that is flowing into 172.16.2.0/24 (Subnet2), which host VM2.

Box 2: Yes

Since Network Watcher is showing that traffic from VM1 to VM2 is not reaching on the TCP port, that means that NSG1 is applied to VM2. We can understand for sure, that it is not applied to VM1.

Box 3: Yes

In Network Watcher, you can see that the next hop is the destination VM2. This means that they are part of the same virtual network.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works>

Question: 413

CertyIQ

You have the Azure virtual network named VNet1 that contains a subnet named Subnet1. Subnet1 contains three Azure virtual machines. Each virtual machine has a public IP address.

The virtual machines host several applications that are accessible over port 443 to users on the Internet.

Your on-premises network has a site-to-site VPN connection to VNet1.

You discover that the virtual machines can be accessed by using the Remote Desktop Protocol (RDP) from the Internet and from the on-premises network.

You need to prevent RDP access to the virtual machines from the Internet, unless the RDP connection is established from the on-premises network. The solution must ensure that all the applications can still be accessed by the Internet users.

What should you do?

- A. Modify the address space of the local network gateway
- B. Create a deny rule in a network security group (NSG) that is linked to Subnet1
- C. Remove the public IP addresses from the virtual machines
- D. Modify the address space of Subnet1

Answer: B**Explanation:**

You can use a site-to-site VPN to connect your on-premises network to an Azure virtual network. Users on your on-premises network connect by using the RDP or

SSH protocol over the site-to-site VPN connection. You don't have to allow direct RDP or SSH access over the internet.

Reference:

<https://docs.microsoft.com/en-us/azure/security/fundamentals/network-best-practices>

Question: 414

CertyIQ

You have an Azure subscription that contains the resources in the following table.

Name	Type
ASG1	Application security group
NSG1	Network security group (NSG)
Subnet1	Subnet
VNet1	Virtual network
NIC1	Network interface
VM1	Virtual machine

Subnet1 is associated to VNet1. NIC1 attaches VM1 to Subnet1.

You need to apply ASG1 to VM1.

What should you do?

- A. Associate NIC1 to ASG1
- B. Modify the properties of ASG1
- C. Modify the properties of NSG1

Answer: A

Explanation:

Application Security Group can be associated with NICs.

Application security groups enable you to configure network security as a natural extension of an application's structure, allowing you to group virtual machines and define network security policies based on those groups. You can reuse your security policy at scale without manual maintenance of explicit IP addresses. The platform handles the complexity of explicit IP addresses and multiple rule sets, allowing you to focus on your business logic.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups>

<https://tutorialsdojo.com/network-security-group-nsg-vs-application-security-group>

References:

<https://docs.microsoft.com/en-us/azure/virtual-network/security-overview#application-security-groups>

CertyIQ**Question: 415**

You have an Azure subscription named Subscription1 that contains an Azure virtual network named VNet1. VNet1 connects to your on-premises network by using Azure ExpressRoute.

You plan to prepare the environment for automatic failover in case of ExpressRoute failure.

You need to connect VNet1 to the on-premises network by using a site-to-site VPN. The solution must minimize cost.

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

NOTE: Each correct selection is worth one point.

- A. Create a connection
- B. Create a local site VPN gateway
- C. Create a VPN gateway that uses the VpnGw1 SKU
- D. Create a gateway subnet
- E. Create a VPN gateway that uses the Basic SKU

Answer: ABC**Explanation:**

For a site to site VPN, you need:

- a local gateway
- a gateway subnet
- a VPN gateway
- a connection to connect the local gateway and the VPN gateway

However, the question states that VNet1 connects to your on-premises network by using Azure ExpressRoute.

For an ExpressRoute connection, VNET1 must already be configured with a gateway subnet so we don't need another one.

Note: BasicSKU cannot coexist with ExpressRoute. You must use a non-Basic SKU gateway for both the ExpressRoute gateway and the VPN gateway.

Question: 416

CertyIQ

HOTSPOT -

You have peering configured as shown in the following exhibit.

The screenshot shows two separate sections of the Azure portal. On the left, under 'Virtual networks', there is a list of virtual networks: test1-vnet, testVNET1, vNET1, vNET2, vNET3, vNET4, vNET5, and vNET6. vNET6 is highlighted with a light blue background. On the right, under 'VNet 6 - Peerings', there is a table titled 'Peerings' with two entries: 'peering1' and 'peering2'. Both peerings are listed as 'Disconnected'. The 'PEER' column shows 'vNET1' for peering1 and 'vNET2' for peering2. The 'GATEWAY TRANSIT' column shows 'Enabled' for peering1 and 'Disabled' for peering2.

NAME	PEERING STATUS	PEER	GATEWAY TRANSIT
peering1	Disconnected	vNET1	Enabled
peering2	Disconnected	vNET2	Disabled

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Hosts on vNET6 can communicate with hosts on [answer choice].

vNET6 only
vNET6 and vNET1 only
vNET6, vNET1, and vNET2 only
all the virtual networks in the subscription

To change the status of the peering connection to vNET1 to **Connected**, you must first [answer choice].

add a service endpoint
add a subnet
delete peering1
modify the address space

Answer:

Answer Area

Hosts on vNET6 can communicate with hosts on [answer choice].

vNET6 only
vNET6 and vNET1 only
vNET6, vNET1, and vNET2 only
all the virtual networks in the subscription

To change the status of the peering connection to vNET1 to **Connected**, you must first [answer choice].

add a service endpoint
add a subnet
delete peering1
modify the address space

Explanation:

Box 1: vNET6 only -

Peering status to both VNet1 and Vnet2 are disconnected.

Box 2: delete peering1 -

Peering to Vnet1 is Enabled but disconnected. We need to update or re-create the remote peering to get it back to Initiated state.

Reference:

<https://blog.kloud.com.au/2018/10/19/address-space-maintenance-with-vnet-peering/>

Question: 417

CertyIQ

HOTSPOT -

You have an Azure subscription that contains the resources in the following table.

Name	Type
VM1	Virtual machine
VM2	Virtual machine
LB1	Load balancer (Basic SKU)

You install the Web Server server role (IIS) on VM1 and VM2, and then add VM1 and VM2 to LB1. LB1 is configured as shown in the LB1 exhibit. (Click the LB1 tab.)

Essentials ^

Resource group (change)	Backend pool
VMRG	Backend1 (2 virtual machines)
Location	Health probe
West Europe	Probe1(HTTP:80/Probe1.htm)
Subscription name (change)	Load balancing rule
Azure Pass	Rule1 (TCP/80)
Subscription ID	NAT rules
e65d2b22-fde8	-
SKU	Public IP address
Basic	104.40.178.194 (LB1)

Rule1 is configured as shown in the Rule1 exhibit. (Click the Rule1 tab.)

* Name

Rule1

* IP Version

IPv4

IPv6

* Frontend IP address ⓘ

104.40.178.194 (LoadBalanceFrontEnd)



Protocol

TCP

UDP

* Port

80

* Backend port ⓘ

80

Backend pool ⓘ

Backend1 (2 virtual machines)



Health probe ⓘ

Probe1 (HTTP:80/Probe1.htm)



Session persistence ⓘ

None



Idle timeout (minutes) ⓘ



4

Floating IP (direct server return) ⓘ

Disabled

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
VM1 is in the same availability set as VM2.	<input type="radio"/>	<input type="radio"/>
If Probe1.htm is present on VM1 and VM2, LB1 will balance TCP port 80 between VM1 and VM2.	<input type="radio"/>	<input type="radio"/>
If you delete Rule1, LB1 will balance all the requests between VM1 and VM2 for all the ports.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
VM1 is in the same availability set as VM2.	<input checked="" type="radio"/>	<input type="radio"/>
If Probe1.htm is present on VM1 and VM2, LB1 will balance TCP port 80 between VM1 and VM2.	<input checked="" type="radio"/>	<input type="radio"/>
If you delete Rule1, LB1 will balance all the requests between VM1 and VM2 for all the ports.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Box 1: Yes -

A Basic Load Balancer supports virtual machines in a single availability set or virtual machine scale set.

Box 2: Yes -

When using load-balancing rules with Azure Load Balancer, you need to specify health probes to allow Load Balancer to detect the backend endpoint status. The configuration of the health probe and probe responses determine which backend pool instances will receive new flows. You can use health probes to detect the failure of an application on a backend endpoint. You can also generate a custom response to a health probe and use the health probe for flow control to manage load or planned downtime. When a health probe fails, Load Balancer will stop sending new flows to the respective unhealthy instance. Outbound connectivity is not impacted, only inbound connectivity is impacted.

Box 3: No -

There will be no loadbalancing between the VMs.

Basic Load Balancer: Virtual machines in a single availability set or virtual machine scale set.

Standard Load Balancer: Any virtual machines or virtual machine scale sets in a single virtual network.

Reference:

<https://docs.microsoft.com/en-us/azure/load-balancer/skus>

<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-custom-probe-overview>

Question: 418

CertyIQ

HOTSPOT -

You have an Azure virtual machine named VM1 that connects to a virtual network named VNet1. VM1 has the following configurations:

- ⇒ Subnet: 10.0.0.0/24
- ⇒ Availability set: AVSet
- ⇒ Network security group (NSG): None
- ⇒ Private IP address: 10.0.0.4 (dynamic)
- ⇒ Public IP address: 40.90.219.6 (dynamic)

You deploy a standard, Internet-facing load balancer named slb1.

You need to configure slb1 to allow connectivity to VM1.

Which changes should you apply to VM1 as you configure slb1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Before you create a backend pool on slb1, you must:

- | |
|--|
| Create and assign an NSG to VM1 |
| Remove the public IP address from VM1 |
| Change the private IP address of VM1 to static |

Before you can connect to VM1 from slb1, you must:

- | |
|--|
| Create and configure an NSG |
| Remove the public IP address from VM1 |
| Change the private IP address of VM1 to static |

Answer:

Answer Area

Before you create a backend pool on slb1, you must:

- | |
|--|
| Create and assign an NSG to VM1 |
| Remove the public IP address from VM1 |
| Change the private IP address of VM1 to static |

Before you can connect to VM1 from slb1, you must:

- | |
|--|
| Create and configure an NSG |
| Remove the public IP address from VM1 |
| Change the private IP address of VM1 to static |

Explanation:

Change the private IP address of VM1 to static

Box 1: Remove the public IP address from VM1

Note: A public load balancer can provide outbound connections for virtual machines (VMs) inside your virtual

network. These connections are accomplished by translating their private IP addresses to public IP addresses. Public Load Balancers are used to load balance internet traffic to your VMs.

Box 2: Create and configure an NSG

NSGs are used to explicitly permit allowed traffic. If you do not have an NSG on a subnet or NIC of your virtual machine resource, traffic is not allowed to reach this resource.

Reference:

<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview>

Question: 419

CertyIQ

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

Name	Type	Location
VNET1	Virtual network	East US
IP1	Public IP address	West Europe
RT1	Route table	North Europe

You need to create a network interface named NIC1.

In which location can you create NIC1?

- A. East US and North Europe only
- B. East US only
- C. East US, West Europe, and North Europe
- D. East US and West Europe only

Answer: B

Explanation:

Before creating a network interface, you must have an existing virtual network in the same location and subscription you create a network interface in.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface>

Question: 420

CertyIQ

You have Azure virtual machines that run Windows Server 2019 and are configured as shown in the following table.

Name	Virtual network name	DNS suffix configured in Windows Server
VM1	VNET1	Contoso.com
VM2	VNET2	Contoso.com

You create a public Azure DNS zone named adatum.com and a private Azure DNS zone named contoso.com. For contoso.com, you create a virtual network link named link1 as shown in the exhibit. (Click the Exhibit tab.)

Save Discard Delete Access Control (IAM) Tags

Link name

link1

Link state

Completed

Provisioning state

Succeeded

Virtual network details

Virtual network id

/subscriptions/8372f433-2dcd-4361-b5ef-5b188fed87d0/resourceGroups/RG2/provi...

Virtual network

VNET1

Configuration

Enable auto registration

You discover that VM1 can resolve names in contoso.com but cannot resolve names in adatum.com. VM1 can resolve other hosts on the Internet.

You need to ensure that VM1 can resolve host names in adatum.com.

What should you do?

- A. Update the DNS suffix on VM1 to be adatum.com
- B. Configure the name servers for adatum.com at the domain registrar
- C. Create an SRV record in the contoso.com zone
- D. Modify the Access control (IAM) settings for link1

Answer: B

Explanation:

Adatum.com is a public DNS zone. The Internet top level domain DNS servers need to know which DNS servers to direct DNS queries for adatum.com to. You configure this by configuring the name servers for adatum.com at the domain registrar.

Question: 421

CertyIQ

HOTSPOT -

You plan to use Azure Network Watcher to perform the following tasks:

- ⇒ Task1: Identify a security rule that prevents a network packet from reaching an Azure virtual machine.
- ⇒ Task2: Validate outbound connectivity from an Azure virtual machine to an external host.

Which feature should you use for each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Task1:

- IP flow verify
- Next hop
- Packet capture
- Security group view
- Traffic Analytics

Task2:

- Connection troubleshoot
- IP flow verify
- Next hop
- NSG flow logs
- Traffic Analytics

Answer:

Answer Area

Task1:

- IP flow verify
- Next hop
- Packet capture
- Security group view
- Traffic Analytics

Task2:

- Connection troubleshoot
- IP flow verify
- Next hop
- NSG flow logs
- Traffic Analytics

Explanation:

Box 1: IP flow verify -

At some point, a VM may become unable to communicate with other resources, because of a security rule. The IP flow verify capability enables you to specify a source and destination IPv4 address, port, protocol (TCP or UDP), and traffic direction (inbound or outbound). IP flow verify then tests the communication and informs you if the connection succeeds or fails. If the connection fails, IP flow verify tells you which.

Box 2: Connection troubleshoot -

Diagnose outbound connections from a VM: The connection troubleshoot capability enables you to test a connection between a VM and another VM, an FQDN, a URI, or an IPv4 address. The test returns similar information returned when using the connection monitor capability, but tests the connection at a point in time, rather than monitoring it over time, as connection monitor does. Learn more about how to troubleshoot connections using connection-troubleshoot.

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview>

Question: 422

CertyIQ

HOTSPOT -

You have an Azure subscription that contains the Azure virtual machines shown in the following table.

Name	Operating system	Subnet	Virtual network
VM1	Windows Server 2019	Subnet1	VNET1
VM2	Windows Server 2019	Subnet2	VNET1
VM3	Red Hat Enterprise Linux 7.7	Subnet3	VNET1

You configure the network interfaces of the virtual machines to use the settings shown in the following table.

Name	DNS server
VM1	None
VM2	192.168.10.15
VM3	192.168.10.15

From the settings of VNET1 you configure the DNS servers shown in the following exhibit.

DNS servers 

Default (Azure-provided)

Custom

193.77.134.10

...

Add DNS ser

...

The virtual machines can successfully connect to the DNS server that has an IP address of 192.168.10.15 and the

DNS server that has an IP address of 193.77.134.10.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
VM1 connects to 193.77.134.10 for DNS queries.	<input type="radio"/>	<input type="radio"/>
VM2 connects to 193.77.134.10 for DNS queries.	<input type="radio"/>	<input type="radio"/>
VM3 connects to 192.168.10.15 for DNS queries.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
VM1 connects to 193.77.134.10 for DNS queries.	<input checked="" type="radio"/>	<input type="radio"/>
VM2 connects to 193.77.134.10 for DNS queries.	<input type="radio"/>	<input checked="" type="radio"/>
VM3 connects to 192.168.10.15 for DNS queries.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Box 1: Yes -

You can specify DNS server IP addresses in the VNet settings. The setting is applied as the default DNS server(s) for all VMs in the VNet.

Box 2: No -

You can set DNS servers per VM or cloud service to override the default network settings.

Box 3: Yes -

You can set DNS servers per VM or cloud service to override the default network settings.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-faq#name-resolution-dns>

Question: 423

CertyIQ

HOTSPOT -

You have an Azure subscription that contains the resource groups shown in the following table.

Name	Lock name	Lock type
RG1	None	None
RG2	Lock	Delete

RG1 contains the resources shown in the following table.

Name	Type	Lock name	Lock type
storage2	Storage account	Lock1	Delete
VNET2	Virtual network	Lock2	Read-only
IP2	Public IP address	None	None

You need to identify which resources you can move from RG1 to RG2, and which resources you can move from RG2 to RG1.

Which resources should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Resources that you can move from RG1 to RG2:

▼

None

IP1 only

IP1 and storage1 only

IP1 and VNET1 only

IP1, VNET2, and storage1

Resources that you can move from RG2 to RG1:

▼

None

IP2 only

IP2 and storage2 only

IP2 and VNET2 only

IP2, VNET2, and storage2

Answer:

Answer Area

Resources that you can move from RG1 to RG2:

None
IP1 only
IP1 and storage1 only
IP1 and VNET1 only
IP1, VNET2, and storage1

Resources that you can move from RG2 to RG1:

None
IP2 only
IP2 and storage2 only
IP2 and VNET2 only
IP2, VNET2, and storage2

Explanation:

Box 1: IP1, VNET2, and storage1

Box 2: IP2, VNET2, and storage2

Locks are designed for any update or removal. In this case we want to move only, we are not deleting, and we are not changing anything in the resource.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources>

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/move-support-resources>

Question: 424

CertyIQ

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 subscription that contains the virtual machines shown in the following table.

Name	Public IP SKU	Connected to	Status
VM1	None	VNET1/Subnet1	Stopped (deallocated)
VM2	Basic	VNET1/Subnet2	Running

You deploy a load balancer that has the following configurations:

- ⇒ Name: LB1
- ⇒ Type: Internal
- ⇒ SKU: Standard
- ⇒ Virtual network: VNET1

You need to ensure that you can add VM1 and VM2 to the backend pool of LB1.

Solution: You create a Basic SKU public IP address, associate the address to the network interface of VM1, and then start VM1.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

A Backend Pool configured by IP address has the following limitations:

- ⇒ Standard load balancer only

Reference:

<https://docs.microsoft.com/en-us/azure/load-balancer/backend-pool-management>

Question: 425

CertyIQ

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 subscription that contains the virtual machines shown in the following table.

Name	Public IP SKU	Connected to	Status
VM1	None	VNET1/Subnet1	Stopped (deallocated)
VM2	Basic	VNET1/Subnet2	Running

You deploy a load balancer that has the following configurations:

- ⇒ Name: LB1
- ⇒ Type: Internal
- ⇒ SKU: Standard
- ⇒ Virtual network: VNET1

You need to ensure that you can add VM1 and VM2 to the backend pool of LB1.

Solution: You create a Standard SKU public IP address, associate the address to the network interface of VM1, and then stop VM2.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

A Backend Pool configured by IP address has the following limitations:

- ⇒ Standard load balancer only

Reference:

Question: 426

CertyIQ

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 subscription that contains the virtual machines shown in the following table.

Name	Public IP SKU	Connected to	Status
VM1	None	VNET1/Subnet1	Stopped (deallocated)
VM2	Basic	VNET1/Subnet2	Running

You deploy a load balancer that has the following configurations:

- ⇒ Name: LB1
- ⇒ Type: Internal
- ⇒ SKU: Standard
- ⇒ Virtual network: VNET1

You need to ensure that you can add VM1 and VM2 to the backend pool of LB1.

Solution: You create two Standard SKU public IP addresses and associate a Standard SKU public IP address to the network interface of each virtual machine.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

A - Yes

You can only attach virtual machines that are in the same location and on the same virtual network as the LB.

Virtual machines must have a standard SKU public IP or no public IP.

The LB needs to be a standard SKU to accept individual VMs outside an availability set or vms. VMs do not need to have public IPs but if they do have them they have to be standard SKU. VMs can only be from a single network. When they don't have a public IP they are assigned an ephemeral IP.

Also, when adding them to a backend pool, it doesn't matter in which status are the VMs.

Note: Load balancer and the public IP address SKU must match when you use them with public IP addresses.

A Backend Pool configured by IP address has the following limitations:

- ⇒ Standard load balancer only

Reference:

<https://docs.microsoft.com/en-us/azure/load-balancer/backend-pool-management>

Question: 427

CertyIQ

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 a computer named Computer1 that has a point-to-site VPN connection to an Azure virtual network named VNet1. The point-to-site connection uses a self-signed certificate.

From Azure, you download and install the VPN client configuration package on a computer named Computer2.

You need to ensure that you can establish a point-to-site VPN connection to VNet1 from Computer2.

Solution: You export the client certificate from Computer1 and install the certificate on Computer2.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Each client computer that connects to a VNet using Point-to-Site must have a client certificate installed. You generate a client certificate from the self-signed root certificate, and then export and install the client certificate. If the client certificate is not installed, authentication fails.

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-certificates-point-to-site>

Question: 428

CertyIQ

You have an Azure virtual machine named VM1.

The network interface for VM1 is configured as shown in the exhibit. (Click the Exhibit tab.)

APPLICATION SECURITY GROUPS

 Configure the application security groups

INBOUND PORT RULES

 Network security group **VM1-nsg** (attached to network interface: **vm1175**)
 Impacts 0 subnets, 1 network interfaces

Add inbound port rule

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION	
300	 RDP	3389	TCP	Any	Any	 Allow	
400	 Rule1	80	TCP	Any	Any	 Deny	
500	Rule2	80,443	TCP	Any	Any	 Deny	
1000	Rule4	50-100,400-500	UDP	Any	Any	 Allow	
2000	Rule5	50-5000	Any	Any	VirtualNetwork	 Deny	
3000	Rule6	150-300	Any	Any	Any	 Allow	
4000	Rule3	60-500	Any	Any	VirtualNetwork	 Allow	
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	 Allow	
65001	AllowAzureLoadBalancerInBo...	Any	Any	AzureLoadBal... ancer	Any	 Allow	
65500	DenyAllInBound	Any	Any	Any	Any	 Deny	

You deploy a web server on VM1, and then create a secure website that is accessible by using the HTTPS protocol. VM1 is used as a web server only.

You need to ensure that users can connect to the website from the Internet.

What should you do?

- A. Modify the protocol of Rule4
- B. Delete Rule1
- C. For Rule5, change the Action to Allow and change the priority to 401
- D. Create a new inbound rule that allows TCP protocol 443 and configure the rule to have a priority of 501.

Answer: C

Explanation:

HTTPS uses port 443.

Rule2, with priority 500, denies HTTPS traffic.

Rule5, with priority changed from 2000 to 401, would allow HTTPS traffic.

Note: Priority is a number between 100 and 4096. Rules are processed in priority order, with lower numbers processed before higher numbers, because lower numbers have higher priority. Once traffic matches a rule, processing stops. As a result, any rules that exist with lower priorities (higher numbers) that have the same attributes as rules with higher priorities are not processed.

Note:

There are several versions of this question in the exam. The question has two possible correct answers:

- 1. Change the priority of Rule3 to 450.
- 2. For Rule5, change the Action to Allow and change the priority to 401.

Other incorrect answer options you may see on the exam include the following:

- ⇒ Modify the action of Rule1.

- ⇒ Change the priority of Rule6 to 100.
- ⇒ For Rule4, change the protocol from UDP to Any.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview>

CertyIQ

Question: 429

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 subscription that contains 10 virtual networks. The virtual networks are hosted in separate resource groups.

Another administrator plans to create several network security groups (NSGs) in the subscription.

You need to ensure that when an NSG is created, it automatically blocks TCP port 8080 between the virtual networks.

Solution: From the Resource providers blade, you unregister the Microsoft.ClassicNetwork provider.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

You should use a policy definition.

Resource policy definition used by Azure Policy enables you to establish conventions for resources in your organization by describing when the policy is enforced and what effect to take. By defining conventions, you can control costs and more easily manage your resources.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-policy/policy-definition>

CertyIQ

Question: 430

HOTSPOT -

You manage two Azure subscriptions named Subscription1 and Subscription2.

Subscription1 has following virtual networks:

Name	Address space	Location
VNET1	10.10.10.0/24	West Europe
VNET2	172.16.0.0/16	West US

The virtual networks contain the following subnets:

Name	Address space	In virtual network
Subnet11	10.10.10.0/24	VNET1
Subnet21	172.16.0.0/18	VNET2
Subnet22	172.16.128.0/18	VNET2

Subscription2 contains the following virtual network:

- ⇒ Name: VNETA

⇒ Address space: 10.10.128.0/17

⇒ Location: Canada Central

VNETA contains the following subnets:

Name	Address space
SubnetA1	10.10.130.0/24
SubnetA2	10.10.131.0/24

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
------------	-----	----

A Site-to-Site connection can be established between VNET1 and VNET2.

VNET1 and VNET2 can be peered.

VNET1 and VNETA can be peered.

Answer:

Answer Area

Statements	Yes	No
------------	-----	----

A Site-to-Site connection can be established between VNET1 and VNET2.

VNET1 and VNET2 can be peered.

VNET1 and VNETA can be peered.

Explanation:

VNET1: 10.10.10.0 - 10.10.10.255

VNET2: 172.16.0.0 - 172.16.255.255

VNETA: 10.10.128.0 - 10.10.255.255

Box 1: No

To create a VNet to VNet VPN you need to have a special Gateway Subnet. Here, the VNet has no sufficient address space to create a Gateway Subnet and thus to establish a VNet to VNet VPN connection.

Box 2: Yes

For VNet peering the only consideration is that the VNets do not overlap. VNET1 and VNET2 do not overlap.

Box 3: Yes

For VNet peering the only consideration is that the VNets do not overlap. VNET1 and VNETA do not overlap.

Reference:

<https://azure.microsoft.com/en-us/blog/vnet-to-vnet-connecting-virtual-networks-in-azure-across-different-regions/> <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering#requirements-and-constraints>

Question: 431

CertyIQ

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 app named App1 that is installed on two Azure virtual machines named VM1 and VM2. Connections to App1 are managed by using an Azure Load Balancer.

The effective network security configurations for VM2 are shown in the following exhibit.

The screenshot shows the Azure portal interface for VM2 Networking. The left sidebar lists VM2 - Networking, Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. Under Settings, Networking is selected. The main pane displays the Network Interface: VM2-NIC1, with tabs for Effective security rules and Topology. It shows Virtual network/subnet: Vnet1/Subnet11, NIC Public IP: -, NIC Private IP: 10.240.11.5, and Accelerated networking: Disabled. Below this, there are tabs for Inbound port rules, Outbound port rules, Application security groups, and Load balancing. The Inbound port rules table is visible, showing the following rules:

Priority	Name	Port	Protocol	Source	Destination	Action
100	Allow_131.107.100.50	443	TCP	131.107.100.50	VirtualNetwork	Allow
200	BlockAllOther443	443	Any	Any	Any	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

You discover that connections to App1 from 131.107.100.50 over TCP port 443 fail.

You verify that the Load Balancer rules are configured correctly.

You need to ensure that connections to App1 can be established successfully from 131.107.100.50 over TCP port 443.

Solution: You create an inbound security rule that denies all traffic from the 131.107.100.50 source and has a cost of 64999.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

B - No

You want to establish a successful connection from 131.107.100.50 over TCP port 43, and the solution suggests to create a deny inbound rule with low priority. It doesn't make any sense.

Virtual machines in load-balanced pools: The source port and address range applied are from the originating computer, not the load balancer. The destination port and address range are for the destination computer, not the load balancer.

AllowAzureLoadBalancerInBound: The AzureLoadBalancer service tag translates to the virtual IP address of the host, 168.63.129.16 where the Azure health probe originates. Actual traffic does not travel through here, and if you don't use Azure Load Balancing, this rule can be overridden.

Reference:

<https://fastreroute.com/azure-network-security-groups-explained/>

Question: 432

CertyIQ

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 app named App1 that is installed on two Azure virtual machines named VM1 and VM2. Connections to App1 are managed by using an Azure Load Balancer.

The effective network security configurations for VM2 are shown in the following exhibit.

Priority	Name	Port	Protocol	Source	Destination	Action
100	Allow_131.107.100.50	443	TCP	131.107.100.50	VirtualNetwork	Allow
200	BlockAllOther443	443	Any	Any	Any	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

You discover that connections to App1 from 131.107.100.50 over TCP port 443 fail.

You verify that the Load Balancer rules are configured correctly.

You need to ensure that connections to App1 can be established successfully from 131.107.100.50 over TCP port 443.

Solution: You delete the BlockAllOther443 inbound security rule.

Does this meet the goal?

- A. Yes
- B. No

Answer: B**Explanation:**

Allow_131.107.100.50 rule has a higher priority (100) than BlockAllOther441 (200) and it allows inbound traffic over TCP 443 from source 131.107.100.50. App1 (VM1 and VM2) is in a VNet, so this rule applies. Unfortunately, we still cannot access App1, so the issue is somewhere else, maybe the VMs are off, or the firewall is blocking it.

Reference:

<https://fastreroute.com/azure-network-security-groups-explained/>

Question: 433**CertyIQ**

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 app named App1 that is installed on two Azure virtual machines named VM1 and VM2. Connections to App1 are managed by using an Azure Load Balancer.

The effective network security configurations for VM2 are shown in the following exhibit.

Priority	Name	Port	Protocol	Source	Destination	Action
100	Allow_131.107.100.50	443	TCP	131.107.100.50	VirtualNetwork	Allow
200	BlockAllOther443	443	Any	Any	Any	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

You discover that connections to App1 from 131.107.100.50 over TCP port 443 fail.

You verify that the Load Balancer rules are configured correctly.

You need to ensure that connections to App1 can be established successfully from 131.107.100.50 over TCP port 443.

Solution: You modify the priority of the Allow_131.107.100.50 inbound security rule.

Does this meet the goal?

- A. Yes
- B. No

Answer: B**Explanation:**

The rule currently has the highest priority.

Reference:

<https://fastreroute.com/azure-network-security-groups-explained/>

CertyIQ

Question: 434

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 subscription that contains 10 virtual networks. The virtual networks are hosted in separate resource groups.

Another administrator plans to create several network security groups (NSGs) in the subscription.

You need to ensure that when an NSG is created, it automatically blocks TCP port 8080 between the virtual networks.

Solution: You assign a built-in policy definition to the subscription.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Resource policy definition used by Azure Policy enables you to establish conventions for resources in your organization by describing when the policy is enforced and what effect to take. By defining conventions, you can control costs and more easily manage your resources.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-policy/policy-definition>

CertyIQ

Question: 435

You have an Azure subscription.

You plan to deploy an Azure Kubernetes Service (AKS) cluster to support an app named App1. On-premises clients connect to App1 by using the IP address of the pod.

For the AKS cluster, you need to choose a network type that will support App1.

What should you choose?

- A. kubenet
- B. Azure Container Networking Interface (CNI)
- C. Hybrid Connection endpoints
- D. Azure Private Link

Answer: B

Explanation:

With Azure CNI, every pod gets an IP address from the subnet and can be accessed directly. These IP addresses must be unique across your network space.

Incorrect Answers:

A: The kubenet networking option is the default configuration for AKS cluster creation. With kubenet, nodes

get an IP address from the Azure virtual network subnet. Pods receive an IP address from a logically different address space to the Azure virtual network subnet of the nodes. Network address translation (NAT) is then configured so that the pods can reach resources on the Azure virtual network.

C, D: AKS only supports Kubelet networking and Azure Container Networking Interface (CNI) networking

Reference:

<https://docs.microsoft.com/en-us/azure/aks/concepts-network>

CertyIQ

Question: 436

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 subscription that contains the virtual machines shown in the following table.

Name	Public IP SKU	Connected to	Status
VM1	None	VNET1/Subnet1	Stopped (deallocated)
VM2	Basic	VNET1/Subnet2	Running

You deploy a load balancer that has the following configurations:

- ⇒ Name: LB1
- ⇒ Type: Internal
- ⇒ SKU: Standard
- ⇒ Virtual network: VNET1

You need to ensure that you can add VM1 and VM2 to the backend pool of LB1.

Solution: You disassociate the public IP address from the network interface of VM2.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

You can only attach virtual machines that have a standard SKU public IP configuration or no public IP configuration. All IP configurations must be on the same virtual network.

Also, VMs do not have to be powered on when adding them to a backend pool.

CertyIQ

Question: 437

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 subscription that contains 10 virtual networks. The virtual networks are hosted in separate resource groups.

Another administrator plans to create several network security groups (NSGs) in the subscription.

You need to ensure that when an NSG is created, it automatically blocks TCP port 8080 between the virtual networks.

Solution: You configure a custom policy definition, and then you assign the policy to the subscription.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

Resource policy definition used by Azure Policy enables you to establish conventions for resources in your organization by describing when the policy is enforced and what effect to take. By defining conventions, you can control costs and more easily manage your resources.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-policy/policy-definition>

CertyIQ

Question: 438

You have two Azure virtual networks named VNet1 and VNet2. VNet1 contains an Azure virtual machine named VM1. VNet2 contains an Azure virtual machine named VM2.

VM1 hosts a frontend application that connects to VM2 to retrieve data.

Users report that the frontend application is slower than usual.

You need to view the average round-trip time (RTT) of the packets from VM1 to VM2.

Which Azure Network Watcher feature should you use?

- A. IP flow verify
- B. Connection troubleshoot
- C. Connection monitor
- D. NSG flow logs

Answer: C

Explanation:

The connection monitor capability monitors communication at a regular interval and informs you of reachability, latency, and network topology changes between the VM and the endpoint

Incorrect Answers:

A: The IP flow verify capability enables you to specify a source and destination IPv4 address, port, protocol (TCP or UDP), and traffic direction (inbound or outbound). IP flow verify then tests the communication and informs you if the connection succeeds or fails. If the connection fails, IP flow verify tells you which security rule allowed or denied the communication, so that you can resolve the problem.

B: The connection troubleshoot capability enables you to test a connection between a VM and another VM, an FQDN, a URI, or an IPv4 address. The test returns similar information returned when using the connection monitor capability, but tests the connection at a point in time, rather than monitoring it over time, as connection monitor does.

D: The NSG flow log capability allows you to log the source and destination IP address, port, protocol, and whether traffic was allowed or denied by an NSG.

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview>

CertyIQ

Question: 439

HOTSPOT -

You have an Azure subscription that contains the public load balancers shown in the following table.

Name	SKU
LB1	Basic
LB2	Standard

You plan to create six virtual machines and to load balance requests to the virtual machines. Each load balancer will load balance three virtual machines.

You need to create the virtual machines for the planned solution.

How should you create the virtual machines? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

The virtual machines that will be load balanced by using LB1 must:

- be connected to the same virtual network
- be created in the same resource group
- be created in the same availability set or virtual machine scale set
- run the same operating system

The virtual machines that will be load balanced by using LB2 must:

- be connected to the same virtual network
- be created in the same resource group
- be created in the same availability set or virtual machine scale set
- run the same operating system

Answer:

Answer Area

The virtual machines that will be load balanced by using LB1 must:

- be connected to the same virtual network
- be created in the same resource group
- be created in the same availability set or virtual machine scale set
- run the same operating system

The virtual machines that will be load balanced by using LB2 must:

- be connected to the same virtual network
- be created in the same resource group
- be created in the same availability set or virtual machine scale set
- run the same operating system

Explanation:

Box 1: be created in the same availability set or virtual machine scale set.

The Basic tier is quite restrictive. A load balancer is restricted to a single availability set, virtual machine scale set, or a single machine.

Box 2: be connected to the same virtual network

The Standard tier can span any virtual machine in a single virtual network, including blends of scale sets, availability sets, and machines.

Reference:

<https://www.petri.com/comparing-basic-standard-azure-load-balancers>

HOTSPOT -

You have an on-premises data center and an Azure subscription. The data center contains two VPN devices. The subscription contains an Azure virtual network named VNet1. VNet1 contains a gateway subnet.

You need to create a site-to-site VPN. The solution must ensure that if a single instance of an Azure VPN gateway fails, or a single on-premises VPN device fails, the failure will not cause an interruption that is longer than two minutes.

What is the minimum number of public IP addresses, virtual network gateways, and local network gateways required in Azure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Public IP addresses:

1
2
3
4

Virtual network gateways:

1
2
3
4

Local network gateways:

1
2
3
4

Answer:

Answer Area

Public IP addresses:

1
2
3
4

Virtual network gateways:

1
2
3
4

Local network gateways:

1
2
3
4

Explanation:

Box 1: 2 -

2 public IP addresses in the on-premises data center, and 2 public IP addresses in the VNET for the active-active. The most reliable option is to combine the active-active gateways on both your network and Azure, as shown in the diagram below.

Box 2: 2 -

Every Azure VPN gateway consists of two instances in an active-standby configuration. For any planned maintenance or unplanned disruption that happens to the active instance, the standby instance would take over (failover) automatically, and resume the S2S VPN or VNet-to-VNet connections.

Box 3: 2 -

Dual-redundancy: active-active VPN gateways for both Azure and on-premises networks

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-highlyavailable>

Question: 441**CertyIQ**

You have an Azure subscription that contains two virtual machines as shown in the following table.

Name	Operating system	Location	IP address	DNS server
VM1	Windows Server 2019	West Europe	10.0.0.4	Default (Azure-provided)
VM2	Windows Server 2019	West Europe	10.0.0.5	Default (Azure-provided)

You perform a reverse DNS lookup for 10.0.0.4 from VM2.

Which FQDN will be returned?

- A. vm1.core.windows.net
- B. vm1.azure.com
- C. vm1.westeurope.cloudapp.azure.com
- D. vm1.internal.cloudapp.net

Answer: D**Explanation:**

D. vm1.internal.cloudapp.net

In Azure, when performing a reverse DNS lookup for a private IP address within a virtual network (VNet), Azure assigns an internal Fully Qualified Domain Name (FQDN) in the format:

<vm-name>.internal.cloudapp.net

Since VM1 has the private IP 10.0.0.4, when VM2 performs a reverse DNS lookup, it will return:

vm1.internal.cloudapp.net

Question: 442**CertyIQ**

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 app named App1 that is installed on two Azure virtual machines named VM1 and VM2. Connections to App1 are managed by using an Azure Load Balancer.

The effective network security configurations for VM2 are shown in the following exhibit.

VM2 - Networking Virtual machine

Search (Ctrl+ /) Attach network interface Detach network interface

Network Interface: VM2-NIC1 Effective security rules Topology

Virtual network/subnet: Vnet1/Subnet1 NIC Public IP: - NIC Private IP: 10.240.11.5 Accelerated networking: Disabled

Inbound port rules Outbound port rules Application security groups Load balancing

Network security group NSG2 (attached to network interface: Subnet1) Impacts 1 subnets, 0 network interfaces Add inbound port rule

Priority	Name	Port	Protocol	Source	Destination	Action	...
100	Allow_131.107.100.50	443	TCP	131.107.100.50	VirtualNetwork	Allow	...
200	⚠️ BlockAllOther443	443	Any	Any	Any	Deny	...
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	...
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow	...
65500	DenyAllInBound	Any	Any	Any	Any	Deny	...

You discover that connections to App1 from 131.107.100.50 over TCP port 443 fail.

You verify that the Load Balancer rules are configured correctly.

You need to ensure that connections to App1 can be established successfully from 131.107.100.50 over TCP port 443.

Solution: You create an inbound security rule that allows any traffic from the AzureLoadBalancer source and has a cost of 150.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

B. No

To allow connections to App1 from 131.107.100.50 over TCP port 443, you need to create an inbound security rule that specifically allows traffic from the IP address 131.107.100.50 to port 443.

The given solution allows traffic from "AzureLoadBalancer" as the source. However, this only permits traffic originating from Azure's internal load balancer health probes, not from external public IP addresses like 131.107.100.50.

You create an inbound security rule that allows any traffic from the AzureLoadBalancer source and has a PRIORITY of 150.

Question: 443

CertyIQ

You have an Azure subscription that contains a policy-based virtual network gateway named GW1 and a virtual network named VNet1.

You need to ensure that you can configure a point-to-site connection from an on-premises computer to VNet1. Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Add a service endpoint to VNet1
- B. Reset GW1
- C. Create a route-based virtual network gateway
- D. Add a connection to GW1
- E. Delete GW1

F. Add a public IP address space to VNet1

Answer: CE

Explanation:

C: A VPN gateway is used when creating a VPN connection to your on-premises network.

Route-based VPN devices use any-to-any (wildcard) traffic selectors, and let routing/forwarding tables direct traffic to different IPsec tunnels. It is typically built on router platforms where each IPsec tunnel is modeled as a network interface or VTI (virtual tunnel interface).

E: Policy-based VPN devices use the combinations of prefixes from both networks to define how traffic is encrypted/decrypted through IPsec tunnels. It is typically built on firewall devices that perform packet filtering. IPsec tunnel encryption and decryption are added to the packet filtering and processing engine.

Incorrect Answers:

F: Point-to-Site connections do not require a VPN device or a public-facing IP address.

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/create-routebased-vpn-gateway-portal> <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-connect-multiple-policybased-rm-ps>

Question: 444

CertyIQ

HOTSPOT -

You have an Azure subscription that contains the resources in the following table:

Name	Type
VMRG	Resource group
VNet1	Virtual network
VNet2	Virtual network
VM5	Virtual machine connected to VNet1
VM6	Virtual machine connected to VNet2

In Azure, you create a private DNS zone named adatum.com. You set the registration virtual network to VNet2. The adatum.com zone is configured as shown in the following exhibit:

Resource group ([change](#))
vmrg

Name server 1

-

Subscription ([change](#))
Azure Pass

Name server 2

-

Subscription ID
a4fde29b-d56a-4f6c-8298-6c53cd0b720c

Name server 3

-

Name server 4

-

Tags ([change](#))
[Click here to add tags](#)



Search record sets

Name	Type	TTL	VALUE
@	SOA	3600	Email: azuredns-hostmaster.microsoft.com Host: internal.cloudapp.net Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 300 Serial number: 1
vm1	A	3600	10.1.0.4
vm9	A	3600	10.1.0.12

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements

Yes

No

The A record for VM5 will be registered automatically in the adatum.com zone.

VM5 can resolve VM9.adatum.com.

VM6 can resolve VM9.adatum.com.

Answer:

Answer Area

Statements	Yes	No
The A record for VM5 will be registered automatically in the adatum.com zone.	<input type="radio"/>	<input checked="" type="radio"/>
VM5 can resolve VM9.adatum.com.	<input type="radio"/>	<input checked="" type="radio"/>
VM6 can resolve VM9.adatum.com.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Box 1: No -

Azure DNS provides automatic registration of virtual machines from a single virtual network that's linked to a private zone as a registration virtual network. VM5 does not belong to the registration virtual network though.

Box 2: No -

Forward DNS resolution is supported across virtual networks that are linked to the private zone as resolution virtual networks. VM5 does belong to a resolution virtual network.

Box 3: Yes -

VM6 belongs to registration virtual network, and an A (Host) record exists for VM9 in the DNS zone.

By default, registration virtual networks also act as resolution virtual networks, in the sense that DNS resolution against the zone works from any of the virtual machines within the registration virtual network.

Reference:

<https://docs.microsoft.com/en-us/azure/dns/private-dns-overview>

Question: 445

CertyIQ

HOTSPOT -

You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Location
VNET1	West US
VNET2	West US
VNET3	East US

The subscription contains the private DNS zones shown in the following table.

Name	Location
Zone1.com	West US
Zone2.com	West US
Zone3.com	East US

You add virtual network links to the private DNS zones as shown in the following table.

Name	Private DNS zone	Virtual network	Enable auto registration
Link1	Zone1.com	VNET1	Yes
Link2	Zone2.com	VNET2	No
Link3	Zone3.com	VNET3	No

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
You can enable auto registration for Link2.	<input type="radio"/>	<input type="radio"/>
You can add a virtual network link for VNET1 to Zone3.com.	<input type="radio"/>	<input type="radio"/>
You can add a virtual network link for VNET2 to Zone1.com and enable auto registration.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
You can enable auto registration for Link2.	<input checked="" type="radio"/>	<input type="radio"/>
You can add a virtual network link for VNET1 to Zone3.com.	<input checked="" type="radio"/>	<input type="radio"/>
You can add a virtual network link for VNET2 to Zone1.com and enable auto registration.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

<https://docs.microsoft.com/en-us/azure/dns/private-dns-virtual-network-links>

A virtual network can be linked to private DNS zone as a registration or as a resolution virtual network.

Registration virtual network:

A private DNS zone can have multiple registration virtual networks. However, every virtual network can only have one registration zone associated with it.

Resolution virtual network:

One private DNS zone can have multiple resolution virtual networks and a virtual network can have multiple

resolution zones associated to it.

1. Yes

No registration zone for VNET2.

2. Yes

A virtual network can have multiple resolution zones associated to it.

3. Yes

No registration zone for VNET2.

Reference:

<https://docs.microsoft.com/en-us/azure/dns/private-dns-virtual-network-links> <https://docs.microsoft.com/en-us/azure/dns/private-dns-autoregistration>

Question: 446

CertyIQ

HOTSPOT -

You have an Azure subscription.

You plan to use an Azure Resource Manager template to deploy a virtual network named VNET1 that will use Azure Bastion.

How should you complete the template? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
{  
  "type": "Microsoft.Network/virtualNetworks",  
  "name": "VNET1"  
  "apiVersion": "2019-02-01",  
  "location": "[resourceGroup().location]",  
  "properties": {  
    "addressSpace": {  
      "addressPrefixes": ["10.10.10.0/24"]  
    },  
    "subnets": [  
      {  
        "name": "AzureBastionSubnet"  
        "properties": {  
          "addressPrefix": "10.10.10.0/27"  
        }  
      },  
      {  
        "name": "AzureFirewallSubnet"  
        "properties": {  
          "addressPrefix": "10.10.10.0/29"  
        }  
      },  
      {  
        "name": "LAN01"  
        "properties": {  
          "addressPrefix": "10.10.10.0/30"  
        }  
      },  
      {  
        "name": "RemoteAccessSubnet"  
        "properties": {  
          "addressPrefix": "10.10.10.0/30"  
        }  
      }  
    ]  
  }  
}
```

Answer:

Answer Area

```
{  
  "type": "Microsoft.Network/virtualNetworks",  
  "name": "VNET1",  
  "apiVersion": "2019-02-01",  
  "location": "[resourceGroup().location]",  
  "properties": {  
    "addressSpace": {  
      "addressPrefixes": ["10.10.10.0/24"]  
    },  
    "subnets": [  
      {  
        "name": "AzureBastionSubnet",  
        "AzureFirewallSubnet",  
        "LAN01",  
        "RemoteAccessSubnet"  
      },  
      {"  
        "properties": {  
          "addressPrefix": "10.10.10.0/27",  
          "10.10.10.0/29",  
          "10.10.10.0/30"  
        }  
      },  
      {  
        "name": "LAN02",  
        "properties": {  
          "addressPrefix": "10.10.10.128/25"  
        }  
      }  
    ]  
  }  
}
```

Explanation:

1. AzureBastionSubnet

2. 10.10.10.0/27

<https://learn.microsoft.com/en-us/azure/bastion/configuration-settings#subnet>

Azure Bastion requires a dedicated subnet: AzureBastionSubnet. You must create this subnet in the same virtual network that you want to deploy Azure Bastion to.

For Azure Bastion resources deployed on or after November 2, 2021, the minimum AzureBastionSubnet size is /26 or larger (/25, /24, etc.). All Azure Bastion resources deployed in subnets of size /27 prior to this date are unaffected by this change and will continue to work, but we highly recommend increasing the size of any existing AzureBastionSubnet to /26 in case you choose to take advantage of host scaling in the future.

Reference:

<https://medium.com/charot/deploy-azure-bastion-preview-using-an-arm-template-15e3010767d6>

Question: 447

CertyIQ

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 manage a virtual network named VNet1 that is hosted in the West US Azure region.

VNet1 hosts two virtual machines named VM1 and VM2 that run Windows Server.

You need to inspect all the network traffic from VM1 to VM2 for a period of three hours.

Solution: From Azure Network Watcher, you create a packet capture.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

Network Watcher variable packet capture allows you to create packet capture sessions to track traffic to and from a virtual machine. Packet capture helps to diagnose network anomalies both reactively and proactively.

Other uses include gathering network statistics, gaining information on network intrusions, to debug client-server communications and much more.

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-packet-capture-overview>

Question: 448

CertyIQ

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 manage a virtual network named VNet1 that is hosted in the West US Azure region.

VNet1 hosts two virtual machines named VM1 and VM2 that run Windows Server.

You need to inspect all the network traffic from VM1 to VM2 for a period of three hours.

Solution: From Azure Network Watcher, you create a connection monitor.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

No.

We need to inspect all the network traffic "from" VM1 "to" VM2 and not between the 2 VMs.

Even if we were using Connection monitor, this one would inspect only network traffic over a specific port.

And for a period of 3 hours, packet capture session time limit default value is 18000 seconds or 5 hours.

CertyIQ

Question: 449

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 manage a virtual network named VNet1 that is hosted in the West US Azure region.

VNet1 hosts two virtual machines named VM1 and VM2 that run Windows Server.

You need to inspect all the network traffic from VM1 to VM2 for a period of three hours.

Solution: From Performance Monitor, you create a Data Collector Set (DCS).

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Use the Connection Monitor feature of Azure Network Watcher.

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview>

CertyIQ

Question: 450

DRAG DROP -

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

Name	Type	Description
vm1	Virtual machine	Uses a basic public IP address
vm2	Virtual machine	Uses a basic public IP address
nsg1	Network security group (NSG)	Allows incoming traffic from port 443
lb1	Azure Standard Load Balancer	Not applicable

You need to load balance HTTPS connections to vm1 and vm2 by using lb1.

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

- Remove nsg1.
- Remove the public IP addresses from vm1 and vm2.
- Create a health probe and backend pool on lb1.
- Create an availability set.
- Create a load balancing rule on lb1.

Answer Area



Answer:

Actions

- Remove nsg1.
-
-
- Create an availability set.
-

Answer Area

- Remove the public IP addresses from vm1 and vm2.
- Create a health probe and backend pool on lb1.
- Create a load balancing rule on lb1.



Explanation:

1. Remove the public IP addresses from VM1 and VM2

When using an internal load balancer, backend VMs should not have public IPs. Removing public IPs ensures that all inbound traffic is routed through the load balancer.

2. Create a health probe and backend pool on lb1

A health probe is required to monitor the availability of backend VMs.

A backend pool groups the VMs that will receive traffic from the load balancer.

3.Create a load balancing rule on lb1

A load balancing rule defines how traffic is distributed across the backend VMs (e.g., specifying ports and protocols).

Reference:

<https://docs.microsoft.com/en-us/azure/load-balancer/tutorial-load-balancer-standard-public-zone-redundant-portal>

CertyIQ

Question: 451

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 manage a virtual network named VNet1 that is hosted in the West US Azure region.

VNet1 hosts two virtual machines named VM1 and VM2 that run Windows Server.

You need to inspect all the network traffic from VM1 to VM2 for a period of three hours.

Solution: From Azure Monitor, you create a metric on Network In and Network Out.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

You use the Packet Capture, not Connection Monitor nor Network watcher.

Reference:

<https://azure.microsoft.com/en-us/updates/general-availability-azure-network-watcher-connection-monitor-in-all-public-regions/>

CertyIQ

Question: 452

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 app named App1 that is installed on two Azure virtual machines named VM1 and VM2. Connections to App1 are managed by using an Azure Load Balancer.

The effective network security configurations for VM2 are shown in the following exhibit.

VM2 - Networking

Virtual machine

Network Interface: VM2-NIC1 [Effective security rules](#) [Topology](#)

Virtual network/subnet: Vnet1/Subnet11 NIC Public IP: - NIC Private IP: 10.240.11.5 Accelerated networking: Disabled

Inbound port rules Outbound port rules Application security groups Load balancing

Network security group NSG2 (attached to network interface: Subnet11)
Impacts 1 subnets, 0 network interfaces [Add inbound port rule](#)

Priority	Name	Port	Protocol	Source	Destination	Action	...
100	Allow_131.107.100.50	443	TCP	131.107.100.50	VirtualNetwork	Allow	...
200	BlockAllOther441	443	Any	Any	Any	Deny	...
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	...
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow	...
65500	DenyAllInBound	Any	Any	Any	Any	Deny	...

You discover that connections to App1 from 131.107.100.50 over TCP port 443 fail.

You verify that the Load Balancer rules are configured correctly.

You need to ensure that connections to App1 can be established successfully from 131.107.100.50 over TCP port 443.

Solution: You create an inbound security rule that denies all traffic from the 131.107.100.50 source and has a priority of 64999.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

B (No)

When an Azure Load Balancer get created, it will probe backend to detect if the backend service is healthy or not, the probe packet is sent from source address "AzureLoadBalancer", the IP address of "AzureLoadBalancer" is always 168.63.129.16.

<https://msazure.club/addendum-of-azure-load-balancer-and-nsg-rules/>

What is happening here is the LB Health Probe of TCP 443 to VM1 & VM2 are getting blocked by Rule 200 so it thinks both VM1 and VM2 are down. Hence App1 is failing as the LB won't direct any 443 traffic anywhere as it considers all Hosts are down.

Make a new rule above 200 or move rule 65001 up to <200, so the Health Probe will start working again, it will find a health host and start to direct 443 traffic from 131.107.100.50 to it.

Reference:

<https://fastreroute.com/azure-network-security-groups-explained/>

Question: 453

CertyIQ

DRAG DROP -

You have an Azure subscription that contains two on-premises locations named site1 and site2.

You need to connect site1 and site2 by using an Azure Virtual WAN.

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

- Create a virtual hub.
- Create VPN sites.
- Connect the virtual networks to the hub.
- Create a Virtual WAN resource.
- Connect the VPN sites to the hub.

Answer Area

Answer:

Actions

-
-
- Connect the virtual networks to the hub.
-
-

Answer Area

- Create a Virtual WAN resource.
- Create a virtual hub.
- Create VPN sites.
- Connect the VPN sites to the hub.

Explanation:

Create a Virtual WAN resource.

This is the first step in setting up Azure Virtual WAN, which acts as a centralized networking service for connectivity.

Create a virtual hub.

A Virtual Hub is required within Virtual WAN to facilitate connections between VPNs, ExpressRoute, and Virtual Networks.

Create VPN sites.

In Azure Virtual WAN, VPN sites represent on-premises locations that connect to Azure via Site-to-Site VPN.

Connect the VPN sites to the hub.

Once VPN sites are created, they need to be connected to the Virtual Hub to enable communication between on-premises networks and Azure.

Question: 454

CertyIQ

HOTSPOT -

You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Peered with	DNS server
VNET1	VNET2	Default (Azure-provided)
VNET2	VNET1	10.10.0.4

You have the virtual machines shown in the following table.

Name	IP address	Network interface	Connects to
Server1	10.10.0.4	NIC1	VNET1/Subnet1
Server2	172.16.0.4	NIC2	VNET1/Subnet2
Server3	192.168.0.4	NIC3	VNET2/Subnet2

You have the virtual network interfaces shown in the following table.

Name	DNS server
NIC1	Inherit from virtual network
NIC2	10.10.0.4
NIC3	Inherit from virtual network

Server1 is a DNS server that contains the resources shown in the following table.

Name	Type	Value
contoso.com	Primary DNS zone	Not applicable
Host1.contoso.com	A record	131.107.10.15

You have an Azure private DNS zone named contoso.com that has a virtual network link to VNET2 and the records shown in the following table.

Name	Type	Value
Host1	A record	131.107.200.20
Host2	A record	131.107.50.50

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements

Yes No

Server2 resolves host2.contoso.com to 131.107.50.50.

Server2 resolves host1.contoso.com to 131.107.10.15.

Server3 resolves host2.contoso.com to 131.107.50.50.

Answer:

Answer Area

Statements

Yes No

Server2 resolves host2.contoso.com to 131.107.50.50.

Server2 resolves host1.contoso.com to 131.107.10.15.

Server3 resolves host2.contoso.com to 131.107.50.50.

Explanation:

No: Server2 uses Server1 for DNS. Server1 has no host2.contoso.com record for 131.107.50.50. It would work if VNET1 had a virtual network link to the private zone contoso.com.

Yes: Server2 uses Server1 for DNS. Server1 has a host1.contoso.com record for 131.107.10.15

No: Server3 uses 10.10.0.4 as DNS (inherited from VNET2). 10.10.0.4 (Server1) has no record for host2.contoso.com. The virtual network link for the private zone contoso.com on VNET2 won't be used since the DNS from VNET1 is set on VNET2. VNET1 DNS is not aware of the private zone contoso.com. It would work if VNET1 had a virtual network link to the private zone contoso.com.

Key: Server1 considers itself authoritative for contoso.com (its a Primary DNS zone)

If it doesn't have a record, that's game over man

Server2 gets a DNS server of Server 1 (NIC2 is hard set to Server1's IP)

Server2 can not resolve host2.contoso.com as Server1 has no record for it

Server2 resolves host1.contoso.com as 131.107.10.15 as that's Server1's record for it

Server3 (NIC3) inherits from its VNET (VNET2) which is also Server1

Server3 resolves host2.contoso.com the same as Server2 with NO resolution

Question: 455

CertyIQ

You have a virtual network named VNet1 as shown in the exhibit. (Click the Exhibit tab.)



Move



Delete

Resource group ([change](#))

Production

Address space

10.2.0.0/16

Location

West US

DNS servers

Azure provided DNS service

Subscription ([change](#))

Production subscription

Subscription ID

14d26092-8e42-4ea7-b770-9dcef70fb1ea

Tags ([change](#))[Click here to add tags](#)

Connected devices



Search connected devices

DEVICE

TYPE

IP ADDRESS

SUBNET

No results.

No devices are connected to VNet1.

You plan to peer VNet1 to another virtual network named VNet2. VNet2 has an address space of 10.2.0.0/16.

You need to create the peering.

What should you do first?

- A. Modify the address space of VNet1.
- B. Add a gateway subnet to VNet1.
- C. Create a subnet on VNet1 and VNet2.
- D. Configure a service endpoint on VNet2.

Answer: A**Explanation:**

The virtual networks you peer must have non-overlapping IP address spaces. The exhibit indicates that VNet1 has an address space of 10.2.0.0/16, which is the same as VNet2, and thus overlaps. We need to change the address space for VNet1.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering#requirements-and-constraints> <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-faq>

Question: 456**CertyIQ**

You have the Azure virtual machines shown in the following table.

Name	IP address	Virtual network
VM1	10.0.0.4	VNET1
VM2	10.0.0.5	VNET1

VNET1 is linked to a private DNS zone named contoso.com that contains the records shown in the following table.

Name	Type	TTL	Value	Auto registered
comp1	TXT	3600	10.0.0.5	False
comp2	A	3600	10.0.0.5	False
comp3	CNAME	3600	comp1.contoso.com	False
comp4	PTR	3600	10.0.0.5	False

You need to ping VM2 from VM1.

Which DNS names can you use to ping VM2?

- A. comp2.contoso.com and comp4.contoso.com only
- B. comp1.contoso.com, comp2.contoso.com, comp3.contoso.com, and comp4.contoso.com
- C. comp2.contoso.com only
- D. comp1.contoso.com and comp2.contoso.com only
- E. comp1.contoso.com, comp2.contoso.com, and comp4.contoso.com only

Answer: C

Explanation:

comp2.contoso.com only

A record: Is used to map a DNS/domain name to an IP

TXT records in a lot of cases get used to prove ownership of a domain, it has other purposes too.

PTR: A Reverse DNS lookup is used by remote hosts to determine who 'owns' an IP address.

CNAME records get used to redirect a DNS name or subdomain name to another DNS name or domain name or subdomain name.

It would do good to read up on DNS record types and what they are used for, you will be lost if you don't have a basic understanding of it.

DNS is a key component in the IT field.

reference:

<https://support.dnsimple.com/articles/cname-record/>

<https://ns1.com/resources/dns-types-records-servers-and-queries>

<https://www.mailenable.com/kb/content/article.asp?ID=ME020206>

<https://support.google.com/a/answer/2716800?hl=en#:~:text=txt%20records%20are%20a%20type, and%20to%20ensure%20email%20security.>

<https://www.cloudflare.com/learning/dns/dns-records/dns-a-record/>

Question: 457

HOTSPOT -

You have a network security group (NSG) named NSG1 that has the rules defined in the exhibit. (Click the Exhibit tab.)

```
PS C:\> Get-AzNetworkSecurityGroup -Name "NSG1" -ResourceGroupName "RG1" | Select -ExpandProperty SecurityRules

Name          : ALLOW_HTTPS
Id            : /subscriptions/09d06b22-ff51-48b7-a8be-947f15cbd69d/resourceGroups/RG1/providers/Microsoft.Network/networkSecurityGroups/NSG1/securityRules/ALLOW_HTTPS
Etag          : W/"8e3e9995-aa78-41e2-bfea-44b50c389873"
ProvisioningState : Succeeded
Description    :
Protocol      : TCP
SourcePortRange : {*}
DestinationPortRange : {443}
SourceAddressPrefix   : {*}
DestinationAddressPrefix : {*}
SourceApplicationSecurityGroups : []
DestinationApplicationSecurityGroups : []
Access         : Allow
Priority       : 100
Direction      : Inbound

Name          : DENY_PING
Id            : /subscriptions/09d06b22-ff51-48b7-a8be-947f15cbd69d/resourceGroups/RG1/providers/Microsoft.Network/networkSecurityGroups/NSG1/securityRules/DENY_PING
Etag          : W/"8e3e9995-aa78-41e2-bfea-44b50c389873"
ProvisioningState : Succeeded
Description    :
Protocol      : ICMP
SourcePortRange : {*}
DestinationPortRange : {*}
SourceAddressPrefix   : {VirtualNetwork}
DestinationAddressPrefix : {*}
SourceApplicationSecurityGroups : []
DestinationApplicationSecurityGroups : []
Access         : Deny
Priority       : 111
Direction      : Outbound
```

NSG1 is associated to a subnet named Subnet1. Subnet1 contains the virtual machines shown in the following table.

Name	IP address
VM1	10.1.0.10
VM2	10.1.0.11

You need to add a rule to NSG1 to ensure that VM1 can ping VM2. The solution must use the principle of least privilege.

How should you configure the rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Direction:

Inbound
Outbound

Source:

Any
10.1.0.10
10.1.0.11
10.1.0.10; 10.1.0.11
10.1.0.0/28

Destination:

Any
10.1.0.10
10.1.0.11
10.1.0.10; 10.1.0.11
10.1.0.0/28

Priority:

110
111
112

Answer:

Answer Area

Direction:

Inbound
Outbound

Source:

Any
10.1.0.10
10.1.0.11
10.1.0.10; 10.1.0.11
10.1.0.0/28

Destination:

Any
10.1.0.10
10.1.0.11
10.1.0.10; 10.1.0.11
10.1.0.0/28

Priority:

110
111
112

Explanation:

Direction: Outbound

Source 10.1.0.10 (VM1)

Destination: 10.1.0.11 (VM2)

Priority: 110

Please note that the rule won't block outbound response from VM2.

NSGs allow or deny the establishment of a TCP connection. Once a connection is established, traffic can flow both ways as needed without obstruction. NSGs will not end active TCP connections either.

Reference:

<https://www.thomasmaurer.ch/2019/09/how-to-enable-ping-icmp-echo-on-an-azure-vm/>

Question: 458

CertyIQ

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 a computer named Computer1 that has a point-to-site VPN connection to an Azure virtual network named VNet1. The point-to-site connection uses a self-signed certificate.

From Azure, you download and install the VPN client configuration package on a computer named Computer2.

You need to ensure that you can establish a point-to-site VPN connection to VNet1 from Computer2.

Solution: On Computer2, you set the Startup type for the IPSec Policy Agent service to Automatic.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Each client computer that connects to a VNet using Point-to-Site must have a client certificate installed. You generate a client certificate from the self-signed root certificate, and then export and install the client certificate. If the client certificate is not installed, authentication fails.

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-certificates-point-to-site>

Question: 459

CertyIQ

You have five Azure virtual machines that run Windows Server 2016. The virtual machines are configured as web servers.

You have an Azure load balancer named LB1 that provides load balancing services for the virtual machines.

You need to ensure that visitors are serviced by the same web server for each request.

What should you configure?

- A. Session persistence to Client IP and protocol
- B. Protocol to UDP
- C. Session persistence to None
- D. Floating IP (direct server return) to Enabled

Answer: A

Explanation:

None (hash-based) - Specifies that successive requests from the same client may be handled by any virtual machine.

Client IP (source IP affinity two-tuple) - Specifies that successive requests from the same client IP address will be handled by the same virtual machine.

Client IP and protocol (source IP affinity three-tuple) - Specifies that successive requests from the same client IP address and protocol combination will be handled by the same virtual machine.

Reference:

<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-distribution-mode?tabs=azure-portal>

Question: 460

You have an Azure subscription that uses the public IP addresses shown in the following table.

Name	IP version	SKU	IP address assignment	Availability zone
IP1	IPv6	Basic	Static	Not applicable
IP2	IPv6	Basic	Dynamic	Not applicable
IP3	IPv6	Standard	Static	Zone-redundant

You need to create a public Azure Standard Load Balancer.

Which public IP addresses can you use?

- A. IP1, IP2, and IP3
- B. IP2 only
- C. IP3 only
- D. IP1 and IP3 only

Answer: C

Explanation:

Matching SKUs are required for load balancer and public IP resources. You can't have a mixture of Basic SKU resources and standard SKU resources.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-addresses>

Question: 461

You have an Azure subscription.

You are deploying an Azure Kubernetes Service (AKS) cluster that will contain multiple pods. The pods will use kubernetes networking.

You need to restrict network traffic between the pods.

What should you configure on the AKS cluster?

- A. the Azure network policy
- B. the Calico network policy
- C. pod security policies
- D. an application security group

Answer: B

Explanation:

The question describes “the pods will use kubernetes networking.”

To provide network connectivity, AKS clusters can use kubernetes (basic networking) or Azure CNI (advanced

networking).

Azure Network Policies supports Azure CNI only. Calico Network Policies supports both Azure CNI (Windows Server 2019 and Linux) and kubenet (Linux).

Reference

<https://docs.microsoft.com/en-us/azure/aks/use-network-policies>

<https://docs.microsoft.com/en-us/azure/aks/configure-kubenet>

Reference:

<https://docs.microsoft.com/en-us/azure/aks/use-network-policies>

CertyIQ

Question: 462

HOTSPOT -

You have an Azure subscription that contains a virtual network named VNet1. VNet1 uses an IP address space of 10.0.0.0/16 and contains the VPN Gateway and subnets in the following table:

Name	IP address range
Subnet0	10.0.0.0/24
Subnet1	10.0.1.0/24
Subnet2	10.0.2.0/24
GatewaySubnet	10.0.254.0/24

Subnet1 contains a virtual appliance named VM1 that operates as a router.

You create a routing table named RT1.

You need to route all inbound traffic from the VPN gateway to VNet1 through VM1.

How should you configure RT1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Address prefix

10.0.0.0/16
10.0.1.0/24
10.0.254.0/24

Next hop type

Virtual appliance
Virtual network
Virtual network gateway

Assigned to

GatewaySubnet
Subnet0
Subnet1 and Subnet2

Answer:

Answer Area

Address prefix

10.0.0.0/16
10.0.1.0/24
10.0.254.0/24

Next hop type

Virtual appliance
Virtual network
Virtual network gateway

Assigned to

GatewaySubnet
Subnet0
Subnet1 and Subnet2

Explanation:

Box 1: 10.0.0.0/16

Address prefix

destination-> Vnet 1 (Address space of Vnet1)

Box 2: Virtual appliance

Next hop type

VM1 ->Virtual Appliance. You can specify IP address of VM 1 when configuring next hop as Virtual appliance.

Box 3: Gateway Subnet

Assigned to

This route is to be followed by Gateway Subnet for the incoming traffic. You can associate routing table to the Subnet from Rout Table -> subnet ->Associate.

Question: 463

CertyIQ

You have five Azure virtual machines that run Windows Server 2016. The virtual machines are configured as web servers.

You have an Azure load balancer named LB1 that provides load balancing services for the virtual machines.

You need to ensure that visitors are serviced by the same web server for each request.

What should you configure?

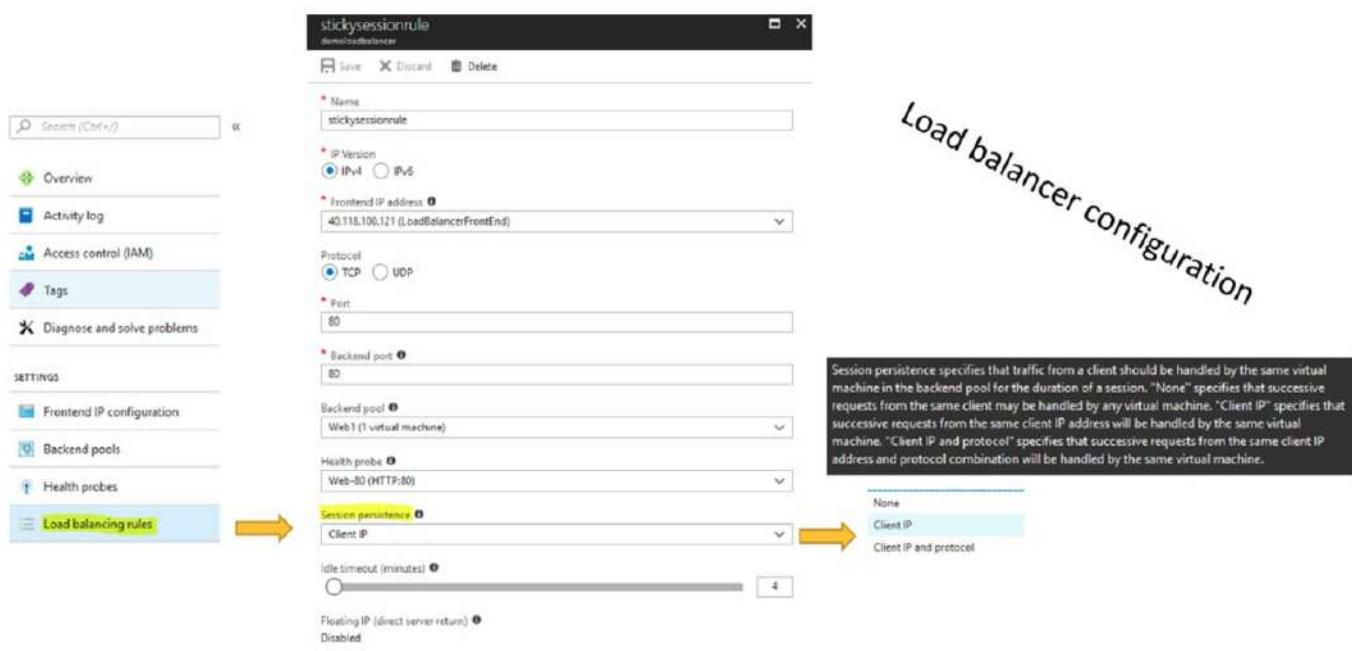
- A. Floating IP (direct server return) to Enabled
- B. Floating IP (direct server return) to Disabled
- C. a health probe
- D. Session persistence to Client IP and Protocol

Answer: D

Explanation:

With Sticky Sessions when a client starts a session on one of your web servers, session stays on that specific server. To configure An Azure Load-Balancer For Sticky Sessions set Session persistence to Client IP.

On the following image you can see sticky session configuration:



Note:

There are several versions of this question in the exam. The question can have other incorrect answer options, including the following:

1. Idle Time-out (minutes) to 20
2. Protocol to UDP

Reference:

<https://cloudopszone.com/configure-azure-load-balancer-for-sticky-sessions/>

Question: 464

CertyIQ

HOTSPOT -

You have an Azure subscription that contains the virtual machines shown in the following table:

Name	Operating system	Connects to
VM1	Windows Server 2019	Subnet1
VM2	Windows Server 2019	Subnet2

VM1 and VM2 use public IP addresses. From Windows Server 2019 on VM1 and VM2, you allow inbound Remote Desktop connections.

Subnet1 and Subnet2 are in a virtual network named VNET1.

The subscription contains two network security groups (NSGs) named NSG1 and NSG2. NSG1 uses only the default rules.

NSG2 uses the default rules and the following custom incoming rule:

⇒ Priority: 100

- ⇒ Name: Rule1
- ⇒ Port: 3389
- ⇒ Protocol: TCP
- ⇒ Source: Any
- ⇒ Destination: Any
- ⇒ Action: Allow

NSG1 is associated to Subnet1. NSG2 is associated to the network interface of VM2.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
From the Internet, you can connect to VM1 by using Remote Desktop.	<input type="radio"/>	<input type="radio"/>
From the Internet, you can connect to VM2 by using Remote Desktop.	<input type="radio"/>	<input type="radio"/>
From VM1, you can connect to VM2 by using Remote Desktop	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
From the Internet, you can connect to VM1 by using Remote Desktop.	<input type="radio"/>	<input checked="" type="radio"/>
From the Internet, you can connect to VM2 by using Remote Desktop.	<input checked="" type="radio"/>	<input type="radio"/>
From VM1, you can connect to VM2 by using Remote Desktop	<input type="radio"/>	<input type="radio"/>

Explanation:

No: VM1 has default rules which denies any port open for inbound rules

Yes: VM2 has custom rule allowing RDP port

Yes: VM1 and VM2 are in the same Vnet. by default, communication are allowed

Question: 465

CertyIQ

You have an Azure subscription that contains two virtual machines named VM1 and VM2.

You create an Azure load balancer.

You plan to create a load balancing rule that will load balance HTTPS traffic between VM1 and VM2.

Which two additional load balancer resources should you create before you can create the load balancing rule?

Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. a frontend IP address

- B. an inbound NAT rule
- C. a virtual network
- D. a backend pool
- E. a health probe

Answer: DE

Explanation:

You can't create a LB without FrontEnd IP, so if we have a LB we also have a FrontEnd IP already. You can however create a LB without a backend pool and without any rules. If you want to add a rule to your LB later you have to create a backend pool and health probe first. Those are mandatory properties for a rule. I also tested it in my lab to be sure.

Reference:

<https://docs.microsoft.com/en-us/azure/load-balancer/components>

CertyIQ

Question: 466

You have an on-premises network that contains a database server named dbserver1.

You have an Azure subscription.

You plan to deploy three Azure virtual machines. Each virtual machine will be deployed to a separate availability zone.

You need to configure an Azure VPN gateway for a site-to-site VPN. The solution must ensure that the virtual machines can connect to dbserver1.

Which type of public IP address SKU and assignment should you use for the gateway?

- A. a basic SKU and a static IP address assignment
- B. a standard SKU and a static IP address assignment
- C. a basic SKU and a dynamic IP address assignment

Answer: B

Explanation:

since the VMs are in AZ then VPN gateway will have to be in AZ which will rely on Azure public IP resource Standard SKU. And must be Static as Dynamic is only for non-AZ. See links below.

<https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-addresses#at-a-glance>

<https://learn.microsoft.com/en-us/azure/vpn-gateway/about-zone-redundant-vnet-gateways>

CertyIQ

Question: 467

HOTSPOT -

You have the Azure virtual machines shown in the following table.

Name	IP address	Virtual network
VM1	10.0.0.4	VNET1
VM2	172.16.0.4	VNET2
VM3	192.168.0.4	VNET3
VM4	192.168.0.5	VNET3

VNET1, VNET2, and VNET3 are peered.

Name	Type	Value
Server1	A	131.107.2.3
Server2	A	131.107.2.4

VNET1 and VNET2 are linked to an Azure private DNS zone named contoso.com that contains the records shown in the following table.

Name	Type	Value
Server1	A	131.107.3.3
Server2	A	131.107.3.4

The virtual networks are configured to use the DNS servers shown in the following table.

Virtual network	DNS server
VNET1	Default (Azure-provided)
VNET2	Custom: 192.168.0.5
VNET3	Custom: 192.168.0.5

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Statements

From VM1, server1.contoso.com resolves to 131.107.3.3.

From VM2, server1.contoso.com resolves to 131.107.3.3.

From VM3, server2.contoso.com resolves to 131.107.2.4.

Answer:

Statements	Yes	No
From VM1, server1.contoso.com resolves to 131.107.3.3.	<input checked="" type="radio"/>	<input type="radio"/>
From VM2, server1.contoso.com resolves to 131.107.3.3.	<input type="radio"/>	<input checked="" type="radio"/>
From VM3, server2.contoso.com resolves to 131.107.2.4.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Box 1: Yes -

VM1 is in VNET1. In VNET1 Server1 resolves to 131.107.3.3

Name	Type	Value
Server1	A	131.107.3.3
Server2	A	131.107.3.4

Box 2: No -

VM2 is in VNET2. VNET2 uses custom DNS server 192.168.05

Box 3: Yes.

Question: 468

CertyIQ

HOTSPOT -

You have two Azure virtual machines as shown in the following table.

Name	Operating system	Private IP address	Public IP address	DNS suffix configured in the operating system	Connected to
vm1	Windows Server 2019	10.0.1.4	131.107.50.20	Contoso.com	vnet1
vm2	SUSE Linux Enterprise Server 15 (SLES) SP2	10.0.1.5	131.107.90.80	None	vnet1

You create the Azure DNS zones shown in the following table.

Name	Type
Contoso.com	DNS zone
Fabrikam.com	Private DNS zone

You perform the following actions:

- ⇒ In fabrikam.com, you add a virtual network link to vnet1 and enable auto registration.

⇒ For contoso.com, you assign vm1 and vm2 the Owner role.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Statements	Yes	No
The DNS A record for vm1 is added to contoso.com and has the IP address of 131.107.50.20.	<input type="radio"/>	<input type="radio"/>
The DNS A record for vm1 is added to fabrikam.com and has the IP address of 10.0.1.4.	<input type="radio"/>	<input type="radio"/>
The DNS A record for vm2 is added to fabrikam.com and has the IP address of 10.0.1.5.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
The DNS A record for vm1 is added to contoso.com and has the IP address of 131.107.50.20.	<input type="radio"/>	<input checked="" type="radio"/>
The DNS A record for vm1 is added to fabrikam.com and has the IP address of 10.0.1.4.	<input checked="" type="radio"/>	<input type="radio"/>
The DNS A record for vm2 is added to fabrikam.com and has the IP address of 10.0.1.5.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Box 1: No

None of the actions in question added the VM1 record to contoso.com dns

Box 2: Yes -

Fabrikam.com is a Private DNS zone. The private IP address is used.

Note: The Azure DNS private zones auto registration feature manages DNS records for virtual machines deployed in a virtual network. When you link a virtual network with a private DNS zone with this setting enabled, a DNS record gets created for each virtual machine deployed in the virtual network.

For each virtual machine, an A record and a PTR record are created. DNS records for newly deployed virtual machines are also automatically created in the linked private DNS zone.

Note: If you use Azure Provided DNS then appropriate DNS suffix will be automatically applied to your virtual machines. For all other options you must either use

Fully Qualified Domain Names (FQDN) or manually apply appropriate DNS suffix to your virtual machines.

Box 3: Yes -

N - Public Ips wont auto register DNS

Y - Auto registration is enabled

N - Linux won't do auto registration

Reference:

<https://docs.microsoft.com/en-us/azure/dns/dns-zones-records>

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-name-resolution-for-vms-and-role-instances>

Question: 469

CertyIQ

You have an on-premises datacenter and an Azure subscription.

You plan to connect the datacenter to Azure by using ExpressRoute.

You need to deploy an ExpressRoute gateway. The solution must meet the following requirements:

- ⇒ Support up to 10 Gbps of traffic.
- ⇒ Support availability zones.
- ⇒ Support FastPath.
- ⇒ Minimize costs.

Which SKU should you deploy?

- A. ERGw1AZ
- B. ERGw2
- C. ErGw3
- D. ErGw3AZ

Answer: D

Explanation:

ErGw3Az supports FastPath.

The following table shows the features supported across each gateway type.

Gateway SKU	VPN Gateway and ExpressRoute coexistence	FastPath	Max Number of Circuit Connections
Standard SKU/ERGw1Az	Yes	No	4
High Perf SKU/ERGw2Az	Yes	No	8
Ultra Performance SKU/ErGw3Az	Yes	Yes	16

Note: ExpressRoute virtual network gateways can use the following SKUs:

Standard -

HighPerformance -

UltraPerformance -

ErGw1Az -

ErGw2Az -

ErGw3Az -

Reference:

<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-about-virtual-network-gateways>

Question: 470

CertyIQ

HOTSPOT -

You have a virtual network named VNET1 that contains the subnets shown in the following table:

Name	Subnet	Network security group (NSG)
Subnet1	10.10.1.0/24	NSG1
Subnet2	10.10.2.0/24	<i>None</i>

You have Azure virtual machines that have the network configurations shown in the following table:

Name	Subnet	IP address	NSG
VM1	Subnet1	10.10.1.5	NSG2
VM2	Subnet2	10.10.2.5	<i>None</i>
VM3	Subnet2	10.10.2.6	<i>None</i>

For NSG1, you create the inbound security rule shown in the following table:

Priority	Source	Destination	Destination port	Action
101	10.10.2.0/24	10.10.1.0/24	TCP/1433	Allow

For NSG2, you create the inbound security rule shown in the following table:

Priority	Source	Destination	Destination port	Action
125	10.10.2.5	10.10.1.5	TCP/1433	Block

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements

Yes

No

VM2 can connect to the TCP port 1433 services on VM1.

VM1 can connect to the TCP port 1433 services on VM2.

VM2 can connect to the TCP port 1433 services on VM3.

Answer:

Answer Area

Statements	Yes	No
VM2 can connect to the TCP port 1433 services on VM1.	<input type="radio"/>	<input checked="" type="radio"/>
VM1 can connect to the TCP port 1433 services on VM2.	<input checked="" type="radio"/>	<input type="radio"/>
VM2 can connect to the TCP port 1433 services on VM3.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Box 1: NO - here is why "Remember this- The rule closest to destination take precedence over other rules" i.e. if subnet allows for TCP traffic to flow on port 1433 but the

NSG denies access/blocks access and is applied to Network interface of VM1 and lets say VM2 tries to access VM1 @ port 1433 then NSG1 applied at subnet level will allow traffic to flow but access will Definitely be denied at NIC level and hence VM2 gets blocked. Remember what i said earlier the NSG rule nearest to destination take precedence and Deny takes precedence over allow assuming the NSG rule has Higher priority (meaning will be applied first). Important Note if you have NSG1 rule with priority 100 (allows RDP traffic 3389) and NSG2 rule with priority 110 (Deny RDP traffic 3389) and both are applied at same level i.e. SUBNET or NIC (If applied at NIC level assume subnet level is allow for example sake) then the NSG1 rule will take precedence and traffic is allowed and Rule NSG2 is NEVER checked - basically has no value

Box 2: Yes -

No rule explicitly blocks communication from VM1. The default rules, which allow communication, are thus applied.

Box 3: Yes -

No rule explicitly blocks communication between VM2 and VM3 which are both on Subnet2. The default rules, which allow communication, are thus applied.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/security-overview>

Question: 471

CertyIQ

HOTSPOT -

You have an Azure subscription named Subscription1.

Subscription1 contains the virtual machines in the following table:

Name	IP address
VM1	10.0.1.4
VM2	10.0.2.4
VM3	10.0.3.4

Subscription1 contains a virtual network named VNet1 that has the subnets in the following table:

Name	Address space	Connected virtual machine
Subnet1	10.0.1.0/24	VM1
Subnet2	10.0.2.0/24	VM2
Subnet3	10.0.3.0/24	VM3

VM3 has multiple network adapters, including a network adapter named NIC3. IP forwarding is enabled on NIC3. Routing is enabled on VM3.

You create a route table named RT1 that contains the routes in the following table:

Address prefix	Next hop type	Next hop address
10.0.1.0/24	Virtual appliance	10.0.3.4
10.0.2.0/24	Virtual appliance	10.0.3.4

You apply RT1 to Subnet1 and Subnet2.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
VM3 can establish a network connection to VM1.	<input type="radio"/>	<input type="radio"/>
If VM3 is turned off, VM2 can establish a network connection to VM1.	<input type="radio"/>	<input type="radio"/>
VM1 can establish a network connection to VM2.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
VM3 can establish a network connection to VM1.	<input checked="" type="radio"/>	<input type="radio"/>
If VM3 is turned off, VM2 can establish a network connection to VM1.	<input type="radio"/>	<input checked="" type="radio"/>
VM1 can establish a network connection to VM2.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

IP forwarding enables the virtual machine a network interface is attached to:

- ⇒ Receive network traffic not destined for one of the IP addresses assigned to any of the IP configurations assigned to the network interface.

Send network traffic with a different source IP address than the one assigned to one of a network interface's IP configurations.

The setting must be enabled for every network interface that is attached to the virtual machine that receives traffic that the virtual machine needs to forward. A virtual machine can forward traffic whether it has multiple network interfaces or a single network interface attached to it.

Box 1: Yes -

The routing table allows connections from VM3 to VM1 and VM2. And as IP forwarding is enabled on VM3, VM3 can connect to VM1.

Box 2: No -

VM3, which has IP forwarding, must be turned on, in order for VM2 to connect to VM1.

Box 3: Yes -

The routing table allows connections from VM1 and VM2 to VM3. IP forwarding on VM3 allows VM1 to connect to VM2 via VM3.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview> <https://www.quora.com/What-is-IP-forwarding>

CertyIQ

Question: 472

Your on-premises network contains an SMB share named Share1.

You have an Azure subscription that contains the following resources:

- ⇒ A web app named webapp1
- ⇒ A virtual network named VNET1

You need to ensure that webapp1 can connect to Share1.

What should you deploy?

- A. an Azure Application Gateway
- B. an Azure Active Directory (Azure AD) Application Proxy
- C. an Azure Virtual Network Gateway

Answer: C

Explanation:

A Site-to-Site VPN gateway connection can be used to connect your on-premises network to an Azure virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel.

This type of connection requires a VPN device, a VPN gateway, located on-premises that has an externally facing public IP address assigned to it.

Incorrect Answers:

B: Application Proxy is a feature of Azure AD that enables users to access on-premises web applications from a remote client.

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal>

Question: 473

You plan to deploy several Azure virtual machines that will run Windows Server 2019 in a virtual machine scale set by using an Azure Resource Manager template.

You need to ensure that NGINX is available on all the virtual machines after they are deployed.

What should you use?

- A. the Publish-AzVMDscConfiguration cmdlet
- B. Azure Application Insights
- C. Azure Custom Script Extension
- D. the New-AzConfigurationAssignment cmdlet

Answer: C**Explanation:**

Note:

There are several versions of this question in the exam. The question has two correct answers:

1. a Desired State Configuration (DSC) extension
2. Azure Custom Script Extension

The question can have other incorrect answer options, including the following:

- ⇒ Deployment Center in Azure App Service
- ⇒ a Microsoft Intune device configuration profile

Reference:

<https://docs.microsoft.com/en-us/azure/architecture/framework/devops/automation-configuration>

Question: 474

Your on-premises network contains a VPN gateway.

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

Name	Type	Description
vgw1	Virtual network gateway	Gateway for Site-to-Site VPN to the on-premises network
storage1	Storage account	Standard performance tier
Vnet1	Virtual network	Enabled forced tunneling
VM1	Virtual machine	Connected to Vnet1

You need to ensure that all the traffic from VM1 to storage1 travels across the Microsoft backbone network. What should you configure?

- A. a network security group (NSG)
- B. service endpoints
- C. Azure Peering Service
- D. Azure Firewall

Answer: B**Explanation:**

"Virtual Network (VNet) service endpoint provides secure and direct connectivity to Azure services over an optimized route over the Azure backbone network."

Reference:

Question: 475

You plan to deploy route-based Site-to-Site VPN connections between several on-premises locations and an Azure virtual network.

Which tunneling protocol should you use?

- A. IKEv1
- B. PPTP
- C. IKEv2
- D. L2TP

Answer: C

Explanation:

A Site-to-Site (S2S) VPN gateway connection is used to connect your on-premises network to an Azure virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel.

IKEv2 supports 10 S2S connections, while IKEv1 only supports 1.

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-classic-portal> <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-connect-multiple-policybased-rm-ps>

Question: 476

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

Name	Type	Description
VNET1	Virtual network	Azure region: US East Contains the following subnets: <ul style="list-style-type: none">• Subnet1: 172.16.1.0/24• Subnet2: 172.16.2.0/24• Subnet3: 172.16.3.0/24
VNET2	Virtual network	Azure region: West US Contains the following subnets: <ul style="list-style-type: none">• DemoSubnet1: 172.16.1.0/24• RecoverySubnetA: 172.16.5.0/24• RecoverySubnetB: 172.16.3.0/24• TestSubnet1: 172.16.2.0/24
VM1	Virtual machine	Connected to Subnet2

You configure Azure Site Recovery to replicate VM1 between the US East and West US regions.

You perform a test failover of VM1 and specify VNET2 as the target virtual network.

When the test version of VM1 is created, to which subnet will the virtual machine be connected?

- A. TestSubnet1
- B. DemoSubnet1
- C. RecoverySubnetA
- D. RecoverySubnetB

Answer: B

Explanation:

<https://learn.microsoft.com/en-us/azure/site-recovery/azure-to-azure-network-mapping>

The subnet of the target VM is selected based on the name of the subnet of the source VM.

- If a subnet with the same name as the source VM subnet is available in the target network, that subnet is set for the target VM.
- If a subnet with the same name doesn't exist in the target network, the first subnet in the alphabetical order is set as the target subnet.

Question: 477

CertyIQ

You have five Azure virtual machines that run Windows Server 2016. The virtual machines are configured as web servers.

You have an Azure load balancer named LB1 that provides load balancing services for the virtual machines.

You need to ensure that visitors are serviced by the same web server for each request.

What should you configure?

- A. Protocol to UDP
- B. Session persistence to None
- C. Floating IP (direct server return) to Disabled
- D. Session persistence to Client IP

Answer: D

Explanation:

D. Session persistence to Client IP.

When configuring an Azure Load Balancer (LB1) for web servers, you can define session persistence to ensure that a user is always connected to the same virtual machine (VM) for the duration of their session.

Session persistence (also known as "sticky sessions") ensures that requests from the same client IP are directed to the same backend server.

This is especially useful for stateful applications, where session data is stored locally on a specific server.

Question: 478

CertyIQ

You plan to deploy several Azure virtual machines that will run Windows Server 2019 in a virtual machine scale set by using an Azure Resource Manager template.

You need to ensure that NGINX is available on all the virtual machines after they are deployed.

What should you use?

- A. the Publish-AzVMDscConfiguration cmdlet
- B. a Microsoft Endpoint Manager device configuration profile
- C. Deployment Center in Azure App Service
- D. a Desired State Configuration (DSC) extension

Answer: D

Explanation:

D. a Desired State Configuration (DSC) extension.

When deploying Azure Virtual Machine Scale Sets (VMSS) using an Azure Resource Manager (ARM) template, you need to ensure that NGINX is installed on all instances after deployment. The best way to automate software installation and configuration in an ARM template is by using the Desired State Configuration (DSC) extension.

Question: 479

CertyIQ

You have five Azure virtual machines that run Windows Server 2016. The virtual machines are configured as web servers.

You have an Azure load balancer named LB1 that provides load balancing services for the virtual machines.

You need to ensure that visitors are serviced by the same web server for each request.

What should you configure?

- A. Floating IP (direct server return) to Disabled
- B. Session persistence to Client IP
- C. Protocol to UDP
- D. Idle Time-out (minutes) to 20

Answer: B

Explanation:

B. Session persistence to Client IP.

In an Azure Load Balancer (LB1) scenario where multiple virtual machines (web servers) are serving traffic, we need to ensure that a visitor is always connected to the same web server during their session.

This is achieved by Session Persistence, which ensures that traffic from the same client is routed to the same backend VM.

Question: 480

CertyIQ

You have an Azure subscription that contains 20 virtual machines, a network security group (NSG) named NSG1, and two virtual networks named VNET1 and VNET2 that are peered.

You plan to deploy an Azure Bastion Basic SKU host named Bastion1 to VNET1.

You need to configure NSG1 to allow inbound access to the virtual machines via Bastion1.

Which port should you configure for the inbound security rule?

- A. 22
- B. 443
- C. 389
- D. 8080

Answer: B

Explanation:

443

Using Bastion your RDP/SSH session is over TLS on port 443.

<https://learn.microsoft.com/en-us/azure/bastion/bastion-overview>

If you say port 22 then what about windows VM as it is not mentioned that the VM is windows or Linux? You will have to allow port 443 in NSG.

Question: 481

CertyIQ

HOTSPOT

-

Your network contains an on-premises Active Directory Domain Services (AD DS) domain named contoso.com. The domain contains the servers shown in the following table.

Name	IP address	Role
DC1	192.168.2.1/16	Domain controller DNS server
Server1	192.168.2.50/16	Member server

You plan to migrate contoso.com to Azure.

You create an Azure virtual network named VNET1 that has the following settings:

- Address space: 10.0.0.0/16
- Subnet:
 - Name: Subnet1
 - IPv4: 10.0.1.0/24

You need to move DC1 to VNET1. The solution must ensure that the member servers in contoso.com can resolve AD DS DNS names.

How should you configure DC1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

IP address

Obtain an IP address automatically
Use 10.0.1.3
Use 10.0.2.1
Use 192.168.2.1

Name resolution

Configure VNET1 to use a custom DNS server
Configure VNET1 to use the default Azure-provided DNS server
Create an Azure Private DNS zone named contoso.com
Create an Azure public DNS zone named contoso.com

Answer:

Answer Area

IP address

Obtain an IP address automatically
Use 10.0.1.3
Use 10.0.2.1
Use 192.168.2.1

Name resolution

Configure VNET1 to use a custom DNS server
Configure VNET1 to use the default Azure-provided DNS server
Create an Azure Private DNS zone named contoso.com
Create an Azure public DNS zone named contoso.com

Explanation:

1) Obtain an IP address automatically

The first 4 IP addresses within a subnet space are getting reserved for Azure automatically. Thus, 10.0.1.3 can't be the right answer. 10.0.2.1 is in the VNET space but falls out of the subnet space. 192.168.2.1 is just out of the VNET.

2) Configure VNET1 to use a custom DNS server

This VNET1 should use our pre-created DNS server as its DNS server so that the member servers in contoso.com can resolve AD DS DNS names.

Question: 482

CertyIQ

You have five Azure virtual machines that run Windows Server 2016. The virtual machines are configured as web servers.

You have an Azure load balancer named LB1 that provides load balancing services for the virtual machines.

You need to ensure that visitors are serviced by the same web server for each request.

What should you configure?

- A. Session persistence to None
- B. a health probe
- C. Session persistence to Client IP
- D. Idle Time-out (minutes) to 20

Answer: C

Explanation:

Session persistence to Client IP.

Traffic from the same client IP is routed to the same backend instance

Reference:

<https://learn.microsoft.com/en-us/azure/load-balancer/distribution-mode-concepts>

Question: 483

CertyIQ

You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Azure region	Resource group
VNET1	West US	RG1
VNET2	Central US	RG1
VNET3	Central US	RG2
VNET4	West US	RG2

You need to deploy an Azure firewall named AF1 to RG1 in the West US Azure region.

To which virtual networks can you deploy AF1?

- A. VNET1, VNET2, VNET3, and VNET4
- B. VNET1 and VNET2 only
- C. VNET1 only
- D. VNET1, VNET2, and VNET4 only
- E. VNET1 and VNET4 only

Answer: C**Explanation:**

VNET1 only.

No idea why people are saying option E as the question clearly states that "You need to deploy an Azure firewall named AF1 to RG1 in the West US", so RG1 in the West US region means the correct answer is C(VNET1).

An Azure Firewall can protect a VNet in the same resource group, but it cannot directly protect a VNet in a different resource group. This is because an Azure Firewall is deployed in a VNet and filters traffic entering and exiting that VNet. It cannot interact with resources in other resource groups.

If you need to protect a VNet in a different resource group, you can use one of the following workarounds:

VNet peering

Azure Virtual WAN

VPN

Question: 484**CertyIQ**

You have an on-premises network.

You have an Azure subscription that contains three virtual networks named VNET1, VNET2, and VNET3. The virtual networks are peered and connected to the on-premises network. The subscription contains the virtual machines shown in the following table.

Name	Location	Connected to
VM1	West US	VNET1
VM2	West US	VNET1
VM3	West US	VNET2
VM4	Central US	VNET3

You need to monitor connectivity between the virtual machines and the on-premises network by using Connection Monitor.

What is the minimum number of connection monitors you should deploy?

- A. 1
- B. 2
- C. 3
- D. 4

Answer: B**Explanation:**

The answer is B. 2 minimum connection monitors. The reason is you have on-premises network and Azure(Cloud) network. So, you need 2. This is nothing to do with the location: West US and Central US. This is a trap! Someone people said it's to do with these 2 locations. If you only have 1 kind of network(Azure Cloud/on-premises, then you need minimum 1 connection monitor.

Connection monitor resource: A region-specific Azure resource.

<https://learn.microsoft.com/en-us/azure/network-watcher/connection-monitor-create-using-portal#before-you-begin>

Question: 485

CertyIQ

HOTSPOT

- You plan to deploy the following Azure Resource Manager (ARM) template.

```
{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {},
  "variables": {
    "vnetId": "[resourceId('Microsoft.Network/virtualNetworks/', 'VNET1')]",
    "lbId": "[resourceId('Microsoft.Network/loadBalancers/', 'LB1')]",
    "sku": "Standard",
    "netname": "APP1"
  },
  "resources": [
    {
      "apiVersion": "2017-08-01",
      "type": "Microsoft.Network/loadBalancers/",
      "name": "LB1",
      "location": "EastUS",
      "sku": {
        "name": "[variables('sku')]"
      },
      "properties": {
        "frontendIPConfiguration": [
          {
            "name": "[variables('netname')]",
            "properties": {
              "subnet": {
                "id": "[concat(variables('vnetId'), '/subnets/', variables('netname'))]"
              },
              "privateIPAllocationMethod": "Dynamic"
            }
          }
        ],
        "backendAddressPools": [
          {
            "name": concat(variables('netname'), '-Servers')"
          }
        ],
        "loadBalancingRules": [
          {
            "name": "APP1",
            "properties": {
              "frontendIPConfiguration": [
                "id": "[concat(variables('lbId'), '/frontendIPConfigurations/', variables('netname'))]"
              ],
              "backendAddressPool": [
                "id": "[concat(variables('lbId'), '/backendAddressPool/', variables('netname'))]"
              ],
              "probe": [
                "id": "[concat(variables('lbId'), '/probes/probe')]"
              ],
              "backendPort": 8080,
              "protocol": "Tcp",
              "frontendPort": 80,
              "enableFloatingIP": false,
              "idleTimeoutInMinutes": 4,
              "loadDistribution": "SourceIPProtocol"
            }
          }
        ],
        "probes": [
          {
            "name": "probe",
            "properties": [
              "protocol": "Tcp",
              "port": 8080,
              "intervalInSeconds": 15,
              "numberOfProbes": 2
            ]
          }
        ]
      }
    }
  ]
}
```

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
LB1 will be connected to a subnet named VNET1/netname	<input type="radio"/>	<input type="radio"/>
LB1 can be deployed only to the resource group that contains VNET1	<input type="radio"/>	<input type="radio"/>
The value of the sku variable can be provided as a parameter when the template is deployed from a command prompt	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
LB1 will be connected to a subnet named VNET1/netname	<input type="radio"/>	<input checked="" type="radio"/>
LB1 can be deployed only to the resource group that contains VNET1	<input type="radio"/>	<input checked="" type="radio"/>
The value of the sku variable can be provided as a parameter when the template is deployed from a command prompt	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

NO, NO, NO.

Box 1: instead of "netname" there should be the value of netname variable

Box 2: I don't see Resource Group mentioned anywhere in the template

Box 3: I don't see parameters being referred anywhere in the template, only variables are referred, e.g. "sku" variable.

Question: 486

CertyIQ

You have an Azure subscription that contains a storage account. The account stores website data.

You need to ensure that inbound user traffic uses the Microsoft point-of-presence (POP) closest to the user's location.

What should you configure?

- A. private endpoints

- B. Azure Firewall rules
- C. Routing preference
- D. load balancing

Answer: C

Explanation:

C: Routing preference.

Routing preference in Azure Traffic Manager allows you to specify how to route traffic to your Azure service endpoints based on various criteria, such as the geographic location of the client or the endpoint, the performance of the endpoint, or the priority of the endpoint.

By configuring routing preference, you can direct incoming user traffic to the Microsoft point-of-presence (POP) closest to the user's location, ensuring the best possible user experience. This can be achieved by selecting the "Performance" routing method in Azure Traffic Manager, which uses DNS-based traffic routing to direct users to the endpoint that offers the best performance from the user's location.

Question: 487

CertyIQ

You have two Azure virtual machines named VM1 and VM2 that run Windows Server. The virtual machines are in a subnet named Subnet1. Subnet1 is in a virtual network named VNet1.

You need to prevent VM1 from accessing VM2 on port 3389.

What should you do?

- A. Create a network security group (NSG) that has an outbound security rule to deny destination port 3389 and apply the NSG to the network interface of VM1.
- B. Configure Azure Bastion in VNet1.
- C. Create a network security group (NSG) that has an outbound security rule to deny source port 3389 and apply the NSG to Subnet1.
- D. Create a network security group (NSG) that has an inbound security rule to deny source port 3389 and apply the NSG to Subnet1.

Answer: A

Explanation:

A. Create a network security group (NSG) that has an outbound security rule to deny destination port 3389 and apply the NSG to the network interface of VM1.

By creating an outbound security rule in a network security group (NSG) to deny destination port 3389, you can prevent VM1 from accessing port 3389 on VM2. By applying the NSG to the network interface of VM1, you can enforce the security rule specifically for VM1.

This solution provides a centralized way to manage and enforce network security for VM1, and it helps to prevent unwanted access to port 3389 on VM2 from VM1.

If it was D. "Create a network security group (NSG) that has an inbound security rule to deny source port 3389 and apply the NSG to Subnet1" you could prevent access to port 3389 on VM2 from ANY SOURCE (including VM1). By applying the NSG to Subnet1, you can apply the security rule to both VM1 and VM2.

The question asked "to prevent VM1 from accessing VM2 on port 3389", not from any source.

Question: 488

CertyIQ

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

Name	Type	Description
App1	App Service	Virtual network integration enabled for VNET1
ASP1	App Service plan	Standard SKU
VNET1	Virtual network	None
Firewall1	Azure Firewall	Connected to VNET1

You need to manage outbound traffic from VNET1 by using Firewall1.

What should you do first?

- A. Configure the Hybrid Connection Manager.
- B. Upgrade ASP1 to the Premium SKU.
- C. Create a route table.
- D. Create an Azure Network Watcher.

Answer: C

Explanation:

Route all traffic to the firewall

When you create a virtual network, Azure automatically creates a default route table for each of its subnets and adds system default routes to the table. In this step, you create a user-defined route table that routes all traffic to the firewall, and then associate it with the App Service subnet in the integrated virtual network.

Section3 in document.

<https://learn.microsoft.com/en-us/azure/app-service/network-secure-outbound-traffic-azure-firewall>

Question: 489

CertyIQ

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

Name	Type
VM1	Virtual machine
App1	Web app
contoso.com	Azure Active Directory Domain Services (Azure AD DS) domain

All the resources connect to a virtual network named VNet1.

You plan to deploy an Azure Bastion host named Bastion1 to VNet1.

Which resources can be protected by using Bastion1?

- A. VM1 only
- B. contoso.com only
- C. App1 and contoso.com only
- D. VM1 and contoso.com only
- E. VM1, App1, and contoso.com

Answer: A

Explanation:

Bastion provides secure RDP and SSH connectivity to all of the VMs in the virtual network in which it is provisioned. Using Azure Bastion protects your virtual machines from exposing RDP/SSH ports to the outside world, while still providing secure access using RDP/SSH.

Question: 490

CertyIQ

You have five Azure virtual machines that run Windows Server 2016. The virtual machines are configured as web servers.

You have an Azure load balancer named LB1 that provides load balancing services for the virtual machines.

You need to ensure that visitors are serviced by the same web server for each request.

What should you configure?

- A. Session persistence to None
- B. a health probe
- C. Session persistence to Client IP and protocol
- D. Idle Time-out (minutes) to 20

Answer: C

Explanation:

<https://learn.microsoft.com/en-us/azure/load-balancer/distribution-mode-concepts>

Session persistence: Client IP and protocol

Traffic from the same client IP and protocol is routed to the same backend instance

Question: 491

CertyIQ

You have five Azure virtual machines that run Windows Server 2016. The virtual machines are configured as web servers.

You have an Azure load balancer named LB1 that provides load balancing services for the virtual machines.

You need to ensure that visitors are serviced by the same web server for each request.

What should you configure?

- A. a health probe
- B. Floating IP (direct server return) to Enabled
- C. Session persistence to Client IP and protocol

D. Protocol to UDP

Answer: C

Explanation:

C. Session persistence to Client IP and protocol.

Azure Load Balancer distributes incoming traffic across multiple virtual machines. To ensure that visitors are consistently directed to the same web server for each request, you need to configure session persistence (also known as "sticky sessions").

Session persistence ensures that a client's requests are always sent to the same backend server for the duration of the session.

The "Client IP and protocol" option ensures that the same server handles requests from a client based on both their IP address and protocol.

Question: 492

CertyIQ

You have an Azure subscription that contains 10 virtual machines and the resources shown in the following table.

Name	Type	Description
VNET1	Virtual network	none
Bastion1	Basic SKU Azure Bastion host	Subnet size /26

You need to ensure that Bastion1 can support 100 concurrent SSH users. The solution must minimize administrative effort.

What should you do first?

- A.Resize the subnet of Bastion1
- B.Configure host scaling.
- C.Create a network security group (NSG)
- D.Upgrade Bastion1 to the Standard SKU

Answer: D

Explanation:

<https://learn.microsoft.com/en-us/azure/bastion/configuration-settings#instance>When you configure Azure Bastion using the Basic SKU, two instances are created. If you use the Standard SKU, you can specify the number of instances. This is called host scaling. Each instance can support 20 concurrent RDP connections and 40 concurrent SSH connections for medium workloads. Once the concurrent sessions are exceeded, an additional scale unit (instance) is required.

Question: 493

CertyIQ

You have five Azure virtual machines that run Windows Server 2016. The virtual machines are configured as web servers.

You have an Azure load balancer named LB1 that provides load balancing services for the virtual machines.

You need to ensure that visitors are serviced by the same web server for each request.

What should you configure?

- A. Session persistence to Client IP and protocol
- B. Protocol to UDP
- C. Session persistence to None
- D. Floating IP (direct server return) to Disabled

Answer: A

Explanation:

- A. Session persistence to Client IP and protocol.

Azure Load Balancer distributes traffic among backend virtual machines (VMs). To ensure that each visitor's requests go to the same web server, you need to enable session persistence (also known as "sticky sessions").

"Client IP and protocol" session persistence ensures that requests from a specific client IP always go to the same backend VM, as long as the session is active.

This helps maintain user sessions, especially for applications that rely on stateful data, such as shopping carts or login sessions.

Question: 494

CertyIQ

DRAG DROP

You have a Windows 11 device named Device1 and an Azure subscription that contains the resources shown in the following table.

Name	Description
VNET1	Virtual network
VM1	Virtual machine that runs Windows Server 2022 and does NOT have a public IP address Connected to VNET1
Bastion1	Azure Bastion Basic SKU host connected to VNET1

Device1 has Azure PowerShell and Azure Command-Line Interface (CLI) installed.

From Device1, you need to establish a Remote Desktop connection to VM1.

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.

Actions

- From Azure CLI on Device1, run az network bastion rdp.
- From Bastion1, enable Kerberos authentication.
- From VM1, enable just-in-time (JIT) VM access.
- From Bastion1, select Native Client Support.**
- On Device1, run mstsc.exe.
- Upgrade Bastion1 to the Standard SKU.

Answer Area**Answer:****Actions**

- From Azure CLI on Device1, run az network bastion rdp.
- From Bastion1, enable Kerberos authentication.
- From VM1, enable just-in-time (JIT) VM access.
- From Bastion1, select Native Client Support.**
- On Device1, run mstsc.exe.
- Upgrade Bastion1 to the Standard SKU.

Answer Area

- Upgrade Bastion1 to the Standard SKU.
- From Bastion1, select **Native Client Support**.
- From Azure CLI on Device1, run az network bastion rdp.

**Explanation:****1. Upgrade Bastion1 to the Standard SKU.**

Azure Bastion offers two SKUs: Basic and Standard.

Native Client Support is available only in the Standard SKU, so you must upgrade Bastion1 if it's running on the Basic SKU.

This is a mandatory prerequisite before enabling Native Client Support.

2. From Bastion 1,Select Native Client Support.

After upgrading, you must enable Native Client Support in the Azure Bastion settings.

This allows users to connect using tools like mstsc.exe (Microsoft's RDP client) instead of the browser-based Azure portal.

3. From Azure CLI on Device1,run az network bastion rdp.

Once Native Client Support is enabled, you can connect using Azure CLI with the following command:

sh

Copy

Edit

```
az network bastion rdp --name Bastion1 --resource-group MyResourceGroup --target-ip VM-IP-Address
```

This command starts an RDP connection to the target VM using Azure Bastion and the native RDP client (mstsc.exe).

Question: 495

CertyIQ

You have five Azure virtual machines that run Windows Server 2016. The virtual machines are configured as web servers.

You have an Azure load balancer named LB1 that provides load balancing services for the virtual machines.

You need to ensure that visitors are serviced by the same web server for each request.

What should you configure?

- A.Floating IP (direct server return) to Enabled
- B.Session persistence to Client IP
- C.Protocol to UDP
- D.Idle Time-out (minutes) to 20

Answer: B**Explanation:**

B. Session persistence to Client IP.To ensure that visitors are serviced by the same web server for each request, we need to configure session persistence on the Azure load balancer. Session persistence is also known as affinity, and it ensures that all requests from a client are sent to the same backend server. This is important for applications that maintain session state, such as web applications that require authentication or shopping carts.

Question: 496

CertyIQ

You have an Azure subscription that has the public IP addresses shown in the following table.

Name	IP version	SKU	Tier	IP address assignment
IP1	IPv4	Standard	Regional	Static
IP2	IPv4	Standard	Global	Static
IP3	IPv4	Basic	Regional	Dynamic
IP4	IPv4	Basic	Regional	Static
IP5	IPv6	Basic	Regional	Dynamic

You plan to deploy an Azure Bastion Basic SKU host named Bastion1.

Which IP addresses can you use?

- A.IP1 only
- B.IP1 and IP2 only
- C.IP3, IP4, and IP5 only
- D.IP1, IP2, IP4, and IP5 only
- E.IP1, IP2, IP3, IP4, and IP5

Answer: A**Explanation:**

A. IP1 only.

Azure Bastion requires a Standard SKU public IP address, and the public IP address must be static and regional.

Looking at the provided table:

IP1: Standard SKU, regional, static (meets all the requirements for Azure Bastion Basic SKU).

IP2: Standard SKU, global, static (global tier is not supported for Bastion, only regional tier is allowed).

CertyIQ

Question: 497

You have five Azure virtual machines that run Windows Server 2016. The virtual machines are configured as web servers.

You have an Azure load balancer named LB1 that provides load balancing services for the virtual machines.

You need to ensure that visitors are serviced by the same web server for each request.

What should you configure?

- A.Floating IP (direct server return) to Disabled
- B.Floating IP (direct server return) to Enabled
- C.a health probe
- D.Session persistence to Client IP

Answer: D

Explanation:

D. Session persistence to Client IP.

Azure Load Balancer distributes traffic among backend virtual machines (VMs) to ensure availability and scalability. However, to ensure that each visitor is always serviced by the same web server for each request, you need to configure session persistence (also known as "sticky sessions").

Session Persistence (Client IP):

This setting ensures that all requests from the same client IP address are routed to the same backend VM.

This is useful for stateful applications, such as web applications that store session data on the server.

CertyIQ

Question: 498

You have five Azure virtual machines that run Windows Server 2016. The virtual machines are configured as web servers.

You have an Azure load balancer named LB1 that provides load balancing services for the virtual machines.

You need to ensure that visitors are serviced by the same web server for each request.

What should you configure?

- A.Floating IP (direct server return) to Enabled
- B.Idle Time-out (minutes) to 20

C.a health probe

D.Session persistence to Client IP

Answer: D

Explanation:

D. Session persistence to Client IP.

Azure Load Balancer distributes incoming traffic among multiple virtual machines (VMs). If you need to ensure that each visitor is serviced by the same web server for each request, you must enable session persistence (also called sticky sessions).

Session Persistence (Client IP):

Ensures that requests from the same client IP address are routed to the same backend VM.

This is especially useful for stateful applications that store session data on a specific server.

Question: 499

CertyIQ

You have two Azure subscriptions named Sub1 and Sub2.

Sub1 contains a virtual machine named VM1 and a storage account named storage1.

VM1 is associated to the resources shown in the following table.

Name	Type
Disk1	Operating system disk
NetInt1	Network interface
VNet1	Virtual network

You need to move VM1 to Sub2.

Which resources should you move to Sub2?

- A.VM1, Disk1, and NetInt1 only
- B.VM1, Disk1, and VNet1 only
- C.VM1, Disk1, and storage1 only
- D.VM1, Disk1, NetInt1, and VNet1

Answer: D

Explanation:

When you move a virtual machine from one subscription to another, you need to ensure that all the dependent resources are also moved along with it. In the given scenario, VM1 is associated with the resources Disk1 (OS Disk), NetInt1 (Network Interface), and VNet1 (Virtual Network), and the storage account named storage1 is not associated with VM1. Therefore, to move VM1 to Sub2, you need to move the following resources:
VM1: This is the virtual machine that you want to move to Sub2.
Disk1: This is the OS disk for VM1, and it contains the operating system and boot files.
NetInt1: This is the network interface that is attached to VM1 and provides connectivity to the virtual network.
VNet1: This is the virtual network that is associated with VM1, and it provides the network connectivity to the virtual machine.

Question: 500**CertyIQ**

You have five Azure virtual machines that run Windows Server 2016. The virtual machines are configured as web servers.

You have an Azure load balancer named LB1 that provides load balancing services for the virtual machines.

You need to ensure that visitors are serviced by the same web server for each request.

What should you configure?

- A.Session persistence to Client IP and protocol
- B.Idle Time-out (minutes) to 20
- C.Session persistence to None
- D.Floating IP (direct server return) to Enabled

Answer: A**Explanation:**

A. Session persistence to Client IP and protocol.

Azure Load Balancer distributes incoming traffic among multiple virtual machines (VMs). If you want each visitor to be serviced by the same web server for each request, you must enable session persistence (also known as sticky sessions).

Session Persistence (Client IP and protocol)

Ensures that all requests from the same client IP address and protocol (TCP/UDP) are routed to the same backend VM.

This is useful for stateful applications that store session data on a specific server.

Question: 501**CertyIQ**

You have five Azure virtual machines that run Windows Server 2016. The virtual machines are configured as web servers.

You have an Azure load balancer named LB1 that provides load balancing services for the virtual machines.

You need to ensure that visitors are serviced by the same web server for each request.

What should you configure?

- A.Floating IP (direct server return) to Disabled
- B.Idle Time-out (minutes) to 20
- C.a health probe
- D.Session persistence to Client IP

Answer: D**Explanation:**

D. Session persistence to Client IP.

Azure Load Balancer distributes incoming traffic among multiple backend virtual machines (VMs). If you want each visitor to be serviced by the same web server for each request, you must enable session persistence (also known as sticky sessions).

Session Persistence (Client IP)

Ensures that requests from the same client IP are always routed to the same backend VM.

This is useful for applications that rely on maintaining user sessions, such as web applications with shopping carts, user authentication, or other stateful interactions.

Question: 502

CertyIQ

You have five Azure virtual machines that run Windows Server 2016. The virtual machines are configured as web servers.

You have an Azure load balancer named LB1 that provides load balancing services for the virtual machines.

You need to ensure that visitors are serviced by the same web server for each request.

What should you configure?

- A.Session persistence to Client IP
- B.Idle Time-out (minutes) to 20
- C.Session persistence to None
- D.Protocol to UDP

Answer: A

Explanation:

A. Session persistence to Client IP.

Azure Load Balancer distributes incoming traffic among multiple backend virtual machines (VMs). If you need to ensure that each visitor is always serviced by the same web server for each request, you must enable session persistence (also known as sticky sessions).

Session Persistence (Client IP)

Ensures that requests from the same client IP are always routed to the same backend VM.

This is essential for applications that rely on maintaining user sessions, such as shopping carts, user authentication, or other stateful interactions.

Question: 503

CertyIQ

You plan to deploy several Azure virtual machines that will run Windows Server 2019 in a virtual machine scale set by using an Azure Resource Manager template.

You need to ensure that NGINX is available on all the virtual machines after they are deployed.

What should you use?

- A.the Publish-AzVMDscConfiguration cmdlet
- B.a Microsoft Endpoint Manager device configuration profile

C.Azure Application Insights

D.a Desired State Configuration (DSC) extension

Answer: A

Explanation:

The Publish-AzVMDscConfiguration cmdlet.

<https://learn.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-overview>

The Publish-AzVMDscConfiguration cmdlet takes in a configuration file, scans it for dependent DSC resources, and then creates a .zip file. The .zip file contains the configuration and DSC resources that are needed to enact the configuration. The cmdlet can also create the package locally by using the -OutputArchivePath parameter. Otherwise, the cmdlet publishes the .zip file to Blob Storage, and then secures it with an SAS token.

CertyIQ

Question: 504

You plan to deploy several Azure virtual machines that will run Windows Server 2019 in a virtual machine scale set by using an Azure Resource Manager template.

You need to ensure that NGINX is available on all the virtual machines after they are deployed.

What should you use?

- A.Azure Custom Script Extension
- B.Deployment Center in Azure App Service
- C.the New-AzConfigurationAssignment cmdlet
- D.a Microsoft Endpoint Manager device configuration profile

Answer: A

Explanation:

A. Azure Custom Script Extension.

The Azure Custom Script Extension allows you to run scripts on Azure virtual machines after they are deployed. You can use this to install and configure software like NGINX on all virtual machines in a virtual machine scale set. By specifying a script that installs NGINX in the template, it ensures that the software is available on all the virtual machines after deployment.

CertyIQ

Question: 505

You have an Azure subscription that contains a Recovery Services vault named Vault1.

You need to enable multi-user authorization (MAU) for Vault1.

Which resource should you create first?

- A.an administrative unit
- B.a managed identity
- C.a resource guard

D.a custom Azure role

Answer: C

Explanation:

<https://learn.microsoft.com/en-us/azure/backup/multi-user-authorization?tabs=azure-portal&pivots=vaults-recovery-services-vault> Before you start Testing scenarios Create a Resource Guard Enable MUA on a Recovery Services vault Protected operations on a vault using MUAAuthorize critical operations on a vault Disable MUA on a Recovery Services vault

Question: 506

CertyIQ

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 app named App1 that is installed on two Azure virtual machines named VM1 and VM2. Connections to App1 are managed by using an Azure Load Balancer.

The effective network security configurations for VM2 are shown in the following exhibit.

VM2 - Networking

Network Interface: VM2-NIC1 Effective security rules Topology

Inbound port rules Outbound port rules Application security groups Load balancing

Priority	Name	Port	Protocol	Source	Destination	Action
100	Allow_131.107.100.50	443	TCP	131.107.100.50	VirtualNetwork	Allow
200	BlockAllOther443	443	Any	Any	Any	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

You discover that connections to App1 from 131.107.100.50 over TCP port 443 fail.

You verify that the Load Balancer rules are configured correctly.

You need to ensure that connections to App1 can be established successfully from 131.107.100.50 over TCP port 443.

Solution: You create an inbound security rule that allows any traffic from the AzureLoadBalancer source and has a priority of 150.

Does this meet the goal?

- A.Yes
- B.No

Answer: A

Explanation:

A. Yes

Creating an inbound security rule that allows any traffic from the Azure Load Balancer source with a priority of 150 will enable the connections to App1 from the Load Balancer, which is necessary for routing traffic to VM2. Since the Load Balancer forwards traffic to the VMs, this rule will help ensure that connections over TCP port 443 from the specified IP address can be established successfully.

Question: 507**CertyIQ**

Your on-premises network contains a VPN gateway.

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

Name	Type	Description
vgw1	Virtual network gateway	Gateway for Site-to-Site VPN to the on-premises network
storage1	Storage account	Standard performance tier
Vnet1	Virtual network	Enabled forced tunneling
VM1	Virtual machine	Connected to Vnet1

You need to ensure that all the traffic from VM1 to storage1 travels across the Microsoft backbone network.

What should you configure?

- A.Azure Application Gateway
- B.service endpoints
- C.Azure AD Application Proxy
- D.Azure Virtual WAN

Answer: B**Explanation:**

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview>"Virtual Network (VNet) service endpoint provides secure and direct connectivity to Azure services over an optimized route over the Azure backbone network. Endpoints allow you to secure your critical Azure service resources to only your virtual networks. Service Endpoints enables private IP addresses in the VNet to reach the endpoint of an Azure service without needing a public IP address on the VNet."

Question: 508**CertyIQ**

You create an Azure VM named VM1 that runs Windows Server 2019.

VM1 is configured as shown in the exhibit. (Click the Exhibit tab.)

VM1 Virtual machine

Search:

Connect ▾ Start ▾ Restart ▾ Stop Capture Delete Refresh Open in mobile CLI/PS Feedback

Advisor (1 of 8): All network ports should be restricted on network security groups associated to your virtual machine →

Essentials

Resource group ([move](#)) : RG5
 Status : Stopped (deallocated)
 Location : East US (Zone 1)
 Subscription ([move](#)) : Visual Studio Enterprise Subscription
 Subscription ID : 7fefcd66e-8694-4b54-beae-17fc819d4973
 Availability zone : 1
 Tags ([edit](#)) : Click here to add tags

Operating system : Windows
 Size : Standard D51 v2 (1 vcpu, 3.5 GB memory)
 Public IP address : 20.115.52.215
 Virtual network/subnet : VNET1/default
 DNS name : Not configured

Properties Monitoring Capabilities (8) Recommendations (8) Tutorials

Virtual machine

Computer name	VM1
Health state	-
Operating system	Windows
Publisher	MicrosoftWindowsServer

Networking

Public IP address	20.115.52.215
Public IP address (IPv6)	-
Private IP address	10.1.0.4
Private IP address (IPv6)	-

You need to enable Desired State Configuration for VM1.

What should you do first?

- A.Connect to VM1.
- B.Start VM1.
- C.Capture a snapshot of VM1.
- D.Configure a DNS name for VM1.

Answer: B

Explanation:

B. Start VM1.

Desired State Configuration (DSC) is a feature of Windows PowerShell that enables you to manage and configure systems in a consistent way. To use DSC, the virtual machine (VM1 in this case) needs to be running. If the VM is not started, you cannot apply any DSC configurations to it.

Question: 509

CertyIQ

HOTSPOT

You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Location	IP address space	Subnet
VNet1	East US	10.1.128.0/23	Subnet1
VNet2	East US	192.168.0.0/16	Subnet21, Subnet23
VNet3	East US	172.16.0.0/16	Subnet3

The subnets have the IP address spaces shown in the following table.

Name	IP address space
Subnet1	10.1.128.0/24
Subnet21	192.168.0.0/17
Subnet22	192.168.128.0/17
Subnet3	172.16.1.0/24

You plan to create a container app named contapp1 in the East US Azure region.

You need to create a container app environment named con-env1 that meets the following requirements:

- Uses its own virtual network.
- Uses its own subnet.
- Is connected to the smallest possible subnet.

To which virtual networks can you connect con-env1, and which subnet mask should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Virtual network:

VNet1 only
 VNet2 only
 VNet3 only
 VNet1 or VNet2 only
 VNet2 or VNet3 only
 VNet1 or VNet3 only
 VNet1, VNet2, or VNet3

Subnet mask:

/16
 /23
 /24
 /26
 /28

Answer:

Answer Area

Virtual network:

VNet1 only
VNet2 only
VNet3 only
VNet1 or VNet2 only
VNet2 or VNet3 only
VNet1 or VNet3 only
VNet1, VNet2, or VNet3

Subnet mask:

/16
/23
/24
/26
/28

Explanation:

VNet3 only: Indicates that only VNet3 should be used for the configuration.

/23: This subnet mask allows for 512 IP addresses. It is suitable for medium-sized networks.

Question: 510

CertyIQ

You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Location
Vnet1	US East
Vnet2	US East
Vnet3	US East
Vnet4	UK South
Vnet5	UK South
Vnet6	UK South
Vnet7	Asia East
Vnet8	Asia East
Vnet9	Asia East
Vnet10	Asia East

All the virtual networks are peered. Each virtual network contains nine virtual machines.

You need to configure secure RDP connections to the virtual machines by using Azure Bastion.

What is the minimum number of Bastion hosts required?

- A.1
- B.3
- C.9
- D.10

Answer: A

Explanation:

Answer : 1.

Azure Bastion and VNet peering can be used together.

When VNet peering is configured, you don't have to deploy Azure Bastion in each peered VNet. This means if you have an Azure Bastion host configured in one virtual network (VNet), it can be used to connect to VMs deployed in a peered VNet without deploying an additional bastion host.

HOTSPOT

You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Location	Peered with
VNet1	East US	VNet2
VNet2	East US	VNet1, VNet3
VNet3	West US	VNet2

The subscription contains the virtual machines shown in the following table.

Name	Operating system	Connected to
VM1	Windows	VNet1
VM2	Linux	VNet2
VM3	Windows	VNet3

Each virtual machine contains only a private IP address.

You create an Azure bastion for VNet1 as shown in the following exhibit.

Create a Bastion

X

Basics Tags Advanced Review + create

Bastion allows web based RDP access to your vnet VM. [Learn more](#)

Project details

Subscription *

MSDN Platforms

Resource group *

RG1

[Create new](#)

Instance details

Name *

Bastion1

Region *

East US

Tier *

Basic

Instance count

2

Configure virtual networks

Virtual network *

VNet1

[Create new](#)

Subnet *

AzureBastionSubnet (10.0.2.0/24)

[Manage subnet configuration](#)

Public IP address

Public IP address *

Create new Use existing

Public IP address name *

VNet1-ip

Public IP address SKU

Standard

Assignment

Dynamic Static

[Review + create](#)

[Previous](#)

[Next : Tags >](#)

[Download a template for automation](#)

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
The Remote Desktop Connection client (mstsc.exe) can be used to connect to VM1 through Bastion1.	<input type="radio"/>	<input type="radio"/>
The Azure portal can use SSH to connect to VM2 through Bastion1.	<input type="radio"/>	<input type="radio"/>
The Azure portal can be used to connect to VM3 through Bastion1.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
The Remote Desktop Connection client (mstsc.exe) can be used to connect to VM1 through Bastion1.	<input type="radio"/>	<input checked="" type="radio"/>
The Azure portal can use SSH to connect to VM2 through Bastion1.	<input checked="" type="radio"/>	<input type="radio"/>
The Azure portal can be used to connect to VM3 through Bastion1.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

The Remote Desktop Connection client (mstsc.exe) can be used to connect to VM1 through Bastion1.

No

Azure Bastion provides secure and seamless RDP (Remote Desktop Protocol) connectivity to your VMs directly from the Azure portal. If VM1 is configured to allow RDP connections and Bastion1 is properly set up, you can use the Remote Desktop Connection client (mstsc.exe) to connect to VM1 through Bastion1. This method leverages Bastion's secure tunnel to establish the connection without exposing the VM to the public internet.

The Azure portal can use SSH to connect to VM2 through Bastion1.

Yes

Azure Bastion also supports SSH (Secure Shell) connections. If VM2 is configured to allow SSH connections and Bastion1 is set up correctly, you can use the Azure portal to initiate an SSH session to VM2 through Bastion1. This provides a secure way to manage your VM using command-line tools without needing a public IP address on the VM.

The Azure portal can be used to connect to VM3 through Bastion1.

No

Azure Bastion allows you to connect to VMs directly from the Azure portal using either RDP or SSH, depending on the VM's configuration. If VM3 is set up to allow connections through Bastion1, you can use the Azure portal to connect to VM3 using the appropriate protocol (RDP or SSH). This simplifies the process of accessing your VMs securely without the need for additional client software.

HOTSPOT

You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Location
VNet1	West Europe
VNet2	Southeast Asia
VNet3	South Central US

The subscription contains the subnets shown in the following table.

Name	Virtual network	Service endpoint
Subnet1	VNet1	<i>None</i>
Subnet2	VNet2	Microsoft.Storage
Subnet3	VNet3	Microsoft.Storage
Subnet4	VNet4	<i>None</i>

The subscription contains the storage accounts shown in the following table.

Name	Location	Kind
storage1	West Europe	StorageV2
storage2	South Central US	BlobStorage
storage3	Southeast Asia	StorageV2

You create a service endpoint policy named Policy1 in the South Central US Azure region to allow connectivity to all the storage accounts in the subscription.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Policy1 can be applied to Subnet3.	<input type="radio"/>	<input type="radio"/>
Only storage1 and storage2 can be accessed from VNet2.	<input type="radio"/>	<input type="radio"/>
Only storage2 can be accessed from VNet3.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Policy1 can be applied to Subnet3.	<input checked="" type="checkbox"/>	<input type="radio"/>
Only storage1 and storage2 can be accessed from VNet2.	<input type="radio"/>	<input checked="" type="checkbox"/>
Only storage2 can be accessed from VNet3.	<input checked="" type="checkbox"/>	<input type="radio"/>

Explanation:

Box 1: Yes

Virtual networks must be in the same region as the service endpoint policy <https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoint-policies-overview#limitations>

Box 2: No

VNet2 is in SEA Region, so it can only connect to the storage in SEA Region through Service Endpoint, which is storage3

Box 3: Yes

VNet3 is in the South Central US region, and so is the storage2

Question: 513

CertyIQ

You plan to deploy several Azure virtual machines that will run Windows Server 2019 in a virtual machine scale set by using an Azure Resource Manager template.

You need to ensure that NGINX is available on all the virtual machines after they are deployed.

What should you use?

- A.the New-AzConfigurationAssignment cmdlet
- B.Azure Application Insights
- C.the Publish-AzVMDscConfiguration cmdlet
- D.a Desired State Configuration (DSC) extension

Answer: D

Explanation:

D. a Desired State Configuration (DSC) extension.

Desired State Configuration (DSC) is a configuration management platform in PowerShell that ensures that the configuration of a system (in this case, an Azure virtual machine) remains consistent. Using the DSC extension for Azure VMs allows you to apply DSC configurations to all the virtual machines in your virtual machine scale set, ensuring that NGINX is installed and configured after deployment.

Question: 514

CertyIQ

You have an Azure subscription that contains a resource group named RG1 and a virtual network named VNet1.

You plan to create an Azure container instance named container1.

You need to be able to configure DNS name label scope reuse for container1.

What should you configure for container1?

- A.the private networking type
- B.the public networking type
- C.a new subnet on VNet1
- D.a confidential SKU

Answer: B

Explanation:

For Azure portal users, you can set the DNS name reuse policy on the Networking tab during the container instance creation process using the DNS name label scope reuse field. Available after choosing public network type

<https://learn.microsoft.com/en-us/azure/container-instances/how-to-reuse-dns-names#create-a-container-instance>

Question: 515

CertyIQ

HOTSPOT

-
You have the Azure virtual machines shown in the following table.

Name	IP address	Virtual network
VM1	10.0.0.4	VNET1
VM2	172.16.0.4	VNET2
VM3	192.168.0.4	VNET3
VM4	192.168.0.5	VNET3

VNET1, VNET2, and VNET3 are peered.

VM4 has a DNS server that is authoritative for a zone named contoso.com and contains the records shown in the following table.

Name	Type	Value
Server1	A	131.107.3.3
Server2	A	131.107.3.4

The virtual networks are configured to use the DNS servers shown in the following table.

Virtual network	DNS server
VNET1	Default (Azure-provided)
VNET2	Custom: 192.168.0.5
VNET3	Custom: 192.168.0.5

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

- | Statements | Yes | No |
|--|-----------------------|-----------------------|
| From VM1, server1.contoso.com resolves to 131.107.3.3. | <input type="radio"/> | <input type="radio"/> |
| From VM2, server1.contoso.com resolves to 131.107.3.3. | <input type="radio"/> | <input type="radio"/> |
| From VM3, server2.contoso.com resolves to 131.107.2.4. | <input type="radio"/> | <input type="radio"/> |

Answer:

Answer Area

Statements	Yes	No
From VM1, server1.contoso.com resolves to 131.107.3.3.	<input type="radio"/>	<input checked="" type="checkbox"/>
From VM2, server1.contoso.com resolves to 131.107.3.3.	<input checked="" type="checkbox"/>	<input type="radio"/>
From VM3, server2.contoso.com resolves to 131.107.2.4.	<input type="radio"/>	<input checked="" type="checkbox"/>

Explanation:

NYN is a correct answer.

Statement 1: From VM1, server1.contoso.com resolves to 131.107.3.3.

VM1 in VNET1 uses the Azure-provided DNS, which does not reference the DNS records on VM4.

Result: No.

Statement 2: From VM2, server1.contoso.com resolves to 131.107.3.3.

VM2 in VNET2 uses a custom DNS (192.168.0.5), which points to VM4's DNS server.

VM4's DNS contains a record for server1.contoso.com resolving to 131.107.3.3.

Result: Yes.

Statement 3: From VM3, server2.contoso.com resolves to 131.107.2.4.

VM3 in VNET3 uses a custom DNS (192.168.0.5), which points to VM4's DNS server.

VM4's DNS contains a record for server2.contoso.com, but it resolves to 131.107.3.4, not 131.107.2.4.

Result: No.

Question: 516

CertyIQ

DRAG DROP

-

You have an Azure subscription that contains a resource group named RG1.

You plan to create an Azure Resource Manager (ARM) template to deploy a new virtual machine named VM1. VM1 must support the capture of performance data.

You need to specify resource dependencies for the ARM template.

In which order should you deploy the resources? To answer, move all resources from the list of resources to the answer area and arrange them in the correct order.

Resources

Answer Area

virtual machine

Azure Monitor extension

network interface

virtual network



Answer:

Answer Area

virtual network

network interface

virtual machine

Azure Monitor extension

Explanation:

Virtual Network (VNet).

A virtual network in Azure is a logically isolated section of the Azure cloud where you can launch and manage Azure resources. It allows you to securely connect Azure resources to each other, the internet, and on-premises networks. Key features include subnets, network security groups (NSGs), and custom DNS settings.

Network Interface (NIC).

A network interface in Azure is a communication link between a virtual machine (VM) and a virtual network. It allows the VM to interact with other resources within the same VNet, other VNets, and external networks. Each VM can have one or more network interfaces, each with its own private IP address and associated configurations.

Virtual Machine (VM).

A virtual machine in Azure is a scalable, on-demand computing resource provided by Microsoft. VMs can run various operating systems and applications, and they can be customized with different sizes, storage options, and networking configurations. VMs are commonly used for hosting applications, development and testing environments, and more.

Azure Monitor Extension.

The Azure Monitor extension is a tool that collects and analyzes telemetry data from Azure resources, including VMs. It provides insights into the performance, availability, and health of your applications and infrastructure. The extension can be installed on VMs to gather metrics, logs, and other diagnostic data, which can be used for monitoring, alerting, and troubleshooting.

Question: 517**CertyIQ**

You plan to deploy several Azure virtual machines that will run Windows Server 2019 in a virtual machine scale set by using an Azure Resource Manager template.

You need to ensure that NGINX is available on all the virtual machines after they are deployed.

What should you use?

- A.a Desired State Configuration (DSC) extension
- B.a Microsoft Intune device configuration profile
- C.the Publish-AzVMDscConfiguration cmdlet
- D.the New-AzConfigurationAssignment cmdlet

Answer: A**Explanation:**

A. a Desired State Configuration (DSC) extension.

Desired State Configuration (DSC) extension is the most suitable tool to ensure that NGINX is available on all the virtual machines in the scale set after deployment. DSC allows you to define the configuration of your virtual machines, including software installation (like NGINX), and ensures that the configuration is maintained across all VMs in the scale set.

Question: 518**CertyIQ**

You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Region	Peers with
VNet1	West US	VNet2
VNet2	West US	VNet1, VNet3
VNet3	East US	VNet2

The subscription contains the virtual machines shown in the following table.

Name	Connected to
VM1	VNet1
VM2	VNet2
VM3	VNet3

All the virtual machines have only private IP addresses.

You deploy an Azure Bastion host named Bastion1 to VNet1.

To which virtual machines can you connect through Bastion1?

- A. VM1 only
- B. VM1 and VM2 only
- C. VM1 and VM3 only
- D. VM1, VM2, and VM3

Answer: B

Explanation:

B (VM1 and VM2) because Bastion is deployed to VNet1, which is peered with VNet2.

Question: 519

CertyIQ

You plan to deploy several Azure virtual machines that will run Windows Server 2019 in a virtual machine scale set by using an Azure Resource Manager template.

You need to ensure that NGINX is available on all the virtual machines after they are deployed.

What should you use?

- A. a Microsoft Intune device configuration profile
- B. a Desired State Configuration (DSC) extension
- C. Azure Application Insights
- D. Deployment Center in Azure App Service

Answer: B

Explanation:

B. a Desired State Configuration (DSC) extension.

Desired State Configuration (DSC) is a PowerShell-based configuration management platform that ensures a machine's configuration is maintained consistently. Using the DSC extension on Azure virtual machines, you can specify configurations like software installations (e.g., NGINX) and ensure that those configurations are applied and maintained across all virtual machines in a scale set.

Question: 520

CertyIQ

You have an Azure subscription.

You plan to migrate 50 virtual machines from VMware vSphere to the subscription.

You create a Recovery Services vault.

What should you do next?

- A.Configure an extended network.
- B.Create a recovery plan.
- C.Deploy an Open Virtualization Application (OVA) template to vSphere.
- D.Configure a virtual network.

Answer: D

Explanation:

D. Configure a virtual network.

To migrate virtual machines (VMs) from VMware vSphere to Azure, you need to ensure that the target Azure environment is set up with a virtual network. The virtual machines that will be migrated will need to connect to a virtual network in Azure once they are migrated, so it's essential to configure that network ahead of the migration process.

Question: 521

CertyIQ

HOTSPOT

-

You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Location	Peered with
VNet1	East US	VNet2
VNet2	East US	VNet1

Each virtual network has 50 connected virtual machines.

You need to implement Azure Bastion. The solution must meet the following requirements:

- Support host scaling.
- Support uploading and downloading files.
- Support the virtual machines on both VNet1 and VNet2.
- Minimize the number of addresses on the Azure Bastion subnet.

How should you configure Azure Bastion? To answer, select the options in the answer area.

NOTE: Each correct answer is worth one point.

Answer Area

Subnet size:

/24
/26
/28
/29

Public IP:

Basic SKU with a dynamic allocation
Basic SKU with a static allocation
Standard SKU with a static allocation

Answer:

Answer Area

Subnet size:

/24
/26
/28
/29

Public IP:

Basic SKU with a dynamic allocation
Basic SKU with a static allocation
Standard SKU with a static allocation

Explanation:

Subnet size: /26
The recommended subnet size for Azure Bastion is /26 "Subnet size must be /26 or larger (/25, /24 etc.)."
"For host scaling, a /26 or larger subnet is recommended. Using a smaller subnet space limits the number of scale units"
"For Azure Bastion resources deployed on or after November 2, 2021, the minimum AzureBastionSubnet size is /26 or larger (/25, /24, etc.)"

Public IP: Standard SKU with a static allocation
Only Azure Bastion Standard SKU supports 'Host scaling' and 'Upload or download files'. Besides that, Public IP address recommended by Microsoft must be Standard and Static

References:

<https://learn.microsoft.com/en-us/azure/bastion/configuration-settings>
<https://learn.microsoft.com/en-us/azure/bastion/bastion-faq>

Question: 522**CertyIQ**

You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Location
VNet1	West US
VNet2	Central Europe

You need to ensure that all the traffic between VNet1 and VNet2 traverses the Microsoft backbone network.

What should you configure?

- A.a private endpoint
- B.peering
- C.Express Route
- D.a route table

Answer: B**Explanation:**

The traffic between virtual machines in peered virtual networks uses the Microsoft backbone infrastructure. ExpressRoute private peering supports connectivity between multiple virtual networks. Although this behaviour happens by default when linking virtual networks to the same ExpressRoute circuit, Microsoft doesn't recommend this solution. To establish connectivity between virtual networks, VNet peering should be implemented instead for the best performance possible. **Virtual network peering enables you to seamlessly connect two or more Virtual Networks in Azure.** The virtual networks appear as one for connectivity purposes. The traffic between virtual machines in peered virtual networks uses the Microsoft backbone infrastructure. Like traffic between virtual machines in the same network, traffic is routed through Microsoft's private network only.

Reference:

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview>

<https://learn.microsoft.com/en-us/azure/expressroute/virtual-network-connectivity-guidance>

Question: 523**CertyIQ**

You have the Azure virtual networks shown in the following table.

Name	Address space	Subnet	Resource group Azure region
VNet1	10.11.0.0/16	10.11.0.0/17	West US
VNet2	10.11.0.0/17	10.11.0.0/25	West US
VNet3	10.10.0.0/22	10.10.1.0/24	East US
VNet4	192.168.16.0/22	192.168.16.0/24	North Europe

Which virtual networks can you peer with VNet1?

- A.VNet2, VNet3, and VNet4
- B.VNet2 only
- C.VNet3 and VNet4 only
- D.VNet2 and VNet3 only

Answer: C

Explanation:

C:VNet3 and VNet4 only.

VNet3 and VNet4 only (Option C) suggests that these virtual networks are compatible with VNet1 for peering, while the other VNets (VNet2) may have some constraints or conflicts that prevent successful peering with VNet1.

Question: 524

CertyIQ

You have an Azure subscription.

You are creating a new Azure container instance that will have the following settings:

- Container name: cont1
- SKU: Standard
- OS type: Windows
- Networking type: Public
- Memory (GiB): 2.5
- Number of CPU cores: 2

You discover that the Private setting for Networking type is unavailable.

You need to ensure that cont1 can be configured to use private networking.

Which setting should you change?

- A.Memory (GiB)
- B.Networking type
- C.Number of CPU cores
- D.OS type
- E.SKU

Answer: D

Explanation:

To configure an Azure Container Instance (ACI) with private networking, the OS type must be set to Linux, as private networking is not supported for Windows containers in Azure Container Instances.

Azure Container Instances (ACI) supports private networking only for containers running on Linux OS. Changing the OS type from Windows to Linux will allow you to use the private networking type.

Question: 525**CertyIQ**

You have an Azure subscription that has a Recovery Services vault named Vault1. The subscription contains the virtual machines shown in the following table:

Name	Operating system	Auto-shutdown
VM1	Windows Server 2012 R2	Off
VM2	Windows Server 2016	19:00
VM3	Ubuntu Server 18.04 LTS	Off
VM4	Windows 10	19:00

You plan to schedule backups to occur every night at 23:00.

Which virtual machines can you back up by using Azure Backup?

- A. VM1 and VM3 only
- B. VM1, VM2, VM3 and VM4
- C. VM1 and VM2 only
- D. VM1 only

Answer: B**Explanation:**

Azure Backup supports backup of 64-bit Windows server operating system from Windows Server 2008.

Azure Backup supports backup of 64-bit Windows 10 operating system.

Azure Backup supports backup of 64-bit Ubuntu Server operating system from Ubuntu 12.04.

Azure Backup supports backup of VM that are shutdown or offline.

Reference:

<https://docs.microsoft.com/en-us/azure/backup/backup-support-matrix-iaas> <https://docs.microsoft.com/en-us/azure/virtual-machines/linux/endorsed-distros>

Question: 526**CertyIQ****HOTSPOT -**

You create a Recovery Services vault backup policy named Policy1 as shown in the following exhibit:

Policy1

Associated items Delete Save Discard

Backup schedule

- Frequency
- Time
- Timezone

Daily 11:00 PM (UTC) Coordinated Universal Time

Retention range

Retention of daily backup point

• At For Day(s)
11:00 PM 30

Retention of weekly backup point

• On • At For Week(s)
Sunday 11:00 PM 10

Retention of monthly backup point

• On • At For Month(s)
1 11:00 PM 36

Retention of yearly backup point

• In • On • At For Year(s)
March 1 11:00 PM 10

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

The backup that occurs on Sunday, March 1, will be retained for [answer choice].

▼
30 days
10 weeks
36 months
10 years

The backup that occurs on Sunday, November 1, will be retained for [answer choice].

▼
30 days
10 weeks
36 months
10 years

Answer:

Answer Area

The backup that occurs on Sunday, March 1, will be retained for [answer choice].

▼
30 days
10 weeks
36 months
10 years

The backup that occurs on Sunday, November 1, will be retained for [answer choice].

▼
30 days
10 weeks
36 months
10 years

Explanation:

Box 1: 10 years -

The yearly backup point occurs to 1 March and its retention period is 10 years.

Box 2: 36 months -

The monthly backup point occurs on the 1 of every month and its retention period is 36 months.
st

Question: 527

You have the Azure virtual machines shown in the following table:

Name	Azure region
VM1	West Europe
VM2	West Europe
VM3	North Europe
VM4	North Europe

You have a Recovery Services vault that protects VM1 and VM2.

You need to protect VM3 and VM4 by using Recovery Services.

What should you do first?

- A. Create a new Recovery Services vault
- B. Create a storage account
- C. Configure the extensions for VM3 and VM4
- D. Create a new backup policy

Answer: A

Explanation:

A Recovery Services vault is a storage entity in Azure that houses data. The data is typically copies of data, or configuration information for virtual machines (VMs), workloads, servers, or workstations. You can use Recovery Services vaults to hold backup data for various Azure services

Reference:

<https://docs.microsoft.com/en-us/azure/site-recovery/azure-to-azure-tutorial-enable-replicatio>

Question: 528

CertyIQ

HOTSPOT -

You have an Azure subscription that contains an Azure Storage account named storage1 and the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group1

You plan to monitor storage1 and to configure email notifications for the signals shown in the following table.

Name	Type	Users to notify
Ingress	Metric	User1 and User3 only
Egress	Metric	User1 only
Delete storage account	Activity log	User1, User2, and User3
Restore blob ranges	Activity log	User1 and User3 only

You need to identify the minimum number of alert rules and action groups required for the planned monitoring. How many alert rules and action groups should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Alert rules:

1
2
3
4

Action groups:

1
2
3
4

Answer:

Answer Area

Alert rules:

1
2
3
4

Action groups:

1
2
3
4

Explanation:

You can define only one activity log signal per alert rule. To alert on more signals, create another alert rule.

Box 1: 4

You need 1 alert rule per 1 signal (1xIngress, 1xEgress, 1xDelete storage account, 1xRestore blob ranges).

Box 2: 3

You need 3 Action Groups (1xUser1 and User3, 1xUser1 only, 1xUser1 User2 and User3). Check 'Users to notify' column.

Question: 529

CertyIQ

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

Name	Type	Member of
User1	User	None
User2	User	Group1
Principal1	Managed identity	None
Principal2	Managed identity	Group1

User1, Principal1, and Group1 are assigned the Monitoring Reader role.

An action group named AG1 has the Email Azure Resource Manager Role notification type and is configured to email the Monitoring Reader role.

You create an alert rule named Alert1 that uses AG1.

You need to identify who will receive an email notification when Alert1 is triggered.

Who should you identify?

- A. User1 and Principal1 only
- B. User1, User2, Principal1, and Principal2
- C. User1 only
- D. User1 and User2 only

Answer: D

Explanation:

user 1 and user 2 only.

User 2 because its also a member of a group that has the rights

Email Azure Resource Manager

When you use Azure Resource Manager for email notifications, you can send email to the members of a subscription's role. Email is sent to Microsoft Entra ID user or group members of the role. This includes support for roles assigned through Azure Lighthouse.

Note

Action Groups only supports emailing the following roles: Owner, Contributor, Reader, Monitoring Contributor, Monitoring Reader.

<https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/action-groups#email-azure-resource-manager>

Question: 530

CertyIQ

HOTSPOT -

You have an Azure virtual machine named VM1 and a Recovery Services vault named Vault1.

You create a backup policy named Policy1 as shown in the exhibit. (Click the Exhibit tab.)

Policy1

[Associated items](#)[Delete](#)[Save](#)[Discard](#)

Backup schedule

* Frequency

Daily

* Time

2:00 AM

* Timezone

(UTC) Coordinated Universal Time

Retention range

 Retention of daily backup point.

* At

For

2:00 AM

5

Day(s)

 Retention of weekly backup point.

* On

* At

For

Sunday

2:00 AM

20

Week(s)

 Retention of monthly backup point.[Week Based](#)[Day Based](#)

* On

* At

For

2

2:00 AM

24

Month(s)

 Retention of yearly backup point.[Week Based](#)[Day Based](#)

* In

* On

* At

For

January

9

2:00 AM

5

Year(s)

You configure the backup of VM1 to use Policy1 on Thursday, January 1 at 1:00 AM.

You need to identify the number of available recovery points for VM1.

How many recovery points are available on January 8 and January 15? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

January 8 at 2:00 PM (14:00):

5
6
8
9

January 15 at 2:00 PM (14:00):

5
8
17
19

Answer:

Answer Area

January 8 at 2:00 PM (14:00):

5
6
8
9

January 15 at 2:00 PM (14:00):

5
8
17
19

Explanation:

Box 1: 6 -

5 latest daily recovery points, which includes the weekly backup from the previous Sunday, plus the monthly recovery point.

Box 2: 8 -

5 latest daily recovery points, plus two weekly backups, plus the monthly recovery point.

Reference:

<https://social.technet.microsoft.com/Forums/en-US/854ab6ae-79aa-4bad-ac65-471c4d422e94/daily-monthly-yearly-recovery-points-and-storage-used?forum=windowsazureonlinebackup>

Question: 531

CertyIQ

HOTSPOT -

You have the web apps shown in the following table.

Name	Web framework	Hosting environment
App1	Microsoft ASP.NET	An on-premises physical server that runs Windows Server 2019 and has Internet Information Services (IIS) configured
App2	Microsoft ASP.NET Core	An Azure virtual machine that runs Windows Server 2019 and has Internet Information Services (IIS) configured

You need to monitor the performance and usage of the apps by using Azure Application Insights. The solution must minimize modifications to the application code.

What should you do on each app? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

App1:

- Install the Log Analytics agent
- Install the Azure Monitor agent
- Use the Application Insights SDK
- Install the Application Insights Agent

App2:

- Install the Log Analytics agent
- Install the Azure Monitor agent
- Use the Application Insights SDK
- Install the Application Insights Agent

Answer:

Answer Area

App1:

- Install the Log Analytics agent
- Install the Azure Monitor agent
- Use the Application Insights SDK
- Install the Application Insights Agent

App2:

- Install the Log Analytics agent
- Install the Azure Monitor agent
- Use the Application Insights SDK
- Install the Application Insights Agent

Explanation:

Install the Application Insights Agent:

The Application Insights Agent (also known as the Status Monitor) can be installed on servers to monitor applications without modifying the application code. It is particularly useful for monitoring .NET applications running on IIS.

Suitable for monitoring existing applications where modifying the code to include the SDK is not feasible.

Install the Application Insights Agent.

Install this on servers to monitor applications without modifying the code, especially useful for .NET applications on IIS.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/azure-web-apps>

Question: 532

CertyIQ

You have an Azure virtual machine named VM1.

You use Azure Backup to create a backup of VM1 named Backup1.

After creating Backup1, you perform the following changes to VM1:

- ⇒ Modify the size of VM1.
- ⇒ Copy a file named Budget.xls to a folder named Data.
- ⇒ Reset the password for the built-in administrator account.
- ⇒ Add a data disk to VM1.

An administrator uses the Replace existing option to restore VM1 from Backup1.

You need to ensure that all the changes to VM1 are restored.
Which change should you perform again?

- A. Modify the size of VM1.
- B. Reset the password for the built-in administrator account.
- C. Add a data disk.
- D. Copy Budget.xls to Data.

Answer: D

Explanation:

- D. Copy Budget.xls to Data.

When you use the Replace existing option to restore an Azure virtual machine (VM) from a backup, the restoration process will revert the VM to the exact state it was in at the time the backup was created (Backup1). Any changes made to the VM after the backup was created will not be included in the restored VM. Therefore, you need to perform these changes again to ensure they are applied to the restored VM.

Question: 533

CertyIQ

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com that contains the users shown in the following table.

Name	Member of	Role assigned
User1	Group1	<i>None</i>
User2	Group2	<i>None</i>
User3	Group1, Group2	User administrator

You enable password reset for contoso.onmicrosoft.com as shown in the Password Reset exhibit. (Click the Password Reset tab.)

Self service password reset enabled ⓘ

None Selected All

Select group >

Group2

i These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.

You configure the authentication methods for password reset as shown in the Authentication Methods exhibit. (Click the Authentication Methods tab.)

Number of methods required to reset ⓘ

1 2

Methods available to users

- Mobile app notification
- Mobile app code
- Email
- Mobile phone
- Office phone
- Security questions

Number of questions required to register ⓘ

3 4 5

Number of questions required to reset ⓘ

3 4 5

Select security questions

10 security questions selected

i These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements

Yes

No

After User2 answers three security questions correctly, he can reset his password immediately.

If User1 forgets her password, she can reset the password by using the mobile phone app.

User3 can add security questions to the password reset process

Answer:

Statements	Yes	No
After User2 answers three security questions correctly, he can reset his password immediately.	<input type="radio"/>	<input checked="" type="radio"/>
If User1 forgets her password, she can reset the password by using the mobile phone app.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can add security questions to the password reset process	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Box 1: No

Two methods are required (Mobile phone and Security questions).

Box 2: No

Self-service password reset is only enabled for Group2, and User1 is not a member of Group2.

Box 3: No

To be able to add Security questions to the process, you need to be a Global Administrator. User3 is User Administrator, so User3 cannot add security questions to the reset process. User Administrator doesn't have MFA permissions.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/quickstart-sspr>

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/active-directory-passwords-faq>

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr#prerequisites>

<https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#user-administrator>

Question: 534

CertyIQ

Your company has a main office in London that contains 100 client computers.

Three years ago, you migrated to Azure Active Directory (Azure AD).

The company's security policy states that all personal devices and corporate-owned devices must be registered or joined to Azure AD.

A remote user named User1 is unable to join a personal device to Azure AD from a home network.

You verify that User1 was able to join devices to Azure AD in the past.

You need to ensure that User1 can join the device to Azure AD.

What should you do?

- A. Assign the User administrator role to User1.

- B. From the Device settings blade, modify the Maximum number of devices per user setting.
- C. Create a point-to-site VPN from the home network of User1 to Azure.
- D. From the Device settings blade, modify the Users may join devices to Azure AD setting.

Answer: B

Explanation:

The Maximum number of devices setting enables you to select the maximum number of devices that a user can have in Azure AD. If a user reaches this quota, they will not be able to add additional devices until one or more of the existing devices are removed.

Incorrect Answers:

C: Azure AD Join enables users to join their devices to Active Directory from anywhere as long as they have connectivity with the Internet.

D: The Users may join devices to Azure AD setting enables you to select the users who can join devices to Azure AD. Options are All, Selected and None. The default is All.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal> <http://technet.microsoft.com/pros-and-cons-azure-ad-join/>

Question: 535

CertyIQ

HOTSPOT -

You have two Azure App Service app named App1 and App2. Each app has a production deployment slot and a test deployment slot.

The Backup Configuration settings for the production slots are shown in the following table.

App	Backup Every	Start backup schedule from	Retention (Days)	Keep at least one backup
App1	1 Days	January 6, 2021	0	Yes
App2	1 Days	January 6, 2021	30	Yes

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
On January 15, 2021, App1 will have only one backup in storage.	<input type="radio"/>	<input type="radio"/>
On February 6, 2021, you can access the backup of the App2 test slot from January 15, 2021.	<input type="radio"/>	<input type="radio"/>
On January 15, 2021, you can restore the App2 production slot backup from January 6 to the App2 test slot.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
On January 15, 2021, App1 will have only one backup in storage.	<input type="radio"/>	<input checked="" type="radio"/>
On February 6, 2021, you can access the backup of the App2 test slot from January 15, 2021.	<input type="radio"/>	<input checked="" type="radio"/>
On January 15, 2021, you can restore the App2 production slot backup from January 6 to the App2 test slot.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

No - On January 15, 2021, App1 will have only one backup in storage

On January 15th you will have 9 backups as 0 day retention is defined as indefinite.

Retention: Set to 0 for indefinite retention.

No - On February 6, 2021, you can access the backup of the App2 test slot from January 15, 2021

Backup in the questions only includes the production slot. So no backup policy for test slots.

Yes - On January 15, 2021, you can restore the App2 production slot backup from January 6 to the App2 test slot

You can restore the production backup to any slot or new deployment slot

<https://learn.microsoft.com/en-us/azure/app-service/manage-backup?tabs=portal>

Question: 536

CertyIQ

HOTSPOT -

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant is synced to the on-premises Active Directory domain. The domain contains the users shown in the following table.

Name	Role
SecAdmin1	Security administrator
BillAdmin1	Billing administrator
User1	Reports reader

You enable self-service password reset (SSPR) for all users and configure SSPR to have the following authentication methods:

- » Number of methods required to reset: 2
- » Methods available to users: Mobile phone, Security questions
- » Number of questions required to register: 3
- » Number of questions required to reset: 3

You select the following security questions:

- » What is your favorite food?
- » In what city was your first job?
- » What was the name of your first pet?

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
SecAdmin1 must answer the following question during the self-service password reset: In what city was your first job?	<input type="radio"/>	<input type="radio"/>
BillAdmin1 must answer the following question during the self-service password reset: What is your favorite food?	<input type="radio"/>	<input type="radio"/>
User1 must answer the following question during the self-service password reset: What was the name of your first pet?	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
SecAdmin1 must answer the following question during the self-service password reset: In what city was your first job?	<input type="radio"/>	<input checked="" type="radio"/>
BillAdmin1 must answer the following question during the self-service password reset: What is your favorite food?	<input type="radio"/>	<input checked="" type="radio"/>
User1 must answer the following question during the self-service password reset: What was the name of your first pet?	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

NO, NO, YES

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy>

By default, administrator accounts are enabled for self-service password reset, and a strong default two-gate password reset policy is enforced. This policy may be different from the one you have defined for your users, and this policy can't be changed. You should always test password reset functionality as a user without any Azure administrator roles assigned.

With a two-gate policy, administrators don't have the ability to use security questions.

The two-gate policy requires two pieces of authentication data, such as an email address, authenticator app, or a phone number.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment>

Question: 537

CertyIQ

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 subscription that contains the following users in an Azure Active Directory tenant named contoso.onmicrosoft.com:

Name	Role	Scope
User1	Global administrator	Azure Active Directory
User2	Global administrator	Azure Active Directory
User3	User administrator	Azure Active Directory
User4	Owner	Azure Subscription

User1 creates a new Azure Active Directory tenant named external.contoso.onmicrosoft.com.

You need to create new user accounts in external.contoso.onmicrosoft.com.

Solution: You instruct User1 to create the user accounts.

Does that meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Only a global administrator can add users to this tenant.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/organizations/accounts/add-users-to-azure-ad>

Question: 538

CertyIQ

You have an existing Azure subscription that contains 10 virtual machines.

You need to monitor the latency between your on-premises network and the virtual machines.

What should you use?

A. Service Map

B. Connection troubleshoot

C. Network Performance Monitor

D. Effective routes

Answer: C

Explanation:

Network Performance Monitor is a cloud-based hybrid network monitoring solution that helps you monitor network performance between various points in your network infrastructure. It also helps you monitor network connectivity to service and application endpoints and monitor the performance of Azure ExpressRoute.

You can monitor network connectivity across cloud deployments and on-premises locations, multiple data centers, and branch offices and mission-critical multitier applications or microservices. With Performance Monitor, you can detect network issues before users complain.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/insights/network-performance-monitor>

Question: 539

CertyIQ

HOTSPOT -

You have an Azure App Service plan named ASP1. CPU usage for ASP1 is shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

The average CPU percentage is calculated [answer choice] per day

	▼
once	
four times	
six times	
24 times	

ASP1 must be [answer choice] to optimize CPU usage

	▼
scaled up	
scaled down	
scaled out	

Answer:

Answer Area

The average CPU percentage is calculated [answer choice] per day

	▼
once	
four times	
six times	
24 times	

ASP1 must be [answer choice] to optimize CPU usage

	▼
scaled up	
scaled down	
scaled out	

Explanation:

Box 1: four times -

From the exhibit we see that the time granularity is 6 hours: Last 30 days (Automatic - 6 hours).

CPU Percentage Last days Automatic - hours

Box 2: scaled up -

Scale up when:

- * You see that your workloads are hitting some performance limit such as CPU or I/O limits.
- * You need to quickly react to fix performance issues that can't be solved with classic database optimization.
- * You need a solution that allows you to change service tiers to adapt to changing latency requirements.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/metrics-troubleshoot> <https://azure.microsoft.com/>

Question: 540

DRAG DROP -

You have an Azure Linux virtual machine that is protected by Azure Backup.

One week ago, two files were deleted from the virtual machine.

You need to restore the deleted files to an on-premises Windows Server 2016 computer as quickly as possible.

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

Download and run the script to mount a drive on the local computer

Select a restore point that contains the deleted files

From the Azure portal, click **Restore VM from the vault**

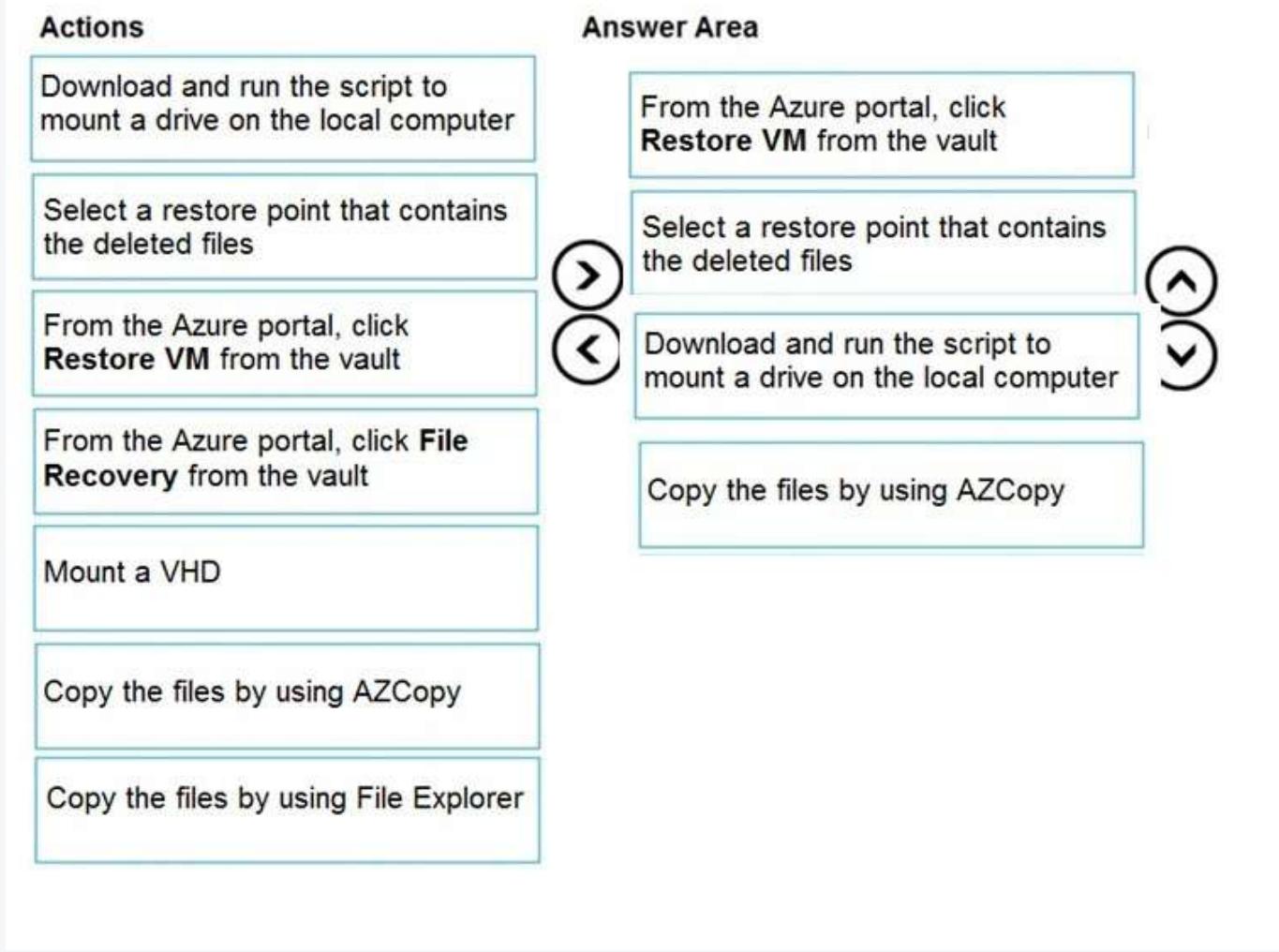
From the Azure portal, click **File Recovery** from the vault

Mount a VHD

Copy the files by using AZCopy

Copy the files by using File Explorer

Answer Area**Answer:**



Explanation:

Step 1: From the Azure portal, click File Recovery from the vault

Step 2. Select a restore point that contains the deleted files

Step 3: Download and run the script to mount a drive on the local computer

Generate and download script to browse and recover files:

Step 4: Copy the files by using AzCopy

To restore files or folders from the recovery point, go to the virtual machine and choose the desired recovery point.

Step 0. In the virtual machine's menu, click Backup to open the Backup dashboard.

Step 1. In the Backup dashboard menu, click File Recovery.

Step 2. From the Select recovery point drop-down menu, select the recovery point that holds the files you want. By default, the latest recovery point is already selected.

Step 3: To download the software used to copy files from the recovery point, click Download Executable (for Windows Azure VM) or Download Script (for Linux

Azure VM, a python script is generated).

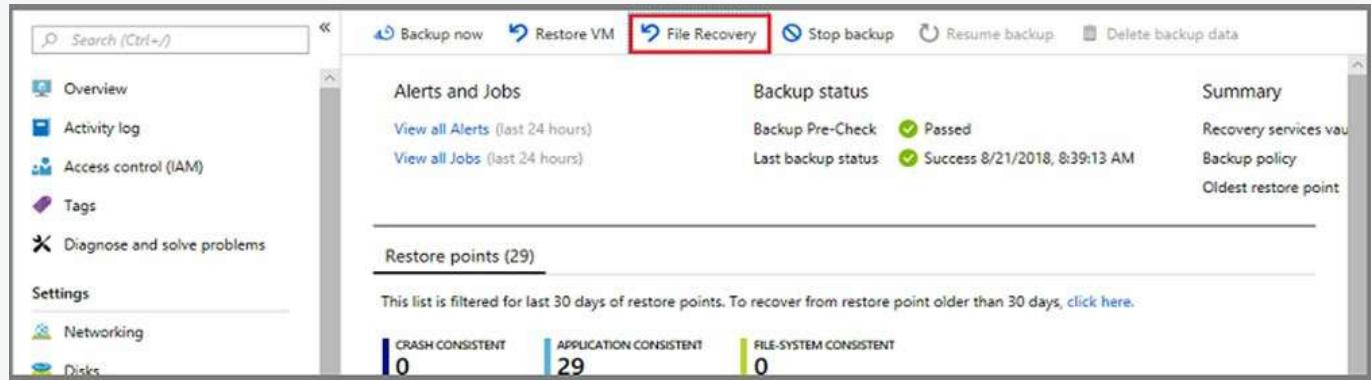
Step 4: Copy the files by using AzCopy

AzCopy is a command-line utility designed for copying data to/from Microsoft Azure Blob, File, and Table storage, using simple commands designed for optimal performance. You can copy data between a file system and a storage account, or between storage accounts.

References:

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-restore-files-from-vm>

<https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy>



The File Recovery menu opens.

File Recovery

myvmh1

✓ Step 1: Select recovery point

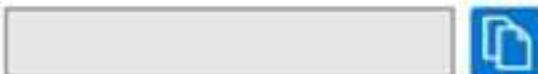
8/2/2020, 11:31:09 AM [Latest] (Cras... ▾)

→ Step 2: Download script to browse and recover files

This script will mount the disks from the selected recovery point **as local drives on the machine where it is run**. These drives will remain mounted for 12 hours.

[Download Script *](#)

Requires password to run



→ Step 3: Unmount the disks after recovery

Unmount disks and close the connection to the recovery point.

[Unmount Disks](#)

Reference:

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-restore-files-from-vm>

Question: 541

HOTSPOT -

You purchase a new Azure subscription named Subscription1.

You create a virtual machine named VM1 in Subscription1. VM1 is not protected by Azure Backup.

You need to protect VM1 by using Azure Backup. Backups must be created at 01:00 and stored for 30 days.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Location in which to store the backups:

- A blob container
- A file share
- A Recovery Services vault
- A storage account

Object to use to configure the protection for VM1:

- A backup policy
- A batch job
- A batch schedule
- A recovery plan

Answer:

Answer Area

Location in which to store the backups:

- A blob container
- A file share
- A Recovery Services vault
- A storage account

Object to use to configure the protection for VM1:

- A backup policy
- A batch job
- A batch schedule
- A recovery plan

Explanation:

Box 1: A Recovery Services vault

You can set up a Recovery Services vault and configure backup for multiple Azure VMs.

Box 2: A backup policy -

In Choose backup policy, do one of the following:

- ⇒ Leave the default policy. This backs up the VM once a day at the time specified, and retains backups in the vault for 30 days.
- ⇒ Select an existing backup policy if you have one.
- ⇒ Create a new policy, and define the policy settings.

Reference:

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-vms-first-look-arm>

CertyIQ**Question: 542**

You have an Azure virtual machine named VM1.

Azure collects events from VM1.

You are creating an alert rule in Azure Monitor to notify an administrator when an error is logged in the System event log of VM1.

Which target resource should you monitor in the alert rule?

- A. virtual machine extension
- B. virtual machine
- C. metric alert
- D. Azure Log Analytics workspace

Answer: D**Explanation:**

For the first step to create the new alert rule, under the Create Alert section, you are going to select your Log Analytics workspace as the resource, since this is a log based alert signal.

Reference:

<https://docs.microsoft.com/en-us/windows-server/storage/storage-spaces/configure-azure-monitor>

CertyIQ**Question: 543**

You have an Azure subscription that contains 100 virtual machines.

You regularly create and delete virtual machines.

You need to identify unattached disks that can be deleted.

What should you do?

- A. From Azure Cost Management, view Cost Analysis
- B. From Azure Advisor, modify the Advisor configuration
- C. From Microsoft Azure Storage Explorer, view the Account Management properties
- D. From Azure Cost Management, view Advisor Recommendations

Answer: D**Explanation:**

From Home "> Cost Management + Billing "> Cost Management, scroll down on the options and select View Recommendations:

Cost Management: Subscription

Search (Ctrl+I) Try preview Go to Cloudyn Help

- Overview
- Access control
- Diagnose and solve problems
- Cost Management
 - Cost analysis
 - Cost alerts
 - Budgets
 - Advisor recommendations
 - Cloudyn
- Products + services
 - Azure subscriptions
 - Azure reservations
- Settings
 - Configuration
 - Exports
 - Connectors for AWS (Preview)
- Support + troubleshooting

Analyze cloud costs
Break down and analyze costs to identify anomalies and drive a deeper understanding of cost and usage patterns.
[Learn more](#)

Monitor with budgets
Create a budget to control costs and configure alerts to warn teams about impending budget overages.
[Learn more](#)

Open cost analysis **Create budget**

Optimize with recommendations
View Advisor recommendations to identify unused or underutilized resources. Take action to reduce waste.
[Learn more](#)

View recommendations

Azure Cost Management / Advisor -

From here you will see the recommendations for your subscription, if you have orphaned disks, they will be listed.

Reference:

<https://codeserendipity.com/2020/07/08/microsoft-azure-find-unattached-disks-that-can-be-deleted-and-other-recommendations/>

Question: 544

CertyIQ

You have an Azure web app named webapp1.

Users report that they often experience HTTP 500 errors when they connect to webapp1.

You need to provide the developers of webapp1 with real-time access to the connection errors. The solution must provide all the connection error details.

What should you do first?

- A. From webapp1, enable Web server logging
- B. From Azure Monitor, create a workbook
- C. From Azure Monitor, create a Service Health alert
- D. From webapp1, turn on Application Logging

Answer: A

Explanation:

Raw HTTP request data is provided by Web server logging and the question mentions 500 error codes.

You need to catch connection error. When the connection fails it happens on web server, not within application. You can do it opening the web application -> Application Service logs -> Web server logging (there are multiple switches there).

You can also see the errors live going to "Log stream" pane.

Web server logging Windows App Service file system or Azure Storage blobs Raw HTTP request data in the W3C extended log file format. Each log message includes data such as the HTTP method, resource URI, client IP, client port, user agent, response code, and so on.

Question: 545

You have an Azure web app named App1.
You need to monitor the availability of App1 by using a multi-step web test.
What should you use in Azure Monitor?

- A. Azure Service Health
- B. Azure Application Insights
- C. the Diagnostic settings
- D. metrics

Answer: B**Explanation:**

Upload the web test -

1. In the Application Insights portal on the Availability pane select Add Classic test, then select Multi-step as the SKU.
2. Upload your multi-step web test.
3. Set the test locations, frequency, and alert parameters.
4. Select Create.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/availability-multistep>

Question: 546

HOTSPOT -

You have an Azure subscription that has diagnostic logging enabled and is configured to send logs to a Log Analytics workspace.

You are investigating a service outage.

You need to view the event time, the event name, and the affected resources.

How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

AzureActivity
Heartbeat
NetworkMonitoring
Perf

```
| Where Level == 'Critical'
```

extend
join
print
project

```
TimeGenerated, OperationNameValue, _ResourceId
```

Answer:

Answer Area

AzureActivity
Heartbeat
NetworkMonitoring
Perf

```
| Where Level == 'Critical'
```

extend
join
print
project

```
TimeGenerated, OperationNameValue, _ResourceId
```

Explanation:

Box 1: AzureActivity -

The AzureActivity table has entries from the Azure activity log, which provides insight into subscription-level or management group-level events occurring in Azure.

Let's see only Critical entries during a specific week.

The where operator is common in the Kusto Query Language. where filters a table to rows that match specific criteria. The following example uses multiple commands. First, the query retrieves all records for the table.

Then, it filters the data for only records that are in the time range. Finally, it filters those results for only records that have a Critical level.

AzureActivity -

```
| where TimeGenerated > datetime(10-01-2020) and TimeGenerated < datetime(10-07-2020)  
| where Level == 'Critical'
```

Incorrect:

not Perf: The Perf table has performance data that's collected from virtual machines that run the Log Analytics agent.

Box 2: | project -

Select a subset of columns: project.

Use project to include only the columns you want. Building on the preceding example, let's limit the output to certain columns:

AzureActivity -

```
| where TimeGenerated > datetime(10-01-2020) and TimeGenerated < datetime(10-07-2020)
```

```
| where Level == 'Critical'
```

```
| project TimeGenerated, Level, OperationNameValue, ResourceGroup, _ResourceId
```

Reference:

<https://github.com/MicrosoftDocs/dataexplorer-docs/blob/main/data-explorer/kusto/query/tutorial.md>

Question: 547

CertyIQ

You have a Recovery Services vault named RSV1. RSV1 has a backup policy that retains instant snapshots for five days and daily backup for 14 days.

RSV1 performs daily backups of VM1. VM1 hosts a static website that was updated eight days ago.

You need to recover VM1 to a point eight days ago. The solution must minimize downtime.

What should you do first?

- A. Deallocate VM1.
- B. Restore VM1 by using the Replace existing restore configuration option.
- C. Delete VM1.
- D. Restore VM1 by using the Create new restore configuration option.

Answer: D

Explanation:

D. Restore VM1 by using the Create new restore configuration option.

This option allows you to keep the existing VM running while restoring a new instance, minimizing downtime for your static website.

Question: 548

CertyIQ

HOTSPOT -

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

Name	Type
VM1	Virtual machine
storage1	Storage account
Workspace1	Log Analytics workspace
DB1	Azure SQL database

You plan to create a data collection rule named DCR1 in Azure Monitor.

Which resources can you set as data sources in DCR1, and which resources can you set as destinations in DCR1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Data sources:

- VM1 only
- VM1 and storage1 only
- VM1, storage1, and DB1 only
- VM1, storage1, Workspace1, and DB1

Destinations:

- storage1 only
- Workspace1 only
- Workspace1 and storage1 only
- Workspace1, storage1, and DB1 only

Answer:

Answer Area

Data sources:

VM1 only
VM1 and storage1 only
VM1, storage1, and DB1 only
VM1, storage1, Workspace1, and DB1

Destinations:

storage1 only
Workspace1 only
Workspace1 and storage1 only
Workspace1, storage1, and DB1 only

Explanation:

Box 1: VM1 only -

A virtual machine may have an association to multiple DCRs, and a DCR may have multiple virtual machines associated to it.

In the Resources tab, add the resources (virtual machines, virtual machine scale sets, Arc for servers) that should have the Data Collection Rule applied.

Box 2: Workspace1 only -

On the Destination tab, add one or more destinations for the data source. You can select multiple destinations of same or different types, for instance multiple Log Analytics workspaces (i.e. "multi-homing").

Note: The Data Collection Rules (or DCR) improve on a few key areas of data collection from VMs including like better control and scoping of data collection (e.g. collect from a subset of VMs for a single workspace), collect once and send to both Log Analytics and Azure Monitor Metrics, send to multiple workspaces (multi-homing for Linux), improved Windows event filtering, and improved extension management.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/agents/data-collection-rule-azure-monitor-agent>

Question: 549

CertyIQ

HOTSPOT -

You have the role assignment file shown in the following exhibit.

```

[

    {
        "RoleAssignmentId": "e3108585-0e5d-4572-91a3-aa5d2df73999",
        "Scope": "/subscriptions/fb960108-fcdc-499b-886e-d9c31d3f26ff",
        "DisplayName": "User1",
        "SignInName": "User1@contoso.onmicrosoft.com",
        "RoleDefinitionName": "Owner",
        ...
    },
    {
        "RoleAssignmentId": "3bab4763-16a9-4d5d-9fcf-e0cc31a21e",
        "Scope": "/subscriptions/fb960108-fcdc-499b-886e-d9c31d3f26ff/resourceGroups/RG2",
        "DisplayName": "User2",
        "SignInName": "User2@contoso.onmicrosoft.com",
        "RoleDefinitionName": "Owner",
        ...
    },
    {
        "RoleAssignmentId": "a071c023-40a3-4b7f-8680-1109b40270c5",
        "Scope": "/subscriptions/fb960108-fcdc-499b-886e-d9c31d3f26ff/resourceGroups/RG1/providers/Microsoft.Compute/virtualMachines/VM1",
        "DisplayName": "User3",
        "SignInName": "User3@contoso.onmicrosoft.com",
        "RoleDefinitionName": "Owner",
        ...
    },
    {
        "RoleAssignmentId": "c5b9e7da-76d4-4888-93b5-8afb2bb780b4",
        "Scope": "/subscriptions/fb960108-fcdc-499b-886e-d9c31d3f26ff/resourceGroups/RG1",
        "DisplayName": "User4",
        "SignInName": "User4@contoso.onmicrosoft.com",
        "RoleDefinitionName": "Contributor",
        ...
    }
]

```

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

[Answer choice] assigned the Owner role for VM1

▼
User3 is
User3 and User4 are
User1 and User3 are
User1, User3, and User4 are
User1, User2, User3, and User4

[Answer choice] can create a virtual machine in RG1

▼
User1 and User4
User1, User2, and User3
User1, User2, and User4
User1, User3, and User4
User1, User2, User3, and User4

Answer:

Answer Area

[Answer choice] assigned the Owner role for VM1

▼
User3 is
User3 and User4 are
User1 and User3 are
User1, User3, and User4 are
User1, User2, User3, and User4

[Answer choice] can create a virtual machine in RG1

▼
User1 and User4
User1, User2, and User3
User1, User2, and User4
User1, User3, and User4
User1, User2, User3, and User4

Explanation:

Box1: Owner of VM1 - User1 andUser3 are.

Box2 : Create VM in RG1 - User1 and User4.

User1 - Owner of the subscription. (He can manage any resources in the subscription.)

User 2 - Owner of RG2(He can manage any resources in the RG2.)

User 3 - Owner of a single VM that is VM1.(he can manage VM1 only)

User 4 - Contributor of RG1.(He can manage everything in RG1, even he can delete VMs in RG1. But cannot change RABC)

Question: 550

CertyIQ

HOTSPOT -

You have the following custom role-based access control (RBAC) role.

```
{
  "id": "b988327b-7dae-4d00-8925-1cc14fd68be4",
  "properties": {
    "roleName": "Role1",
    "description": "",
    "assignableScopes": [
      "/subscriptions/c691ad84-99f2-42fd-949b-58af7ef6ab3"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Resources/subscription/resourceGroups/resources/read",
          "Microsoft.Resources/subscription/resourceGroups/read",
          "Microsoft.Resourcehealth/*",
          "Microsoft.Authorization/*/read",
          "Microsoft.Compute/*/read",
          "Microsoft.Support/*",
          "Microsoft.Authorization/*/read",
          "Microsoft.Network/virtualNetworks/read",
          "Microsoft.Resources/deployments/*",
          "Microsoft.Resources/subscription/resourceGroups/read",
          "Microsoft.Storage/storageAccounts/read",
          "Microsoft.Compute/virtualMachines/start/action",
          "Microsoft.Compute/virtualMachines/powerOff/action",
          "Microsoft.Compute/virtualMachines/deallocate/action",
          "Microsoft.Compute/virtualMachines/restart/action",
          "Microsoft.Compute/virtualMachines/*",
          "Microsoft.Compute/disks/*",
          "Microsoft.Compute/availabilitySets/*",
          "Microsoft.Network/virtualNetworks/subnets/join/action",
          "Microsoft.Network/virtualNetworks/subnets/read",
          "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
          "Microsoft.Network/networkInterfaces/*",
          "Microsoft.Compute/snapshots/*"
        ]
      },
      {
        "notAction": [
          "Microsoft.Authorization/*/Delete",
          "Microsoft.Authorization/*/Write",
          "Microsoft.Authorization/elevateAccess/Action"
        ]
      }
    ]
  }
}
```

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements

Yes	No
-----	----

Users that are assigned Role1 can assign Role1 to users.

<input type="radio"/>	<input type="radio"/>
-----------------------	-----------------------

Users that are assigned Role1 can deploy new virtual machines.

<input type="radio"/>	<input type="radio"/>
-----------------------	-----------------------

Users that are assigned Role1 can set a static IP address on a virtual machine.

<input type="radio"/>	<input type="radio"/>
-----------------------	-----------------------

Answer:

Answer Area

Statements	Yes	No
Users that are assigned Role1 can assign Role1 to users.	<input type="radio"/>	<input checked="" type="radio"/>
Users that are assigned Role1 can deploy new virtual machines.	<input checked="" type="radio"/>	<input type="radio"/>
Users that are assigned Role1 can set a static IP address on a virtual machine.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Microsoft.Compute/virtualMachines/* Perform all virtual machine actions including create, update, delete, start, restart, and power off virtual machines. Execute scripts on virtual machines.

No, yes, yes.

If you look at the virtual machine contributor built-in role which allows you to "Create and manage virtual machines, ..." (<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-contributor>), you'll see that it does only have "resourceGroups/read" permission.

Question: 551

CertyIQ

HOTSPOT -

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

Name	Type	Description
VNET1	Virtual network	Contains subnet1 and subnet2
subnet1	Subnet	IP address space 10.3.0.0/24
subnet2	Subnet	IP address space 10.4.0.0/24
NSG1	Network security group (NS)	None
vm1	Virtual machine	IP address 10.3.0.15
vm2	Virtual machine	IP address 10.4.0.16
storage1	Storage account	None

NSG1 is configured as shown in the following exhibit.

[^ Essentials](#)

JSON View

Resource group (change) : RG1

Custom security rules : 1 inbound, 2 outbound

Location : East US 2

Associated with : 1 subnets, 0 network interfaces

Subscription (change) : Microsoft Azure Sponsorship

Subscription ID :

Tags (change) : Click here to add tags

▼ Inbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
110	HTTPS_VM1_Deny	443	TCP	Internet	10.3.0.15	<input checked="" type="checkbox"/> Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	<input checked="" type="checkbox"/> Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	<input checked="" type="checkbox"/> Allow
65500	DenyAllInBound	Any	Any	Any	Any	<input checked="" type="checkbox"/> Deny

▼ Outbound security rules

145	Storage_Access	443	TCP	VirtualNetwork	Storage	<input checked="" type="checkbox"/> Allow
150	Block_Internet	Any	Any	VirtualNetwork	Internet	<input checked="" type="checkbox"/> Deny
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	<input checked="" type="checkbox"/> Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	<input checked="" type="checkbox"/> Allow
65500	DenyAllOutBound	Any	Any	Any	Any	<input checked="" type="checkbox"/> Deny

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area**Statements**

VM1 can access storage1.

 Yes No

VM2 can access VM1 by using the HTTPS protocol.

 Yes No

The security rules for NSG1 apply to any virtual machine on VNET1.

 Yes No**Answer:****Answer Area****Statements**

VM1 can access storage1.

 Yes No

VM2 can access VM1 by using the HTTPS protocol.

 Yes No

The security rules for NSG1 apply to any virtual machine on VNET1.

 Yes No**Explanation:**

YES - VM1 can access to storage1 with the rule 145 from Outbound Security Rules

YES - When traffic is outbound from VMs, always we are checking Outbound Rules not Inbound Security Rules. Default rule 65000 allow that

NO- this NSG1 is associated with 1 subnet in our case Subnet 1 because there are rules for VM1

<https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#default-security-rules>

Question: 552

CertyIQ

You have an Azure subscription named Subscription1 that contains two Azure virtual networks named VNet1 and VNet2. VNet1 contains a VPN gateway named VPNGW1 that uses static routing. There is a site-to-site VPN connection between your on-premises network and VNet1.

On a computer named Client1 that runs Windows 10, you configure a point-to-site VPN connection to VNet1. You configure virtual network peering between VNet1 and VNet2. You verify that you can connect to VNet2 from the on-premises network. Client1 is unable to connect to VNet2.

You need to ensure that you can connect Client1 to VNet2.

What should you do?

- A. Select Use the remote virtual network's gateway or Route Server on VNet1 to VNet2 peering.
- B. Select Use the remote virtual network's gateway or Route Server on VNet2 to VNet1 peering.
- C. Download and re-install the VPN client configuration package on Client1.
- D. Enable BGP on VPNGW1.

Answer: C

Explanation:

C. Download and re-install the VPN client configuration package on Client1.

If you make a change to the topology of your network and have Windows VPN clients, the VPN client package for Windows clients must be downloaded and installed again.

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-point-to-site-routing>

Question: 553

CertyIQ

HOTSPOT -

You have two Azure subscriptions named Sub1 and Sub2. Sub1 is in a management group named MG1. Sub2 is in a management group named MG2.

You have the resource groups shown in the following table.

Name	Subscription
RG1	Sub1
RG2	Sub2

You have the virtual machines shown in the following table.

Name	Resource group
VM1	RG1
VM2	RG2
VM3	RG2

You assign roles to users as shown in the following table.

User	Role	Resource
User1	Virtual Machine Contributor	MG1
User1	Virtual Machine User Login	Sub2
User2	Virtual Machine Contributor	MG2
User2	Virtual Machine User Login	Sub1
User2	Virtual Machine User Login	VM3

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 can sign in to VM1.	<input type="radio"/>	<input type="radio"/>
User2 can manage disks and disk snapshots of VM1.	<input type="radio"/>	<input type="radio"/>
User2 can manage disks and disk snapshots of VM3.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 can sign in to VM1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can manage disks and disk snapshots of VM1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can manage disks and disk snapshots of VM3.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

1. User1 can sign in to VM1

No

User1 is assigned as Virtual Machine Contributor in MG1.

And Virtual Machine Contributor can't log in to VM as a regular user.

2. User2 can manage disks and disk snapshots of VM1

No

Since User2 only has Virtual Machine User in Sub1, so he can log in to VM1 but can't manage disks or snapshots

3. User2 can manage disks and disk snapshots of VM3

No

Virtual Machine Contributor only has permission to manage disks, but not disk snapshots (Disk Snapshot Contributor permission)

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-contributor>

Question: 554

CertyIQ

You have an Azure Active Directory (Azure AD) tenant that is linked to 10 Azure subscriptions.

You need to centrally monitor user activity across all the subscriptions.

What should you use?

- A. Azure Application Insights Profiler
- B. access reviews
- C. Activity log filters

D. a Log Analytics workspace

Answer: D

Explanation:

To centrally monitor user activity across all the Azure subscriptions, you should use a Log Analytics workspace. The Azure Activity Log, which is available in the Log Analytics workspace, allows you to view and analyze activity logs from Azure resources, including Azure AD, across all the subscriptions linked to your Azure AD tenant.

Question: 555

CertyIQ

DRAG DROP -

You have an Azure subscription that contains a virtual machine name VM1.

VM1 has an operating system disk named Disk1 and a data disk named Disk2.

You need to back up Disk2 by using Azure Backup.

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

Answer Area

Configure a managed identity



Create an Azure Backup vault

Create a Recovery Services vault

Delegate permissions for the vault

Create a backup policy and configure the backup

Answer:

Actions

Answer Area

Create an Azure Backup vault

Create a backup policy and configure the backup

Create a Recovery Services vault

Configure a managed identity

Delegate permissions for the vault

Explanation:

1. Create an Azure Backup Vault.

This refers to creating a Recovery Services vault specifically for Azure Backup. The steps are the same as creating a Recovery Services vault.

2. Create a Backup Policy and Configure the Backup.

Purpose: A backup policy defines how often backups are taken and how long they are retained. Configuring the backup involves applying this policy to specific resources (e.g., VMs, databases).

Steps:

Go to the Recovery Services vault.

Create a new backup policy or use an existing one.

Assign the policy to the resources you want to back up.

3. Configure a Managed Identity.

Purpose: A managed identity is used to grant the Recovery Services vault the necessary permissions to access and back up resources.

Steps:

Enable a system-assigned or user-assigned managed identity for the resource (e.g., a VM).

Assign the managed identity the appropriate role (e.g., Backup Contributor) in the Recovery Services vault.

Question: 556

CertyIQ

You have a subnet named Subnet1 that contains Azure virtual machines. A network security group (NSG) named NSG1 is associated to Subnet1. NSG1 only contains the default rules.

You need to create a rule in NSG1 to prevent the hosts on Subnet1 from connecting to the Azure portal. The hosts must be able to connect to other internet hosts.

To what should you set Destination in the rule?

- A. Application security group
- B. IP Addresses
- C. Service Tag
- D. Any

Answer: C

Explanation:

You can use service tags to achieve network isolation and protect your Azure resources from the general Internet while accessing Azure services that have public endpoints. Create inbound/outbound network security group rules to deny traffic to/from Internet and allow traffic to/from AzureCloud or other available service tags of specific Azure services.

<https://docs.microsoft.com/en-us/azure/virtual-network/service-tags-overview>

Question: 557

CertyIQ

You have an Azure subscription named Subscription1 that contains an Azure Log Analytics workspace named Workspace1.

You need to view the error events from a table named Event.

Which query should you run in Workspace1?

- A. search in (Event) "error"
- B. Event | where EventType is "error"

- C. select * from Event where EventType == "error"
D. Get-Event Event | where \$_.EventType == "error"

Answer: A

Explanation:

1. Event | search "error"
2. Event | where EventType == "error"
3. search in (Event) "error"

Question: 558

CertyIQ

You have an Azure App Service web app named App1.
You need to collect performance traces for App1.
What should you use?

- A. Azure Application Insights Profiler
- B. the Activity log
- C. the Deployment center
- D. the Diagnose and solve problems settings

Answer: A

Explanation:

With Application Insights Profiler, you can capture and view performance traces for your application in all these dynamic situations, automatically at-scale, without negatively affecting your end users."

<https://docs.microsoft.com/en-us/azure/azure-monitor/profiler/profiler-overview>

Question: 559

CertyIQ

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

Name	Kind	Location
storage1	StorageV2	Central US
storage2	BlobStorage	West US
storage3	BlockBlobStorage	West US
storage4	FileStorage	East US

You deploy a web app named App1 to the West US Azure region.

You need to back up App1. The solution must minimize costs.

Which storage account should you use as the target for the backup?

- A. storage1
- B. storage2
- C. storage3
- D. storage4

Answer: B

Explanation:

To minimize costs, you should use the storage account that is in the same region as the web app that you are backing up. In this case, the web app is in the West US region, so you should use storage2.

Azure Blob storage is generally considered to be the more cost-effective option for storing backups of a web app.

Azure Blob storage has several different storage tiers, including Hot, Cool, and Archive, each with different pricing models. The Cool storage tier is designed for infrequent access data and has the lowest storage costs. This makes it the most cost-effective option for storing backups of a web app.

Question: 560

CertyIQ

HOTSPOT

-

You have an Azure subscription that is linked to an Azure AD tenant. The tenant contains two users named User1 and User2.

The subscription contains the resources shown in the following table.

Name	Type	Description
RG1	Resource group	None
VM1	Virtual machine	Created in RG1

The subscription contains the alert rules shown in the following table.

Name	Scope	Condition
Alert1	RG1	All Administrative operations
Alert2	VM1	All Administrative operations

The users perform the following action:

- User1 creates a new virtual disk and attaches the disk to VM1
- User2 creates a new resource tag and assigns the tag to RG1 and VM1

Which alert rules are triggered by each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User1:

- No alert is triggered
- Only Alert1 is triggered
- Only Alert2 is triggered
- Alert1 and Alert2 are triggered

User2:

- No alert is triggered
- Only Alert1 is triggered
- Only Alert2 is triggered
- Alert1 and Alert2 are triggered

Answer:

Answer Area

User1:

- No alert is triggered
- Only Alert1 is triggered
- Only Alert2 is triggered
- Alert1 and Alert2 are triggered**

User2:

- No alert is triggered
- Only Alert1 is triggered
- Only Alert2 is triggered
- Alert1 and Alert2 are triggered**

Explanation:

User1: Alert1 and Alert2 are triggered.

User2 : Alert1 and Alert2 are triggered.

User1 operations:

- Microsoft.Compute/virtualMachines/write (on the VM itself, triggering Alert2)
- Microsoft.Compute/disks/write (on the RG, triggering Alert1)

User2 Operations:

Microsoft.Resources/tags/write (on the RG, triggering Alert1)

Microsoft.Resources/tags/write (on the VM, triggering Alert2)

<https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log-schema#administrative-category>

Question: 561

CertyIQ

You plan to deploy several Azure virtual machines that will run Windows Server 2019 in a virtual machine scale set by using an Azure Resource Manager template.

You need to ensure that NGINX is available on all the virtual machines after they are deployed.

What should you use?

- A. a Desired State Configuration (DSC) extension
- B. the New-AzConfigurationAssignment cmdlet
- C. Azure Application Insights
- D. a Microsoft Endpoint Manager device configuration profile

Answer: A**Explanation:**

- A. a Desired State Configuration (DSC) extension.

Desired State Configuration (DSC) extension is a PowerShell-based configuration management solution that ensures all virtual machines in a Virtual Machine Scale Set (VMSS) are configured consistently.

You can use the DSC extension to install and configure NGINX automatically on all the virtual machines after they are deployed.

DSC ensures that if any VM instance is replaced (which can happen in a scale set), the new instance will also have NGINX installed as per the defined configuration.

Question: 562

CertyIQ

You have an Azure subscription that contains eight virtual machines and the resources shown in the following table.

Name	Description
storage1	Storage account
storage2	Storage account
KeyVault1	Key vault
VNET1	Virtual network with a single subnet that has five virtual machines connected
VNET2	Virtual network with a single subnet that has three virtual machines connected

You need to configure access for VNET1. The solution must meet the following requirements:

- The virtual machines connected to VNET1 must be able to communicate with the virtual machines connected to VNET2 by using the Microsoft backbone.
- The virtual machines connected to VNET1 must be able to access storage1, storage2, and Azure AD by using the Microsoft backbone.

What is the minimum number of service endpoints you should add to VNET1?

- A. 1

- B. 2
- C. 3
- D. 5

Answer: B

Explanation:

<https://learn.microsoft.com/en-us/azure/storage/common/storage-account-overview#standard-endpoints>

A standard service endpoint in Azure Storage includes the protocol (HTTPS is recommended), the storage account name as the subdomain, and a fixed domain that includes the name of the service.

2 service endpoints. VM is not a service endpoint type. So the first question is irrelevant.

Both storage accounts must have service endpoints in vnet 1. So the answer 2

CertyIQ

Question: 563

You need to configure an Azure web app named contoso.azurewebsites.net to host www.contoso.com.

What should you do first?

- A. Create A records named www.contoso.com and asuid.contoso.com.
- B. Create a TXT record named asuid that contains the domain verification ID.
- C. Create a CNAME record named asuid that contains the domain verification ID.
- D. Create a TXT record named www.contoso.com that has a value of contoso.azurewebsites.net.

Answer: B

Explanation:

TXT record is always first. This step is the proof you actually own the domain and TXT record is needed to verify this.

<https://learn.microsoft.com/en-us/azure/app-service/app-service-web-tutorial-custom-domain?tabs=a%2Cazurecli>

CertyIQ

Question: 564

You have an Azure subscription that contains 10 network security groups (NSGs), 10 virtual machines, and a Log Analytics workspace named Workspace1. Each NSG is connected to a virtual machine.

You need to configure an Azure Monitor Network Insights alert that will be triggered when suspicious network traffic is detected.

What should you do first?

- A. Deploy Connection Monitor.
- B. Configure data collection endpoints.
- C. Configure a private link.
- D. Configure NSG flow logs.

Answer: D

Explanation:

To configure an Azure Monitor Network Insights alert that will be triggered when suspicious network traffic is detected, you should first configure NSG flow logs.

NSG flow logs provide information about traffic that is allowed or denied by an NSG. By configuring NSG flow logs, you will be able to monitor the traffic passing through your NSGs and detect any suspicious activity.

Question: 565

CertyIQ

HOTSPOT

-

You have an Azure subscription named Sub1 that contains the resources shown in the following table.

Name	Description
RG1	Resource group
Action1	Action group that sends an email message to admin1@contoso.com

Sub1 contains the following alert rule:

- Name: Alert1
- Scope: All resource groups in Sub1
- o Include all future resources
- Condition: All administrative operations
- Actions: Action1

Sub1 contains the following alert processing rule:

- Name: Rule1
- Scope: Sub1
- Rule type: Suppress notifications
- Apply the rule: On a specific time
 - o Start: August 10, 2022
 - o End: August 13, 2022

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Statements	Yes	No
If you create a resource group in Sub1 on August 11, 2022, Alert1 is listed in the Azure portal.	<input type="radio"/>	<input type="radio"/>
If you create a resource group in Sub1 on August 12, 2022, an email message is sent to admin1@contoso.com.	<input type="radio"/>	<input type="radio"/>
If you add a tag to RG1 on August 15, 2022, an email message is sent to admin1@contoso.com.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
If you create a resource group in Sub1 on August 11, 2022, Alert1 is listed in the Azure portal.	<input checked="" type="radio"/>	<input type="radio"/>
If you create a resource group in Sub1 on August 12, 2022, an email message is sent to admin1@contoso.com.	<input type="radio"/>	<input checked="" type="radio"/>
If you add a tag to RG1 on August 15, 2022, an email message is sent to admin1@contoso.com.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

YES - "alert is listed" does not mean a notification in my understanding therefore yes

NO- The date is within suppression rule boundaries therefore email will be suppressed

YES - The date is outside suppression rule boundaries

CertyIQ

Question: 566

You have an Azure subscription that contains a storage account named storage1 in the North Europe Azure region.

You need to ensure that when blob data is added to storage1, a secondary copy is created in the East US region. The solution must minimize administrative effort.

What should you configure?

- A. operational backup
- B. object replication
- C. geo-redundant storage (GRS)
- D. a lifecycle management rule

Answer: B

Explanation:

Object replication is a feature that allows you to replicate data, such as blobs, across different storage accounts or containers within the same storage account. This can be configured to automatically copy data from one storage location to another, either within the same region or across different regions. Object replication can be used to create disaster recovery solutions or to distribute data globally for better performance and availability.

It is similar to GRS but it is more flexible as you can choose the storage account and container to replicate the data.

The GRS of a North Europe region is a secondary copy of the data stored in a different region. The exact location of the secondary region will depend on the specific Azure region you have selected. For the North Europe region, the secondary copy is stored in the West Europe region. This means that if there is an outage or disaster in the North Europe region, your data will still be available in the West Europe region. This provides a high level of data durability and protection.

CertyIQ

Question: 567

You have an Azure subscription that contains two Log Analytics workspaces named Workspace1 and Workspace2 and 100 virtual machines that run Windows Server.

You need to collect performance data and events from the virtual machines. The solution must meet the following requirements:

- Logs must be sent to Workspace1 and Workspace 2.
- All Windows events must be captured.
- All security events must be captured.

What should you install and configure on each virtual machine?

- A. the Azure Monitor agent
- B. the Windows Azure diagnostics extension (WAD)
- C. the Windows VM agent

Answer: A

Explanation:

<https://learn.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview>

Azure Monitor Agent (AMA) collects monitoring data from the guest operating system of Azure and hybrid virtual machines and delivers it to Azure Monitor for use by features, insights, and other services, such as Microsoft Sentinel and Microsoft Defender for Cloud. Azure Monitor Agent replaces all of Azure Monitor's legacy monitoring agents.

Question: 568

CertyIQ

You have an Azure subscription that contains a virtual machine named VM1 and an Azure function named App1.

You need to create an alert rule that will run App1 if VM1 stops.

What should you create for the alert rule?

- A. an application security group
- B. a security group that has dynamic device membership
- C. an action group
- D. an application group

Answer: C

Explanation:

An action group is a collection of actions that are triggered by an Azure alert. In this scenario, you need to create an alert rule that will run App1 if VM1 stops, and for this purpose, you need to create an action group. An action group defines the set of actions to be taken when an alert is triggered, such as running an Azure function, sending an email, or creating an Azure ticket.

By creating an action group and associating it with the alert rule, you can automate the process of running App1 if VM1 stops, without the need for manual intervention. This helps ensure that critical systems, such as App1, are automatically activated when necessary, improving the overall reliability and availability of your Azure services.

Question: 569

CertyIQ

You have an Azure subscription that contains a virtual network named VNet1.

VNet1 uses two ExpressRoute circuits that connect to two separate on-premises datacenters.

You need to create a dashboard to display detailed metrics and a visual representation of the network topology.

What should you use?

- A. Azure Monitor Network Insights
- B. a Data Collection Rule (DCR)
- C. Azure Virtual Network Watcher
- D. Log Analytics

Answer: A

Explanation:

<https://learn.microsoft.com/en-us/azure/network-watcher/network-insights-overview>

Azure Monitor Network Insights provides a comprehensive and visual representation through topologies, of health and metrics for all deployed network resources, without requiring any configuration. It also provides access to network monitoring capabilities like Connection Monitor, flow logging for network security groups (NSGs), and Traffic Analytics. And it provides other network diagnostic features.

Question: 570

CertyIQ

You deploy Azure virtual machines to three Azure regions

Each region contains a virtual network. Each virtual network contains multiple subnets peered in a full mesh topology.

Each subnet contains a network security group (NSG) that has defined rules.

A user reports that he cannot use port 33000 to connect from a virtual machine in one region to a virtual machine in another region.

Which two options can you use to diagnose the issue? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Azure Virtual Network Manager
- B. IP flow verify
- C. Azure Monitor Network Insights
- D. Connection troubleshoot
- E. elective security rules

Answer: BD

Explanation:

<https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview>

IP flow verify checks if a packet is allowed or denied to or from a virtual machine. The information consists of direction, protocol, local IP, remote IP, local port, and a remote port. If the packet is denied by a security group, the name of the rule that denied the packet is returned. While any source or destination IP can be chosen, IP flow verify helps administrators quickly diagnose connectivity issues from or to the internet and

from or to the on-premises environment.

Question: 571

CertyIQ

You have an Azure subscription.

You need to receive an email alert when a resource lock is removed from any resource in the subscription.

What should you use to create an activity log alert in Azure Monitor?

- A. a resource, a condition, and an action group
- B. a resource, a condition, and a Microsoft 365 group
- C. a Log Analytics workspace, a resource, and an action group
- D. a data collection endpoint, an application security group, and a resource group

Answer: A

Explanation:

You create an alert rule by combining:

- The resources to be monitored.
- The signal or telemetry from the resource.
- Conditions.

Then you define these elements for the resulting alert actions by using:

- Alert processing rules
- Action groups

Reference:

<https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-create-new-alert-rule>

Question: 572

CertyIQ

HOTSPOT

-

You have an Azure subscription that contains the alerts shown in the following exhibit.

Search

Add filter

More (4)

Total alerts

 4

Critical

 0

Error

 0

Warning

 0

Informational

 0

Verbose

 4

No grouping

Name ↑↓ Severity ↑↓ Alert condition ↑↓ User response ↑↓ Fired time ↑↓

<input type="checkbox"/>	Alert2	4 - Verbose	 Fired	New	4/29/2022, 2:09 PM
<input type="checkbox"/>	Alert2	4 - Verbose	 Fired	New	4/29/2022, 2:09 PM
<input type="checkbox"/>	Alert1	4 - Verbose	 Fired	Closed	4/29/2022, 2:04 PM
<input type="checkbox"/>	Alert1	4 - Verbose	 Fired	Closed	4/29/2022, 2:04 PM

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

NOTE: Each correct selection is worth one point.

Answer Area

For Alert1, User response [answer choice].

- cannot be changed
- can be changed to New only
- can be changed to Acknowledged only
- can be changed to New or Acknowledged

For Alert2, User response [answer choice].

- cannot be changed
- can be changed to Acknowledged only
- can be changed to closed only
- can be changed to Acknowledged or Closed

Answer:

Answer Area

For Alert1, User response [answer choice].

- cannot be changed
- can be changed to New only
- can be changed to Acknowledged only
- can be changed to New or Acknowledged**

For Alert2, User response [answer choice].

- cannot be changed
- can be changed to Acknowledged only
- can be changed to closed only
- can be changed to Acknowledged or Closed**

Explanation:

For Alert1: **can be changed to New or Acknowledged.**

This implies that Alert1 is in a state that allows it to be modified either back to New or to Acknowledged.

The other available choices indicate that some alerts may only be changed to "New," "Acknowledged," or may not be changeable at all.

For Alert2: **can be changed to Acknowledged or Closed.**

This means Alert2 is in a state where it can transition to either Acknowledged (indicating recognition of the alert) or Closed (indicating resolution or dismissal of the alert).

The other choices suggest some alerts may only transition to "Acknowledged" or "Closed" individually, or not at all.

Question: 573

CertyIQ

HOTSPOT

You create a Recovery Services vault backup policy named Policy1 as shown in the following exhibit:

Policy name *

Policy1

Backup schedule

Frequency * Time * Timezone *

Daily 11:00 PM (UTC) Coordinated Universal Time

Instant Restore

Retain instant recovery snapshot(s) for

 Day(s) 

Retention range

- Retention of daily backup point.

At 11:00 PM 30  Day(s)

- Retention of weekly backup point.

On * Sunday 11:00 PM 10  Week(s)

- Retention of monthly backup point.

Week Based Day Based

On * 1 11:00 PM 36  Month(s)

- Retention of yearly backup point.

Week Based Day Based

In * March 1 11:00 PM 10  Year(s)

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

NOTE: Each correct selection is worth one point.

Answer Area

The backup that occurs on Sunday, March 1, will be retained for [answer choice].

30 days
10 weeks
36 months
10 years

The backup that occurs on Sunday, November 1, will be retained for [answer choice].

30 days
10 weeks
36 months
10 years

Answer:

Answer Area

The backup that occurs on Sunday, March 1, will be retained for [answer choice].

30 days
10 weeks
36 months
10 years

The backup that occurs on Sunday, November 1, will be retained for [answer choice].

30 days
10 weeks
36 months
10 years

Explanation:

Box 1: 10 years

The yearly backup point occurs to 1 March and its retention period is 10 years.

Box 2: 36 months

The monthly backup point occurs on the 1

of every month and its retention period is 36 months.

Note: Azure retention policy takes the longest period of retention for each backup. In case of conflict between 2 different policies.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide>

HOTSPOT

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

Name	Type
Recovery1	Recovery Services vault
Backup1	Azure Backup vault

You deploy the virtual machines shown in the following table.

Name	Operating system	Security Configuration
VM1	Windows Server	Azure Disk Encryption
VM2	Linux	Trusted launch

You have the backup policies shown in the following table.

Name	Type	In vault
Policy1	Standard	Recovery1
Policy2	Enhanced	Recovery2
Policy3	<i>Not applicable</i>	Backup1

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
VM1 can be backed up by using Policy1.	<input type="radio"/>	<input type="radio"/>
VM2 can be backed up by using Policy3.	<input type="radio"/>	<input type="radio"/>
VM2 can be backed up by using Policy2.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
VM1 can be backed up by using Policy1.	<input checked="" type="checkbox"/>	<input type="radio"/>
VM2 can be backed up by using Policy3.	<input type="radio"/>	<input checked="" type="checkbox"/>
VM2 can be backed up by using Policy2.	<input checked="" type="checkbox"/>	<input type="radio"/>

Explanation:

1. VM1 can be backed up by using Policy1.

The **Yes** option is selected.

This means that Policy1 is applicable to VM1, allowing it to be backed up successfully.

2. VM2 can be backed up by using Policy3.

The **No** option is selected.

This indicates that Policy3 does not apply to VM2, meaning VM2 cannot be backed up using this policy.

3. VM2 can be backed up by using Policy2.

The **Yes** option is selected.

This confirms that Policy2 is applicable to VM2, allowing it to be backed up successfully.

Question: 575

CertyIQ

You have an Azure subscription. The subscription contains virtual machines that connect to a virtual network named VNet1.

You plan to configure Azure Monitor for VM Insights.

You need to ensure that all the virtual machines only communicate with Azure Monitor through VNet1.

What should you create first?

- A.a data collection rule (DCR)
- B.a Log Analytics workspace
- C.an Azure Monitor Private Link Scope (AMPLS)
- D.a private endpoint

Answer: C

Explanation:

Azure Monitor private links are structured differently from private links to other services you might use. Instead of creating multiple private links, one for each resource the virtual network connects to, Azure Monitor uses a single private link connection, from the virtual network to an AMPLS. AMPLS is the set of all Azure Monitor resources to which a virtual network connects through a private link.

Reference:

<https://learn.microsoft.com/en-us/azure/azure-monitor/logs/private-link-security>

Question: 576

CertyIQ

HOTSPOT

-

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

Name	Type
Backup1	Backup vault
Recovery1	Recovery Services vault

You create a storage account that contains the resources shown in the following table.

Name	Type
cont1	Blob container
share1	File share

To which vault can you back up cont1 and share1? To answer, select the appropriate options in the answer area.

NOTE: Each correct answer is worth one point.

Answer Area

cont1:

- Backup1 only
- Recovery1 only
- Backup1 or Recovery1
- Cannot be backed up to Backup1 or Recovery1

share1:

- Backup1 only
- Recovery1 only
- Backup1 or Recovery1
- Cannot be backed up to Backup1 or Recovery1

Answer:

Answer Area

cont1:

- Backup1 only**
- Recovery1 only
- Backup1 or Recovery1
- Cannot be backed up to Backup1 or Recovery1

share1:

- Backup1 only
- Recovery1 only**
- Backup1 or Recovery1
- Cannot be backed up to Backup1 or Recovery1

Explanation:

1. cont1 (Container 1)

Backup1 only.

This means that cont1 is configured to be backed up using Backup1 and is not using Recovery1.

2.share1 (File Share 1)

Recovery1 only.

This means that share1 is configured for recovery under Recovery1 but is not backed up using Backup1.

Question: 577

CertyIQ

You have an Azure subscription that contains an Azure Stream Analytics job named Job1.

You need to monitor input events for Job1 to identify the number of events that were NOT processed.

Which metric should you use?

- A.Out-of-Order Events
- B.Output Events
- C.Late Input Events
- D.Backlogged Input Events

Answer: D

Explanation:

Correct answer: D Out-of-Order Events Number of events received out of order that were either dropped or given an adjusted time stamp, based on the event ordering policy. This metric can be affected by the configuration of the Out-of-Order Tolerance Window setting. Output Events Amount of data that the Stream Analytics job sends to the output target, in number of events. Late Input Events Events that arrived later than the configured tolerance window for late arrivals. Learn more about Azure Stream Analytics event order considerations. Backlogged Input Events Number of input events that are backlogged. A nonzero value for this metric implies that your job can't keep up with the number of incoming events. If this value is slowly increasing or is consistently nonzero, you should scale out your job. To learn more, see Understand and adjust streaming units.

Reference:

<https://learn.microsoft.com/en-us/azure/stream-analytics/stream-analytics-job-metrics>

Question: 578

CertyIQ

You have an Azure subscription that contains an Azure SQL database named DB1.

You plan to use Azure Monitor to monitor the performance of DB1. You must be able to run queries to analyze log data.

Which destination should you configure in the Diagnostic settings of DB1?

- A.Send to a Log Analytics workspace.
- B.Archive to a storage account.
- C.Stream to an Azure event hub.

Answer: A**Explanation:**

Data sent to a Log Analytics workspace can be consumed by SQL Analytics, which provides intelligent monitoring of your databases including performance reports, alerts, and mitigation recommendations. Moreover, data in a Log Analytics workspace can be analysed alongside other monitoring data collected, and also allows you to leverage other Azure Monitor features such as alerts and visualizations.

<https://learn.microsoft.com/en-us/azure/azure-sql/database/metrics-diagnostic-telemetry-logging-streaming-export-configure?view=azuresql&tabs=azure-portal>

[https://www.sqlservercentral.com/articles/monitoring-azure-sql-databases#:~:text=If%20not%2C%20just%20search%20for,to%20your%20Log%20Analytics%20Workspace](https://www.sqlservercentral.com/articles/monitoring-azure-sql-databases#:~:text=If%20not%2C%20just%20search%20for%20Log%20Analytics%20workspace,Set%20the%20destination%20to%20your%20Log%20Analytics%20Workspace.#:~:text=If%20not%2C%20just%20search%20for,to%20your%20Log%20Analytics%20Workspace)

<https://techcommunity.microsoft.com/t5/azure-database-support-blog/azure-sql-db-and-log-analytics-better-together-part-1/ba-p/794833>

CertyIQ**Question: 579**

You have an Azure subscription. The subscription contains virtual machines that run Windows Server.

You have a data collection rule (DCR) named Rule1.

You plan to use the Azure Monitor Agent to collect events from Windows System event logs.

You only need to collect system events that have an ID of 1001.

Which type of query should you use for the data source in Rule1?

- A.SQL
- B.XPath
- C.KQL

Answer: B**Explanation:**

Custom data source in Azure Portal says: "Use XPath queries to filter event logs and limit data collection"

To collect specific events from Windows System event logs, such as those with an Event ID of 1001, you should use an XPath query. XPath is a query language that can be used to filter XML data, which is the format used by Windows Event Logs. In Azure Monitor, when configuring data collection rules for collecting Windows event log data, XPath queries are used to specify the criteria for the events you want to collect.

the correct answer is: B. XPath.

CertyIQ**Question: 580**

You have an Azure subscription that contains a virtual machine named VM1.

You have an on-premises datacenter that contains a domain controller named DC1. ExpressRoute is used to connect the on-premises datacenter to Azure.

You need to use Connection Monitor to identify network latency between VM1 and DC1.

What should you install on DC1?

- A.the Azure Connected Machine agent for Azure Arc-enabled servers
- B.the Azure Network Watcher Agent virtual machine extension
- C.the Log Analytics agent
- D.an Azure Monitor agent extension

Answer: D

Explanation:

Connection monitor supports the Azure Monitor agent extension, which eliminates any dependency on the legacy Log Analytics agent. <https://learn.microsoft.com/en-us/azure/network-watcher/azure-monitor-agent-with-connection-monitor> The following (older) link talks about setting up the Log Analytics agent.

<https://learn.microsoft.com/en-us/azure/network-watcher/connection-monitor-overview#agents-for-on-premises-machines>

Question: 581

CertyIQ

You have an Azure subscription that has Traffic Analytics configured.

You deploy a new virtual machine named VM1 that has the following settings:

- Region: East US
- Virtual network: VNet1
- NIC network security group: NSG1

You need to monitor VM1 traffic by using Traffic Analytics.

Which settings should you configure?

- A.Diagnostic settings for VM1
- B.NSG flow logs for NSG1
- C.Diagnostic settings for NSG1
- D.Insights for VM1

Answer: B

Explanation:

NSG flow logs are a feature of Azure Network Watcher that allows logging of information about IP traffic flowing through a network security group. This data can be used by Traffic Analytics to analyze network traffic in your environment. By enabling NSG flow logs for NSG1, the Network Security Group associated with VM1, you would be able to monitor the traffic of VM1 using Traffic Analytics

<https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics>

<https://learn.microsoft.com/en-us/azure/network-watcher/nsg-flow-logs-tutorial>

Question: 582

CertyIQ

You have an Azure subscription. The subscription contains 10 virtual machines that run Windows Server. Each virtual machine hosts a website in IIS and has the Azure Monitor Agent installed.

You need to collect the IIS logs from each virtual machine and store them in a Log Analytics workspace.

What should you configure first?

- A.a data collection endpoint
- B.an Azure Monitor Private Link Scope (AMPLS)
- C.Diagnostic settings
- D.VM insights
- E.a private endpoint

Answer: C**Explanation:**

C. Diagnostic settings.

Diagnostic settings: Diagnostic settings in Azure allow you to specify which logs and metrics should be collected from your resources and where they should be sent (e.g., to a Log Analytics workspace, an event hub, or a storage account). For collecting IIS logs, you will configure the diagnostic settings on each virtual machine to send the IIS logs to the Log Analytics workspace.

Question: 583

CertyIQ

HOTSPOT

You have an Azure subscription that contains two storage accounts named contoso101 and contoso102.

The subscription contains the virtual machines shown in the following table.

Name	Connected to	Public IP address SKU
VM1	VNet1/Subnet1	Basic
VM2	VNet1/Subnet2	Standard

VNet1 has service endpoints configured as shown in the Service endpoints exhibit. (Click the Service endpoints tab.)



»

Add



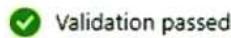
Refresh

Filter service endpoints

Service	Subnet	Status	Locations
Microsoft.AzureActiveDirectory	1		...
	Subnet2	Succeeded	*
Microsoft.Storage	1		...
	Subnet1	Succeeded	*

The Microsoft.Storage service endpoint has the service endpoint policy shown in the Microsoft.Storage exhibit.
(Click the Microsoft.Storage tab.)

Create a service endpoint policy



Basics Policy definitions Tags Review + create

Basics

Subscription Azure Pass - Sponsorship
Resource group RG1
Region East US
Name Policy1

Resources

Microsoft.Storage contoso101 (Storage account)

Tags

None

i For this policy to take effect, you will need to associate it to one or more subnets that have virtual network service endpoints. Please visit a virtual network in East US region and then select the subnets to which you would like to associate this policy.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
VM1 can access contoso102.	<input type="radio"/>	<input type="radio"/>
VM2 can access contoso101.	<input type="radio"/>	<input type="radio"/>
VM2 uses a private IP address to access Azure AD.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
VM1 can access contoso102.	<input type="radio"/>	<input checked="" type="checkbox"/>
VM2 can access contoso101.	<input type="radio"/>	<input checked="" type="checkbox"/>
VM2 uses a private IP address to access Azure AD.	<input checked="" type="checkbox"/>	<input type="radio"/>

Explanation:

No, because the Microsoft.Storage service endpoint is configured for Subnet1, which VM1 is connected to, but the policy shown is specifically for contoso101. There is no indication that VM1 can access contoso102.

VM2 can access contoso101.

No, because VM2 is connected to Subnet2, and the Microsoft.Storage service endpoint is only configured for Subnet1, not Subnet2. Therefore, VM2 cannot access contoso101.

VM2 uses a private IP address to access Azure AD.

Yes, because the Microsoft.AzureActiveDirectory service endpoint is enabled for Subnet2, where VM2 is connected. This allows VM2 to access Azure AD using a private IP.

Question: 584

CertyIQ

You have an Azure subscription that contains multiple virtual machines in the West US Azure region.

You need to use Traffic Analytics in Azure Network Watcher to monitor virtual machine traffic.

Which two resources should you create? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A.a Log Analytics workspace
- B.an Azure Monitor workbook
- C.a storage account
- D.a Microsoft Sentinel workspace
- E.a Data Collection Rule (DCR) in Azure Monitor

Answer: AE

Explanation:

- A. A Log Analytics workspace - Traffic Analytics requires a Log Analytics workspace to store and analyze network traffic data.
- E. A Data Collection Rule (DCR) in Azure Monitor - You need to create a Data Collection Rule within Azure Monitor to specify what data should be collected and sent to the Log Analytics workspace, including the network traffic data for Traffic Analytics.

Question: 585

CertyIQ

You have an Azure subscription that contains a virtual machine named VM1.

You plan to deploy an Azure Monitor alert rule that will trigger an alert when CPU usage on VM1 exceeds 80 percent.

You need to ensure that the alert rule sends an email message to two users named User1 and User2.

What should you create for Azure Monitor?

- A.an action group
- B.a mail-enabled security group
- C.a distribution group
- D.a Microsoft 365 group

Answer: A

Explanation:

- A. an action group.

In Azure Monitor, an action group is used to define actions when an alert is triggered. Since the goal is to send an email to User1 and User2 when CPU usage exceeds 80% on VM1, you need to:

Create an Azure Monitor alert rule that monitors CPU usage on VM1.

Create an action group that includes email addresses for User1 and User2.

Associate the action group with the alert rule, so that when the alert is triggered, an email notification is sent.

HOTSPOT -

You need to configure the Device settings to meet the technical requirements and the user requirements. Which two settings should you modify? To answer, select the appropriate settings in the answer area.

Hot Area:

Answer Area



Save



Discard



Got feedback?

Users may join devices to Azure AD ⓘ

All

Selected

None

Selected

No member selected

Additional local administrators on Azure AD joined devices ⓘ

Selected

None

Selected

No member selected

Users may register their devices with Azure AD ⓘ

All

None

Require Multi-Factor Auth to join devices ⓘ

Yes

No

Maximum number of devices per user ⓘ

50

Answer:

Answer Area



Save



Discard



Got feedback?

Users may join devices to Azure AD ⓘ

All

Selected

None

Selected

No member selected

Additional local administrators on Azure AD joined devices ⓘ

Selected

None

Selected

No member selected

Users may register their devices with Azure AD ⓘ

All

None

Require Multi-Factor Auth to join devices ⓘ

Yes

No

Maximum number of devices per user ⓘ

50

Explanation:

Box 1: Selected -

Only selected users should be able to join devices

Box 2: Yes -

Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.

Case Study Description

Contoso Ltd

Overview

Contoso, Ltd. is a manufacturing company that has offices worldwide. Contoso works with partner organizations to bring products to market.

Contoso products are manufactured by using blueprint files that the company authors and maintains.

Existing Environment

Currently, Contoso uses multiple types of servers for business operations, including the following:

- ⇒ File servers
- ⇒ Domain controllers
- ⇒ Microsoft SQL Server servers

Your network contains an Active Directory forest named contoso.com. All servers and client computers are joined to Active Directory.

You have a public-facing application named App1.

App1 is comprised of the following three tiers:

- ⇒ A SQL database
- ⇒ A web front end
- ⇒ A processing middle tier

Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.

Requirements

Planned Changes

Contoso plans to implement the following changes to the infrastructure:

- Move all the tiers of App1 to Azure.
- Move the existing product blueprint files to Azure Blob storage.
- Create a hybrid directory to support an upcoming Microsoft Office 365 migration project.

Technical Requirements

Contoso must meet the following technical requirements:

- ⇒ Move all the virtual machines for App1 to Azure.

- ⇒ Minimize the number of open ports between the App1 tiers.
- ⇒ Ensure that all the virtual machines for App1 are protected by backups.
- ⇒ Copy the blueprint files to Azure over the Internet.
- ⇒ Ensure that the blueprint files are stored in the archive storage tier.
- ⇒ Ensure that partner access to the blueprint files is secured and temporary.
- ⇒ Prevent user passwords or hashes of passwords from being stored in Azure.
- ⇒ Use unmanaged standard storage for the hard disks of the virtual machines.
- ⇒ Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.

Minimize administrative effort whenever possible.

User Requirements

Contoso identifies the following requirements for users:

- ⇒ Ensure that only users who are part of a group named Pilot can join devices to Azure AD.
- ⇒ Designate a new user named Admin1 as the service administrator of the Azure subscription.
- ⇒ Admin1 must receive email alerts regarding service outages.
- ⇒ Ensure that a new user named User3 can create network objects for the Azure subscription.

Question: 587

CertyIQ

You need to meet the user requirement for Admin1.
What should you do?

- A. From the Azure Active Directory blade, modify the Groups
- B. From the Azure Active Directory blade, modify the Properties
- C. From the Subscriptions blade, select the subscription, and then modify the Access control (IAM) settings
- D. From the Subscriptions blade, select the subscription, and then modify the Properties

Answer: D

Explanation:

Scenario:

- ⇒ Designate a new user named Admin1 as the service admin for the Azure subscription.
- ⇒ Admin1 must receive email alerts regarding service outages.

Follow these steps to change the Service Administrator in the Azure portal.

1. Make sure your scenario is supported by checking the limitations for changing the Service Administrator.
2. Sign in to the Azure portal as the Account Administrator.
3. Open Cost Management + Billing and select a subscription.

4. In the left navigation, click Properties.

5. Click Service Admin.

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/classic-administrators>

Case Study Description

Contoso Ltd

Overview

Contoso, Ltd. is a manufacturing company that has offices worldwide. Contoso works with partner organizations to bring products to market.

Contoso products are manufactured by using blueprint files that the company authors and maintains.

Existing Environment

Currently, Contoso uses multiple types of servers for business operations, including the following:

- ⇒ File servers
- ⇒ Domain controllers
- ⇒ Microsoft SQL Server servers

Your network contains an Active Directory forest named contoso.com. All servers and client computers are joined to Active Directory.

You have a public-facing application named App1.

App1 is comprised of the following three tiers:

- ⇒ A SQL database
- ⇒ A web front end
- ⇒ A processing middle tier

Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.

Requirements

Planned Changes

Contoso plans to implement the following changes to the infrastructure:

- Move all the tiers of App1 to Azure.
- Move the existing product blueprint files to Azure Blob storage.
- Create a hybrid directory to support an upcoming Microsoft Office 365 migration project.

Technical Requirements

Contoso must meet the following technical requirements:

- ⇒ Move all the virtual machines for App1 to Azure.
- ⇒ Minimize the number of open ports between the App1 tiers.
- ⇒ Ensure that all the virtual machines for App1 are protected by backups.
- ⇒ Copy the blueprint files to Azure over the Internet.
- ⇒ Ensure that the blueprint files are stored in the archive storage tier.
- ⇒ Ensure that partner access to the blueprint files is secured and temporary.
- ⇒ Prevent user passwords or hashes of passwords from being stored in Azure.
- ⇒ Use unmanaged standard storage for the hard disks of the virtual machines.
- ⇒ Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.

Minimize administrative effort whenever possible.

User Requirements

Contoso identifies the following requirements for users:

- ⇒ Ensure that only users who are part of a group named Pilot can join devices to Azure AD.
- ⇒ Designate a new user named Admin1 as the service administrator of the Azure subscription.
- ⇒ Admin1 must receive email alerts regarding service outages.
- ⇒ Ensure that a new user named User3 can create network objects for the Azure subscription.

Question: 588

CertyIQ

HOTSPOT -

You need to configure Azure Backup to back up the file shares and virtual machines.

What is the minimum number of Recovery Services vaults and backup policies you should create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Recovery Services vaults

	▼
1	
2	
3	
4	
7	

Backup policies

	▼
1	
2	
3	
4	
5	
6	

Answer:

Answer Area

Recovery Services vaults

	▼
1	
2	
3	
4	
7	

Backup policies

	▼
1	
2	
3	
4	
5	
6	

Explanation:

Box 1: 3 -

If you have data sources in multiple regions, create a Recovery Services vault for each region.

The File Shares and VMs are located in three Regions: West US, East US, Central US.

Box 2: 6 -

A backup policy is scoped to a vault. For each vault we need one backup policy for File Shares and one backup policy for VM.

Note:

Back up the Azure file shares and virtual machines by using Azure Backup

Name	Kind	Location	File share	Identity-based access for file share
storage1	Storage (general purpose v1)	West US	sharea	Azure Active Directory Domain Services (Azure AD DS)
storage2	StorageV2 (general purpose v2)	East US	shareb, sharec	Disabled
storage3	BlobStorage	East US 2	Not applicable	Not applicable
storage4	FileStorage	Central US	shared	Azure Active Directory Domain Services (Azure AD DS)

Name	IP address	Location	Connected to
VM1	10.0.1.4	West US	VNET1/Subnet1
VM2	10.0.2.4	West US	VNET1/Subnet2
VM3	172.16.1.4	Central US	VNET2/Subnet1
VM4	192.168.1.4	West US	VNET3/Subnet1
VM5	10.0.22.4	East US	VNET4/Subnet1

Reference:

<https://docs.microsoft.com/en-us/azure/backup/backup-create-rs-vault> <https://docs.microsoft.com/en-us/azure/backup/guidance-best-practices>

Case Study Description:

Contoso Ltd (Consulting Company)

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to

explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

General Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York.

Environment

Existing Environment

Contoso has an Azure subscription named Sub1 that is linked to an Azure Active Directory (Azure AD) tenant. The network contains an on-premises Active Directory domain that syncs to the Azure AD tenant.

The Azure AD tenant contains the users shown in the following table.

Name	Type	Role
User1	Member	None
User2	Guest	None
User3	Member	None
User4	Member	None

Sub1 contains two resource groups named RG1 and RG2 and the virtual networks shown in the following table.

Name	Subnet	Peered with
VNET1	Subnet1, Subnet2	VNET2
VNET2	Subnet1	VNET1, VNET3
VNET3	Subnet1	VNET2
VNET4	Subnet1	None

User1 manages the resources in RG1. User4 manages the resources in RG2.

Sub1 contains virtual machines that run Windows Server 2019 as shown in the following table

Name	IP address	Location	Connected to
VM1	10.0.1.4	West US	VNET1/Subnet1
VM2	10.0.2.4	West US	VNET1/Subnet2
VM3	172.16.1.4	Central US	VNET2/Subnet1
VM4	192.168.1.4	West US	VNET3/Subnet1
VM5	10.0.22.4	East US	VNET4/Subnet1

No network security groups (NSGs) are associated to the network interfaces or the subnets.

Sub1 contains the storage accounts shown in the following table.

Name	Kind	Location	File share	Identity-based access for file share
storage1	Storage (general purpose v1)	West US	sharea	Azure Active Directory Domain Services (Azure AD DS)
storage2	StorageV2 (general purpose v2)	East US	shareb, sharec	Disabled
storage3	BlobStorage	East US 2	Not applicable	Not applicable
storage4	FileStorage	Central US	shared	Azure Active Directory Domain Services (Azure AD DS)

Requirements

Planned Changes

Contoso plans to implement the following changes:

- ⇒ Create a blob container named container1 and a file share named share1 that will use the Cool storage tier.
- ⇒ Create a storage account named storage5 and configure storage replication for the Blob service.
- ⇒ Create an NSG named NSG1 that will have the custom inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
500	3389	TCP	10.0.2.0/24	Any	Deny
1000	Any	ICMP	Any	VirtualNetwork	Allow

- ⇒ Associate NSG1 to the network interface of VM1.
- ⇒ Create an NSG named NSG2 that will have the custom outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
200	3389	TCP	10.0.0.0/16	VirtualNetwork	Deny
400	Any	ICMP	10.0.2.0/24	10.0.1.0/24	Allow

- ⇒ Associate NSG2 to VNET1/Subnet2.

Technical Requirements

Contoso must meet the following technical requirements:

- ⇒ Create container1 and share1.
- ⇒ Use the principle of least privilege.
- ⇒ Create an Azure AD security group named Group4.
- ⇒ Back up the Azure file shares and virtual machines by using Azure Backup.
- ⇒ Trigger an alert if VM1 or VM2 has less than 20 GB of free space on volume C.
- ⇒ Enable User1 to create Azure policy definitions and User2 to assign Azure policies to RG1.
- ⇒ Create an internal Basic Azure Load Balancer named LB1 and connect the load balancer to VNET1/Subnet1
- ⇒ Enable flow logging for IP traffic from VM5 and retain the flow logs for a period of eight months.
- ⇒ Whenever possible, grant Group4 Azure role-based access control (Azure RBAC) read-only permissions to the Azure file shares.

Question: 589

CertyIQ

DRAG DROP -

You need to configure the alerts for VM1 and VM2 to meet the technical requirements.

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

Select and Place:

Actions
Create a Log Analytics workspace.
Configure the Diagnostic settings.
Create an alert rule.
Collect Windows performance counters from the Log Analytics agents.
Create an Azure SQL database.

Answer Area



Answer:

Actions
Create a Log Analytics workspace.
Configure the Diagnostic settings.
Create an alert rule.
Collect Windows performance counters from the Log Analytics agents.
Create an Azure SQL database.

Answer Area
Create a Log Analytics workspace.
Configure the Diagnostic settings.
Create an alert rule.

Explanation:

1 - Create a Log Analytics workspace: <https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-workspace-overview>

2- Configure the Diagnostic settings: <https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/diagnostic-settings>

3 - Create an alert rule: <https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-log>

Create a Log Analytics workspace:

Provides a central place to collect and analyze log data from your virtual machines. Without a Log Analytics workspace, you cannot effectively gather and analyze the necessary performance metrics.

Configure the Diagnostic settings:

Configuring diagnostic settings on VM1 and VM2 ensures that performance data, including disk space metrics, are sent to the Log Analytics workspace.

Create an alert rule:

After data collection is set up, creating an alert rule based on a log search query allows you to monitor specific conditions, such as the available disk space on VM1 and VM2. The alert rule will notify you when the free space falls below the threshold, enabling proactive management.

Question: 590

CertyIQ

HOTSPOT -

You need to ensure that User1 can create initiative definitions, and User4 can assign initiatives to RG2. The solution must meet the technical requirements.

Which role should you assign to each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User1:

- Contributor for RG1
- Contributor for Sub1
- Security Admin for RG1
- Resource Policy Contributor for Sub1

User4:

- Contributor for RG2
- Contributor for Sub1
- Security Admin for Sub1
- Resource Policy Contributor for RG2

Answer:

Answer Area

User1:

Contributor for RG1	▼
Contributor for Sub1	
Security Admin for RG1	
Resource Policy Contributor for Sub1	

User4:

Contributor for RG2	▼
Contributor for Sub1	
Security Admin for Sub1	
Resource Policy Contributor for RG2	

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/governance/policy/overview>

Case Study Description:

Contoso Ltd (Consulting Company)

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to

explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

General Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York.

Environment

Existing Environment

Contoso has an Azure subscription named Sub1 that is linked to an Azure Active Directory (Azure AD) tenant. The network contains an on-premises Active Directory domain that syncs to the Azure AD tenant.

The Azure AD tenant contains the users shown in the following table.

Name	Type	Role
User1	Member	None
User2	Guest	None
User3	Member	None
User4	Member	None

Sub1 contains two resource groups named RG1 and RG2 and the virtual networks shown in the following table.

Name	Subnet	Peered with
VNET1	Subnet1, Subnet2	VNET2
VNET2	Subnet1	VNET1, VNET3
VNET3	Subnet1	VNET2
VNET4	Subnet1	None

User1 manages the resources in RG1. User4 manages the resources in RG2.

Sub1 contains virtual machines that run Windows Server 2019 as shown in the following table

Name	IP address	Location	Connected to
VM1	10.0.1.4	West US	VNET1/Subnet1
VM2	10.0.2.4	West US	VNET1/Subnet2
VM3	172.16.1.4	Central US	VNET2/Subnet1
VM4	192.168.1.4	West US	VNET3/Subnet1
VM5	10.0.22.4	East US	VNET4/Subnet1

No network security groups (NSGs) are associated to the network interfaces or the subnets.

Sub1 contains the storage accounts shown in the following table.

Name	Kind	Location	File share	Identity-based access for file share
storage1	Storage (general purpose v1)	West US	sharea	Azure Active Directory Domain Services (Azure AD DS)
storage2	StorageV2 (general purpose v2)	East US	shareb, sharec	Disabled
storage3	BlobStorage	East US 2	Not applicable	Not applicable
storage4	FileStorage	Central US	shared	Azure Active Directory Domain Services (Azure AD DS)

Requirements

Planned Changes

Contoso plans to implement the following changes:

- ⇒ Create a blob container named container1 and a file share named share1 that will use the Cool storage tier.
- ⇒ Create a storage account named storage5 and configure storage replication for the Blob service.
- ⇒ Create an NSG named NSG1 that will have the custom inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
500	3389	TCP	10.0.2.0/24	Any	Deny
1000	Any	ICMP	Any	VirtualNetwork	Allow

- ⇒ Associate NSG1 to the network interface of VM1.
- ⇒ Create an NSG named NSG2 that will have the custom outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
200	3389	TCP	10.0.0.0/16	VirtualNetwork	Deny
400	Any	ICMP	10.0.2.0/24	10.0.1.0/24	Allow

- ⇒ Associate NSG2 to VNET1/Subnet2.

Technical Requirements

Contoso must meet the following technical requirements:

- ⇒ Create container1 and share1.
- ⇒ Use the principle of least privilege.
- ⇒ Create an Azure AD security group named Group4.
- ⇒ Back up the Azure file shares and virtual machines by using Azure Backup.
- ⇒ Trigger an alert if VM1 or VM2 has less than 20 GB of free space on volume C.
- ⇒ Enable User1 to create Azure policy definitions and User2 to assign Azure policies to RG1.
- ⇒ Create an internal Basic Azure Load Balancer named LB1 and connect the load balancer to VNET1/Subnet1
- ⇒ Enable flow logging for IP traffic from VM5 and retain the flow logs for a period of eight months.
- ⇒ Whenever possible, grant Group4 Azure role-based access control (Azure RBAC) read-only permissions to the Azure file shares.

Question: 591

CertyIQ

You need to ensure that you can grant Group4 Azure RBAC read only permissions to all the Azure file shares. What should you do?

- A. On storage2, enable identity-based access for the file shares.
- B. Recreate storage2 and set Hierarchical namespace to Enabled.
- C. On storage1 and storage4, change the Account kind type to StorageV2 (general purpose v2).
- D. Create a shared access signature (SAS) for storage1, storage2, and storage4.

Answer: A

Explanation:

Azure Files supports identity-based authentication over Server Message Block (SMB) through on-premises Active Directory Domain Services (AD DS) and Azure

Active Directory Domain Services (Azure AD DS).

Reference:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-files-active-directory-overview>

Case Study Description:

Contoso Ltd (Consulting Company)

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must

manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

General Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York.

Environment

Existing Environment

Contoso has an Azure subscription named Sub1 that is linked to an Azure Active Directory (Azure AD) tenant. The network contains an on-premises Active Directory domain that syncs to the Azure AD tenant.

The Azure AD tenant contains the users shown in the following table.

Name	Type	Role
User1	Member	None
User2	Guest	None
User3	Member	None
User4	Member	None

Sub1 contains two resource groups named RG1 and RG2 and the virtual networks shown in the following table.

Name	Subnet	Peered with
VNET1	Subnet1, Subnet2	VNET2
VNET2	Subnet1	VNET1, VNET3
VNET3	Subnet1	VNET2
VNET4	Subnet1	None

User1 manages the resources in RG1. User4 manages the resources in RG2.

Sub1 contains virtual machines that run Windows Server 2019 as shown in the following table

Name	IP address	Location	Connected to
VM1	10.0.1.4	West US	VNET1/Subnet1
VM2	10.0.2.4	West US	VNET1/Subnet2
VM3	172.16.1.4	Central US	VNET2/Subnet1
VM4	192.168.1.4	West US	VNET3/Subnet1
VM5	10.0.22.4	East US	VNET4/Subnet1

No network security groups (NSGs) are associated to the network interfaces or the subnets.

Sub1 contains the storage accounts shown in the following table.

Name	Kind	Location	File share	Identity-based access for file share
storage1	Storage (general purpose v1)	West US	sharea	Azure Active Directory Domain Services (Azure AD DS)
storage2	StorageV2 (general purpose v2)	East US	shareb, sharec	Disabled
storage3	BlobStorage	East US 2	Not applicable	Not applicable
storage4	FileStorage	Central US	shared	Azure Active Directory Domain Services (Azure AD DS)

Requirements

Planned Changes

Contoso plans to implement the following changes:

- ⇒ Create a blob container named container1 and a file share named share1 that will use the Cool storage tier.
- ⇒ Create a storage account named storage5 and configure storage replication for the Blob service.
- ⇒ Create an NSG named NSG1 that will have the custom inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
500	3389	TCP	10.0.2.0/24	Any	Deny
1000	Any	ICMP	Any	VirtualNetwork	Allow

- ⇒ Associate NSG1 to the network interface of VM1.
- ⇒ Create an NSG named NSG2 that will have the custom outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
200	3389	TCP	10.0.0.0/16	VirtualNetwork	Deny
400	Any	ICMP	10.0.2.0/24	10.0.1.0/24	Allow

- ⇒ Associate NSG2 to VNET1/Subnet2.

Technical Requirements

Contoso must meet the following technical requirements:

- ⇒ Create container1 and share1.
- ⇒ Use the principle of least privilege.
- ⇒ Create an Azure AD security group named Group4.
- ⇒ Back up the Azure file shares and virtual machines by using Azure Backup.
- ⇒ Trigger an alert if VM1 or VM2 has less than 20 GB of free space on volume C.
- ⇒ Enable User1 to create Azure policy definitions and User2 to assign Azure policies to RG1.
- ⇒ Create an internal Basic Azure Load Balancer named LB1 and connect the load balancer to VNET1/Subnet1
- ⇒ Enable flow logging for IP traffic from VM5 and retain the flow logs for a period of eight months.
- ⇒ Whenever possible, grant Group4 Azure role-based access control (Azure RBAC) read-only permissions to the Azure file shares.

Question: 592

CertyIQ

You need to implement a backup solution for App1 after the application is moved. What should you create first?

- A. a recovery plan
- B. an Azure Backup Server
- C. a backup policy
- D. a Recovery Services vault

Answer: D

Explanation:

A Recovery Services vault is a logical container that stores the backup data for each protected resource, such as Azure VMs. When the backup job for a protected resource runs, it creates a recovery point inside the Recovery Services vault.

Scenario:

There are three application tiers, each with five virtual machines.

Move all the virtual machines for App1 to Azure.

Ensure that all the virtual machines for App1 are protected by backups.

Reference:

<https://docs.microsoft.com/en-us/azure/backup/quick-backup-vm-portal>

Case Study Description

Contoso Ltd

Overview

Contoso, Ltd. is a manufacturing company that has offices worldwide. Contoso works with partner organizations to bring products to market.

Contoso products are manufactured by using blueprint files that the company authors and maintains.

Existing Environment

Currently, Contoso uses multiple types of servers for business operations, including the following:

- ⇒ File servers
- ⇒ Domain controllers
- ⇒ Microsoft SQL Server servers

Your network contains an Active Directory forest named contoso.com. All servers and client computers are joined to Active Directory.

You have a public-facing application named App1.

App1 is comprised of the following three tiers:

- ⇒ A SQL database
- ⇒ A web front end
- ⇒ A processing middle tier

Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.

Requirements

Planned Changes

Contoso plans to implement the following changes to the infrastructure:

- Move all the tiers of App1 to Azure.
- Move the existing product blueprint files to Azure Blob storage.

- Create a hybrid directory to support an upcoming Microsoft Office 365 migration project.

Technical Requirements

Contoso must meet the following technical requirements:

- ⇒ Move all the virtual machines for App1 to Azure.
- ⇒ Minimize the number of open ports between the App1 tiers.
- ⇒ Ensure that all the virtual machines for App1 are protected by backups.
- ⇒ Copy the blueprint files to Azure over the Internet.
- ⇒ Ensure that the blueprint files are stored in the archive storage tier.
- ⇒ Ensure that partner access to the blueprint files is secured and temporary.
- ⇒ Prevent user passwords or hashes of passwords from being stored in Azure.
- ⇒ Use unmanaged standard storage for the hard disks of the virtual machines.
- ⇒ Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.

Minimize administrative effort whenever possible.

User Requirements

Contoso identifies the following requirements for users:

- ⇒ Ensure that only users who are part of a group named Pilot can join devices to Azure AD.
- ⇒ Designate a new user named Admin1 as the service administrator of the Azure subscription.
- ⇒ Admin1 must receive email alerts regarding service outages.
- ⇒ Ensure that a new user named User3 can create network objects for the Azure subscription.

Question: 593

CertyIQ

You need to move the blueprint files to Azure.

What should you do?

- Generate an access key. Map a drive, and then copy the files by using File Explorer.
- Use Azure Storage Explorer to copy the files.
- Use the Azure Import/Export service.
- Generate a shared access signature (SAS). Map a drive, and then copy the files by using File Explorer.

Answer: B

Explanation:

Azure Storage Explorer is a free tool from Microsoft that allows you to work with Azure Storage data on Windows, macOS, and Linux. You can use it to upload and download data from Azure blob storage.

Scenario:

Planned Changes include: move the existing product blueprint files to Azure Blob storage.

Technical Requirements include: Copy the blueprint files to Azure over the Internet.

Reference:

<https://docs.microsoft.com/en-us/azure/machine-learning/team-data-science-process/move-data-to-azure-blob-using-azure-storage-explorer>

Case Study Description

Contoso Ltd

Overview

Contoso, Ltd. is a manufacturing company that has offices worldwide. Contoso works with partner organizations to bring products to market.

Contoso products are manufactured by using blueprint files that the company authors and maintains.

Existing Environment

Currently, Contoso uses multiple types of servers for business operations, including the following:

- ⇒ File servers
- ⇒ Domain controllers
- ⇒ Microsoft SQL Server servers

Your network contains an Active Directory forest named contoso.com. All servers and client computers are joined to Active Directory.

You have a public-facing application named App1.

App1 is comprised of the following three tiers:

- ⇒ A SQL database
- ⇒ A web front end
- ⇒ A processing middle tier

Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.

Requirements

Planned Changes

Contoso plans to implement the following changes to the infrastructure:

- Move all the tiers of App1 to Azure.
- Move the existing product blueprint files to Azure Blob storage.
- Create a hybrid directory to support an upcoming Microsoft Office 365 migration project.

Technical Requirements

Contoso must meet the following technical requirements:

- ⇒ Move all the virtual machines for App1 to Azure.
- ⇒ Minimize the number of open ports between the App1 tiers.
- ⇒ Ensure that all the virtual machines for App1 are protected by backups.
- ⇒ Copy the blueprint files to Azure over the Internet.
- ⇒ Ensure that the blueprint files are stored in the archive storage tier.
- ⇒ Ensure that partner access to the blueprint files is secured and temporary.
- ⇒ Prevent user passwords or hashes of passwords from being stored in Azure.
- ⇒ Use unmanaged standard storage for the hard disks of the virtual machines.
- ⇒ Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.

Minimize administrative effort whenever possible.

User Requirements

Contoso identifies the following requirements for users:

- ⇒ Ensure that only users who are part of a group named Pilot can join devices to Azure AD.
- ⇒ Designate a new user named Admin1 as the service administrator of the Azure subscription.
- ⇒ Admin1 must receive email alerts regarding service outages.
- ⇒ Ensure that a new user named User3 can create network objects for the Azure subscription.

Question: 594

CertyIQ

HOTSPOT -

You need to identify the storage requirements for Contoso.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Contoso requires a storage account that supports Blob storage.	<input type="radio"/>	<input type="radio"/>
Contoso requires a storage account that supports Azure Table storage.	<input type="radio"/>	<input type="radio"/>
Contoso requires a storage account that supports Azure File Storage.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Contoso requires a storage account that supports Blob storage.	<input checked="" type="radio"/>	<input type="radio"/>
Contoso requires a storage account that supports Azure Table storage.	<input type="radio"/>	<input checked="" type="radio"/>
Contoso requires a storage account that supports Azure File Storage.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Box 1: Yes -

Contoso is moving the existing product blueprint files to Azure Blob storage.

Use unmanaged standard storage for the hard disks of the virtual machines. We use Page Blobs for these.

Box 2: No -

Box 3: No

Case Study Description

Contoso Ltd

Overview

Contoso, Ltd. is a manufacturing company that has offices worldwide. Contoso works with partner organizations to bring products to market.

Contoso products are manufactured by using blueprint files that the company authors and maintains.

Existing Environment

Currently, Contoso uses multiple types of servers for business operations, including the following:

- ⇒ File servers
- ⇒ Domain controllers
- ⇒ Microsoft SQL Server servers

Your network contains an Active Directory forest named contoso.com. All servers and client computers are joined to Active Directory.

You have a public-facing application named App1.

App1 is comprised of the following three tiers:

- ⇒ A SQL database
- ⇒ A web front end
- ⇒ A processing middle tier

Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.

Requirements

Planned Changes

Contoso plans to implement the following changes to the infrastructure:

- Move all the tiers of App1 to Azure.
- Move the existing product blueprint files to Azure Blob storage.
- Create a hybrid directory to support an upcoming Microsoft Office 365 migration project.

Technical Requirements

Contoso must meet the following technical requirements:

- ⇒ Move all the virtual machines for App1 to Azure.
- ⇒ Minimize the number of open ports between the App1 tiers.
- ⇒ Ensure that all the virtual machines for App1 are protected by backups.
- ⇒ Copy the blueprint files to Azure over the Internet.
- ⇒ Ensure that the blueprint files are stored in the archive storage tier.
- ⇒ Ensure that partner access to the blueprint files is secured and temporary.
- ⇒ Prevent user passwords or hashes of passwords from being stored in Azure.
- ⇒ Use unmanaged standard storage for the hard disks of the virtual machines.
- ⇒ Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.

Minimize administrative effort whenever possible.

User Requirements

Contoso identifies the following requirements for users:

- ⇒ Ensure that only users who are part of a group named Pilot can join devices to Azure AD.
- ⇒ Designate a new user named Admin1 as the service administrator of the Azure subscription.
- ⇒ Admin1 must receive email alerts regarding service outages.
- ⇒ Ensure that a new user named User3 can create network objects for the Azure subscription.

HOTSPOT -

You need to create container1 and share1.

Which storage accounts should you use for each resource? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

container1:

- storage2 only
- storage2 and storage3 only
- storage1, storage2, and storage3 only
- storage2, storage3, and storage4 only
- storage1, storage2, storage3, and storage4

share1:

- storage2 only
- storage4 only
- storage2 and storage4 only
- storage1, storage2, and storage4 only
- storage1, storage2, storage3, and storage4

Answer:

Answer Area

container1:

- storage2 only
- storage2 and storage3 only
- storage1, storage2, and storage3 only
- storage2, storage3, and storage4 only
- storage1, storage2, storage3, and storage4

share1:

- storage2 only
- storage4 only
- storage2 and storage4 only
- storage1, storage2, and storage4 only
- storage1, storage2, storage3, and storage4

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers>
<https://docs.microsoft.com/en-us/azure/storage/common/storage-account-overview>

Case Study Description:

Contoso Ltd (Consulting Company)

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

General Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York.

Environment

Existing Environment

Contoso has an Azure subscription named Sub1 that is linked to an Azure Active Directory (Azure AD) tenant. The network contains an on-premises Active Directory domain that syncs to the Azure AD tenant.

The Azure AD tenant contains the users shown in the following table.

Name	Type	Role
User1	Member	None
User2	Guest	None
User3	Member	None
User4	Member	None

Sub1 contains two resource groups named RG1 and RG2 and the virtual networks shown in the following table.

Name	Subnet	Peered with
VNET1	Subnet1, Subnet2	VNET2
VNET2	Subnet1	VNET1, VNET3
VNET3	Subnet1	VNET2
VNET4	Subnet1	None

User1 manages the resources in RG1. User4 manages the resources in RG2.

Sub1 contains virtual machines that run Windows Server 2019 as shown in the following table

Name	IP address	Location	Connected to
VM1	10.0.1.4	West US	VNET1/Subnet1
VM2	10.0.2.4	West US	VNET1/Subnet2
VM3	172.16.1.4	Central US	VNET2/Subnet1
VM4	192.168.1.4	West US	VNET3/Subnet1
VM5	10.0.22.4	East US	VNET4/Subnet1

No network security groups (NSGs) are associated to the network interfaces or the subnets.

Sub1 contains the storage accounts shown in the following table.

Name	Kind	Location	File share	Identity-based access for file share
storage1	Storage (general purpose v1)	West US	sharea	Azure Active Directory Domain Services (Azure AD DS)
storage2	StorageV2 (general purpose v2)	East US	shareb, sharec	Disabled
storage3	BlobStorage	East US 2	Not applicable	Not applicable
storage4	FileStorage	Central US	shared	Azure Active Directory Domain Services (Azure AD DS)

Requirements

Planned Changes

Contoso plans to implement the following changes:

- ⇒ Create a blob container named container1 and a file share named share1 that will use the Cool storage tier.
- ⇒ Create a storage account named storage5 and configure storage replication for the Blob service.
- ⇒ Create an NSG named NSG1 that will have the custom inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
500	3389	TCP	10.0.2.0/24	Any	Deny
1000	Any	ICMP	Any	VirtualNetwork	Allow

- ⇒ Associate NSG1 to the network interface of VM1.
- ⇒ Create an NSG named NSG2 that will have the custom outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
200	3389	TCP	10.0.0.0/16	VirtualNetwork	Deny
400	Any	ICMP	10.0.2.0/24	10.0.1.0/24	Allow

- ⇒ Associate NSG2 to VNET1/Subnet2.

Technical Requirements

Contoso must meet the following technical requirements:

- ⇒ Create container1 and share1.
- ⇒ Use the principle of least privilege.
- ⇒ Create an Azure AD security group named Group4.
- ⇒ Back up the Azure file shares and virtual machines by using Azure Backup.
- ⇒ Trigger an alert if VM1 or VM2 has less than 20 GB of free space on volume C.
- ⇒ Enable User1 to create Azure policy definitions and User2 to assign Azure policies to RG1.
- ⇒ Create an internal Basic Azure Load Balancer named LB1 and connect the load balancer to VNET1/Subnet1
- ⇒ Enable flow logging for IP traffic from VM5 and retain the flow logs for a period of eight months.
- ⇒ Whenever possible, grant Group4 Azure role-based access control (Azure RBAC) read-only permissions to the Azure file shares.

Question: 596

CertyIQ

HOTSPOT -

You need to create storage5. The solution must support the planned changes.

Which type of storage account should you use, and which account should you configure as the destination storage account? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Account kind:

BlobStorage
BlockBlobStorage
Storage (general purpose v1)
StorageV2 (general purpose v2)

Destination:

Storage1
Storage2
Storage3
Storage4

Answer:

Answer Area

Account kind:

BlobStorage
BlockBlobStorage
Storage (general purpose v1)
StorageV2 (general purpose v2)

Destination:

Storage1
Storage2
Storage3
Storage4

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/storage/blobs/object-replication-configure?tabs=portal>

Case Study Description:

Contoso Ltd (Consulting Company)

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

General Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in Seattle and

New York.

Environment

Existing Environment

Contoso has an Azure subscription named Sub1 that is linked to an Azure Active Directory (Azure AD) tenant. The network contains an on-premises Active Directory domain that syncs to the Azure AD tenant.

The Azure AD tenant contains the users shown in the following table.

Name	Type	Role
User1	Member	None
User2	Guest	None
User3	Member	None
User4	Member	None

Sub1 contains two resource groups named RG1 and RG2 and the virtual networks shown in the following table.

Name	Subnet	Peered with
VNET1	Subnet1, Subnet2	VNET2
VNET2	Subnet1	VNET1, VNET3
VNET3	Subnet1	VNET2
VNET4	Subnet1	None

User1 manages the resources in RG1. User4 manages the resources in RG2.

Sub1 contains virtual machines that run Windows Server 2019 as shown in the following table

Name	IP address	Location	Connected to
VM1	10.0.1.4	West US	VNET1/Subnet1
VM2	10.0.2.4	West US	VNET1/Subnet2
VM3	172.16.1.4	Central US	VNET2/Subnet1
VM4	192.168.1.4	West US	VNET3/Subnet1
VM5	10.0.22.4	East US	VNET4/Subnet1

No network security groups (NSGs) are associated to the network interfaces or the subnets.

Sub1 contains the storage accounts shown in the following table.

Name	Kind	Location	File share	Identity-based access for file share
storage1	Storage (general purpose v1)	West US	sharea	Azure Active Directory Domain Services (Azure AD DS)
storage2	StorageV2 (general purpose v2)	East US	shareb, sharec	Disabled
storage3	BlobStorage	East US 2	Not applicable	Not applicable
storage4	FileStorage	Central US	shared	Azure Active Directory Domain Services (Azure AD DS)

Requirements

Planned Changes

Contoso plans to implement the following changes:

- ⇒ Create a blob container named container1 and a file share named share1 that will use the Cool storage tier.
- ⇒ Create a storage account named storage5 and configure storage replication for the Blob service.
- ⇒ Create an NSG named NSG1 that will have the custom inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
500	3389	TCP	10.0.2.0/24	Any	Deny
1000	Any	ICMP	Any	VirtualNetwork	Allow

- ⇒ Associate NSG1 to the network interface of VM1.
- ⇒ Create an NSG named NSG2 that will have the custom outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
200	3389	TCP	10.0.0.0/16	VirtualNetwork	Deny
400	Any	ICMP	10.0.2.0/24	10.0.1.0/24	Allow

- ⇒ Associate NSG2 to VNET1/Subnet2.

Technical Requirements

Contoso must meet the following technical requirements:

- ⇒ Create container1 and share1.
- ⇒ Use the principle of least privilege.
- ⇒ Create an Azure AD security group named Group4.
- ⇒ Back up the Azure file shares and virtual machines by using Azure Backup.
- ⇒ Trigger an alert if VM1 or VM2 has less than 20 GB of free space on volume C.
- ⇒ Enable User1 to create Azure policy definitions and User2 to assign Azure policies to RG1.

- ⇒ Create an internal Basic Azure Load Balancer named LB1 and connect the load balancer to VNET1/Subnet1
- ⇒ Enable flow logging for IP traffic from VM5 and retain the flow logs for a period of eight months.
- ⇒ Whenever possible, grant Group4 Azure role-based access control (Azure RBAC) read-only permissions to the Azure file shares.

Question: 597

CertyIQ

You need to identify which storage account to use for the flow logging of IP traffic from VM5. The solution must meet the retention requirements.

Which storage account should you identify?

- A. storage1
- B. storage2
- C. storage3
- D. storage4

Answer: B

Explanation:

For at least two reasons, storage2 is the only candidate:

- Location: The storage account used must be in the same region as the NSG.
- Retention is available only if you use General Purpose v2 Storage accounts (GPv2).

Reference:

<https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-overview>

Case Study Description:

Contoso Ltd (Consulting Company)

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to

explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

General Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York.

Environment

Existing Environment

Contoso has an Azure subscription named Sub1 that is linked to an Azure Active Directory (Azure AD) tenant. The network contains an on-premises Active Directory domain that syncs to the Azure AD tenant.

The Azure AD tenant contains the users shown in the following table.

Name	Type	Role
User1	Member	None
User2	Guest	None
User3	Member	None
User4	Member	None

Sub1 contains two resource groups named RG1 and RG2 and the virtual networks shown in the following table.

Name	Subnet	Peered with
VNET1	Subnet1, Subnet2	VNET2
VNET2	Subnet1	VNET1, VNET3
VNET3	Subnet1	VNET2
VNET4	Subnet1	None

User1 manages the resources in RG1. User4 manages the resources in RG2.

Sub1 contains virtual machines that run Windows Server 2019 as shown in the following table

Name	IP address	Location	Connected to
VM1	10.0.1.4	West US	VNET1/Subnet1
VM2	10.0.2.4	West US	VNET1/Subnet2
VM3	172.16.1.4	Central US	VNET2/Subnet1
VM4	192.168.1.4	West US	VNET3/Subnet1
VM5	10.0.22.4	East US	VNET4/Subnet1

No network security groups (NSGs) are associated to the network interfaces or the subnets.

Sub1 contains the storage accounts shown in the following table.

Name	Kind	Location	File share	Identity-based access for file share
storage1	Storage (general purpose v1)	West US	sharea	Azure Active Directory Domain Services (Azure AD DS)
storage2	StorageV2 (general purpose v2)	East US	shareb, sharec	Disabled
storage3	BlobStorage	East US 2	Not applicable	Not applicable
storage4	FileStorage	Central US	shared	Azure Active Directory Domain Services (Azure AD DS)

Requirements

Planned Changes

Contoso plans to implement the following changes:

- ⇒ Create a blob container named container1 and a file share named share1 that will use the Cool storage tier.
- ⇒ Create a storage account named storage5 and configure storage replication for the Blob service.
- ⇒ Create an NSG named NSG1 that will have the custom inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
500	3389	TCP	10.0.2.0/24	Any	Deny
1000	Any	ICMP	Any	VirtualNetwork	Allow

- ⇒ Associate NSG1 to the network interface of VM1.

- ⇒ Create an NSG named NSG2 that will have the custom outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
200	3389	TCP	10.0.0.0/16	VirtualNetwork	Deny
400	Any	ICMP	10.0.2.0/24	10.0.1.0/24	Allow

- ⇒ Associate NSG2 to VNET1/Subnet2.

Technical Requirements

Contoso must meet the following technical requirements:

- ⇒ Create container1 and share1.
- ⇒ Use the principle of least privilege.
- ⇒ Create an Azure AD security group named Group4.
- ⇒ Back up the Azure file shares and virtual machines by using Azure Backup.
- ⇒ Trigger an alert if VM1 or VM2 has less than 20 GB of free space on volume C.
- ⇒ Enable User1 to create Azure policy definitions and User2 to assign Azure policies to RG1.
- ⇒ Create an internal Basic Azure Load Balancer named LB1 and connect the load balancer to VNET1/Subnet1
- ⇒ Enable flow logging for IP traffic from VM5 and retain the flow logs for a period of eight months.
- ⇒ Whenever possible, grant Group4 Azure role-based access control (Azure RBAC) read-only permissions to the Azure file shares.

Question: 598

CertyIQ

You discover that VM3 does NOT meet the technical requirements.

You need to verify whether the issue relates to the NSGs.

What should you use?

- A. Diagram in VNet1
- B. Diagnostic settings in Azure Monitor
- C. Diagnose and solve problems in Traffic Manager profiles
- D. The security recommendations in Azure Advisor
- E. IP flow verify in Azure Network Watcher

Answer: E

Explanation:

Scenario: Contoso must meet technical requirements including:

Ensure that VM3 can establish outbound connections over TCP port 8080 to the applications servers in the Montreal office.

IP flow verify checks if a packet is allowed or denied to or from a virtual machine. The information consists of direction, protocol, local IP, remote IP, local port, and remote port. If the packet is denied by a security group, the name of the rule that denied the packet is returned. While any source or destination IP can be chosen,

IP flow verify helps administrators quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment.

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview>

Case Study Description

Litware, inc.

Overview

Litware, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The Montreal office has 2,000 employees. The Seattle office has 1,000 employees. The New York office has 200 employees.

All the resources used by Litware are hosted on-premises.

Litware creates a new Azure subscription. The Azure Active Directory (Azure AD) tenant uses a domain named Litware.onmicrosoft.com. The tenant uses the P1 pricing tier.

Existing Environment

The network contains an Active Directory forest named Litware.com. All domain controllers are configured as DNS servers and host the Litware.com DNS zone.

Litware has finance, human resources, sales, research, and information technology departments. Each department has an organizational unit (OU) that contains all the accounts of that respective department. All the user accounts have the department attribute set to their respective department. New users are added frequently.

Litware.com contains a user named User1.

All the offices connect by using private links.

Litware has data centers in the Montreal and Seattle offices. Each data center has a firewall that can be configured as a VPN device.

All infrastructure servers are virtualized.

The virtualization environment contains the servers in the following table.

Name	Role	Contains virtual machine
Server1	VMWare vCenter server	VM1
Server2	Hyper-V-host	VM2

Litware uses two web applications named App1 and App2. Each instance on each web application requires 1GB of memory.

The Azure subscription contains the resources in the following table.

Name	Type
VNet1	Virtual network
VM3	Virtual machine
VM4	Virtual machine

The network security team implements several network security groups (NSGs).

Planned Changes

Litware plans to implement the following changes:

- Deploy Azure ExpressRoute to the Montreal office.
- Migrate the virtual machines hosted on Server1 and Server2 to Azure.
- Synchronize on-premises Active Directory to Azure Active Directory (Azure AD).
- Migrate App1 and App2 to two Azure web apps named webApp1 and WebApp2.

Technical requirements

Litware must meet the following technical requirements:

- Ensure that WebApp1 can adjust the number of instances automatically based on the load and can scale up to five instance*.
- Ensure that VM3 can establish outbound connections over TCP port 8080 to the applications servers in the Montreal office.
- Ensure that routing information is exchanged automatically between Azure and the routers in the Montreal office.
- Enable Azure Multi-Factor Authentication (MFA) for the users in the finance department only.
- Ensure that webapp2.azurewebsites.net can be accessed by using the name app2.Litware.com.
- Connect the New Your office to VNet1 over the Internet by using an encrypted connection.
- Create a workflow to send an email message when the settings of VM4 are modified.
- Create a custom Azure role named Role1 that is based on the Reader role.
- Minimize costs whenever possible.

Question: 599

CertyIQ

You need to ensure that VM1 can communicate with VM4. The solution must minimize the administrative effort. What should you do?

- A. Create an NSG and associate the NSG to VM1 and VM4.
- B. Establish peering between VNET1 and VNET3.
- C. Assign VM4 an IP address of 10.0.1.5/24.
- D. Create a user-defined route from VNET1 to VNET3.

Answer: B

Explanation:

Establishing peering between the virtual networks (VNETs) allows traffic to flow between them without the need for additional configuration or routing. This solution minimizes administrative effort, as it requires only a single step to set up the peering. Option A, creating an NSG, would require additional rules and configuration to allow communication between VM1 and VM4. Option C, assigning a specific IP address to VM4, does not address the issue of network communication. Option D, creating a user-defined route, would also require additional configuration and management.

Case Study Description

Litware, inc.

Overview

Litware, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The Montreal office has 2,000 employees. The Seattle office has 1,000 employees. The New York office has 200 employees.

All the resources used by Litware are hosted on-premises.

Litware creates a new Azure subscription. The Azure Active Directory (Azure AD) tenant uses a domain named Litware.onmicrosoft.com. The tenant uses the P1 pricing tier.

Existing Environment

The network contains an Active Directory forest named Litware.com. All domain controllers are configured as DNS servers and host the Litware.com DNS zone.

Litware has finance, human resources, sales, research, and information technology departments. Each department has an organizational unit (OU) that contains all the accounts of that respective department. All the user accounts have the department attribute set to their respective department. New users are added frequently.

Litware.com contains a user named User1.

All the offices connect by using private links.

Litware has data centers in the Montreal and Seattle offices. Each data center has a firewall that can be configured as a VPN device.

All infrastructure servers are virtualized.

The virtualization environment contains the servers in the following table.

Name	Role	Contains virtual machine
Server1	VMWare vCenter server	VM1
Server2	Hyper-V-host	VM2

Litware uses two web applications named App1 and App2. Each instance on each web application requires 1GB of memory.

The Azure subscription contains the resources in the following table.

Name	Type
VNet1	Virtual network
VM3	Virtual machine
VM4	Virtual machine

The network security team implements several network security groups (NSGs).

Planned Changes

Litware plans to implement the following changes:

- Deploy Azure ExpressRoute to the Montreal office.
- Migrate the virtual machines hosted on Server1 and Server2 to Azure.
- Synchronize on-premises Active Directory to Azure Active Directory (Azure AD).
- Migrate App1 and App2 to two Azure web apps named webApp1 and WebApp2.

Technical requirements

Litware must meet the following technical requirements:

- Ensure that WebApp1 can adjust the number of instances automatically based on the load and can scale up to five instance*.
- Ensure that VM3 can establish outbound connections over TCP port 8080 to the applications servers in the Montreal office.
- Ensure that routing information is exchanged automatically between Azure and the routers in the Montreal office.
- Enable Azure Multi-Factor Authentication (MFA) for the users in the finance department only.
- Ensure that webapp2.azurewebsites.net can be accessed by using the name app2.Litware.com.
- Connect the New Your office to VNet1 over the Internet by using an encrypted connection.
- Create a workflow to send an email message when the settings of VM4 are modified.
- Create a custom Azure role named Role1 that is based on the Reader role.
- Minimize costs whenever possible.

Question: 600

CertyIQ

HOTSPOT -

You need to meet the connection requirements for the New York office.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

From the Azure portal:

- Create an ExpressRoute circuit only.
- Create a virtual network gateway only.
- Create a virtual network gateway and a local network gateway.
- Create an ExpressRoute circuit and an on-premises data gateway.
- Create a virtual network gateway and an on-premises data gateway.

In the New York office:

- Deploy ExpressRoute.
- Deploy a DirectAccess server.
- Implement a Web Application Proxy.
- Configure a site-to-site VPN connection.

Answer:

Answer Area

From the Azure portal:

- Create an ExpressRoute circuit only.
- Create a virtual network gateway only.
- Create a virtual network gateway and a local network gateway.
- Create an ExpressRoute circuit and an on-premises data gateway.
- Create a virtual network gateway and an on-premises data gateway.

In the New York office:

- Deploy ExpressRoute.
- Deploy a DirectAccess server.
- Implement a Web Application Proxy.
- Configure a site-to-site VPN connection.

Explanation:

Box 1: Create a virtual network gateway and a local network gateway.

Azure VPN gateway. The VPN gateway service enables you to connect the VNet to the on-premises network through a VPN appliance. For more information, see

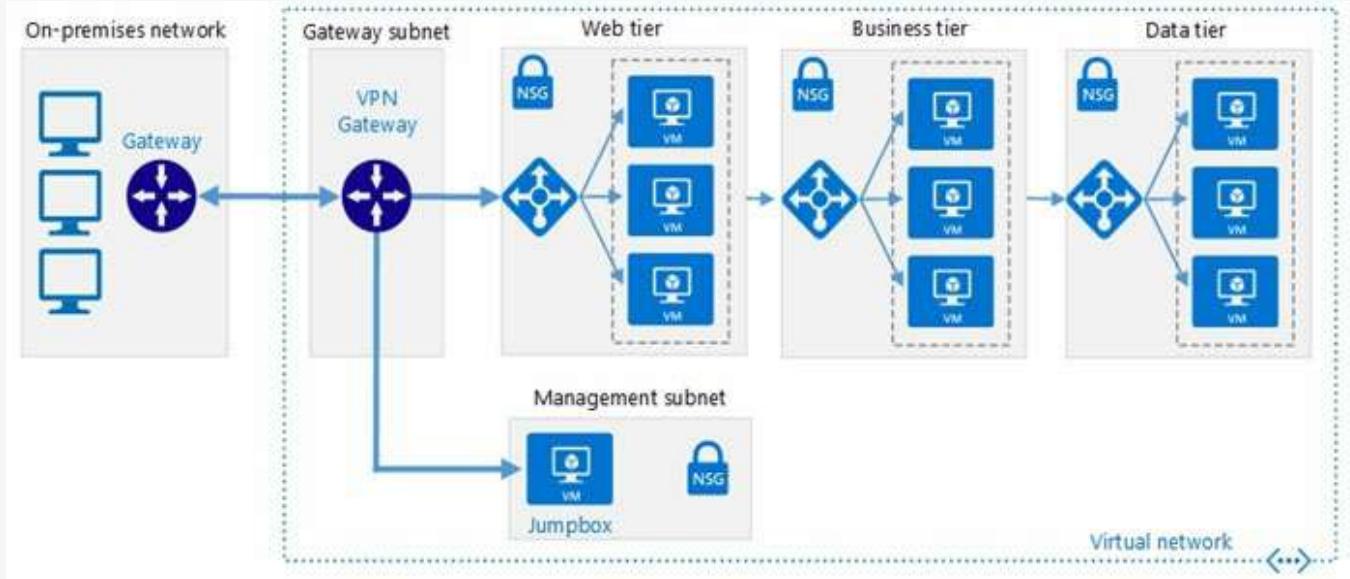
Connect an on-premises network to a Microsoft Azure virtual network. The VPN gateway includes the following elements:

- ⇒ Virtual network gateway. A resource that provides a virtual VPN appliance for the VNet. It is responsible for routing traffic from the on-premises network to the VNet.

- ⇒ Local network gateway. An abstraction of the on-premises VPN appliance. Network traffic from the cloud application to the on-premises network is routed through this gateway.
- ⇒ Connection. The connection has properties that specify the connection type (IPSec) and the key shared with the on-premises VPN appliance to encrypt traffic.
- ⇒ Gateway subnet. The virtual network gateway is held in its own subnet, which is subject to various requirements, described in the Recommendations section below.

Box 2: Configure a site-to-site VPN connection

On premises create a site-to-site connection for the virtual network gateway and the local network gateway.



Scenario: Connect the New York office to VNet1 over the Internet by using an encrypted connection.

Incorrect Answers:

Azure ExpressRoute: Established between your network and Azure, through an ExpressRoute partner. This connection is private. Traffic does not go over the internet.

Reference:

<https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/vpn>

Case Study Description

Litware, inc.

Overview

Litware, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The Montreal office has 2,000 employees. The Seattle office has 1,000 employees. The New York office has 200 employees.

All the resources used by Litware are hosted on-premises.

Litware creates a new Azure subscription. The Azure Active Directory (Azure AD) tenant uses a domain named Litware.onmicrosoft.com. The tenant uses the P1 pricing tier.

Existing Environment

The network contains an Active Directory forest named Litware.com. All domain controllers are configured as DNS servers and host the Litware.com DNS zone.

Litware has finance, human resources, sales, research, and information technology departments. Each department has an organizational unit (OU) that contains all the accounts of that respective department. All the user accounts have the department attribute set to their respective department. New users are added frequently.

Litware.com contains a user named User1.

All the offices connect by using private links.

Litware has data centers in the Montreal and Seattle offices. Each data center has a firewall that can be configured as a VPN device.

All infrastructure servers are virtualized.

The virtualization environment contains the servers in the following table.

Name	Role	Contains virtual machine
Server1	VMWare vCenter server	VM1
Server2	Hyper-V-host	VM2

Litware uses two web applications named App1 and App2. Each instance on each web application requires 1GB of memory.

The Azure subscription contains the resources in the following table.

Name	Type
VNet1	Virtual network
VM3	Virtual machine
VM4	Virtual machine

The network security team implements several network security groups (NSGs).

Planned Changes

Litware plans to implement the following changes:

- Deploy Azure ExpressRoute to the Montreal office.
- Migrate the virtual machines hosted on Server1 and Server2 to Azure.
- Synchronize on-premises Active Directory to Azure Active Directory (Azure AD).
- Migrate App1 and App2 to two Azure web apps named webApp1 and WebApp2.

Technical requirements

Litware must meet the following technical requirements:

- Ensure that WebApp1 can adjust the number of instances automatically based on the load and can scale up to five instances*.
- Ensure that VM3 can establish outbound connections over TCP port 8080 to the applications servers in the

Montreal office.

- Ensure that routing information is exchanged automatically between Azure and the routers in the Montreal office.
- Enable Azure Multi-Factor Authentication (MFA) for the users in the finance department only.
- Ensure that webapp2.azurewebsites.net can be accessed by using the name app2.Litware.com.
- Connect the New York office to VNet1 over the Internet by using an encrypted connection.
- Create a workflow to send an email message when the settings of VM4 are modified.
- Create a custom Azure role named Role1 that is based on the Reader role.
- Minimize costs whenever possible.

Question: 601

CertyIQ

HOTSPOT -

You need to recommend a solution for App1. The solution must meet the technical requirements.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Number of virtual networks:

1
2
3

Number of subnets per virtual network:

1
2
3

Answer:

Answer Area

Number of virtual networks:

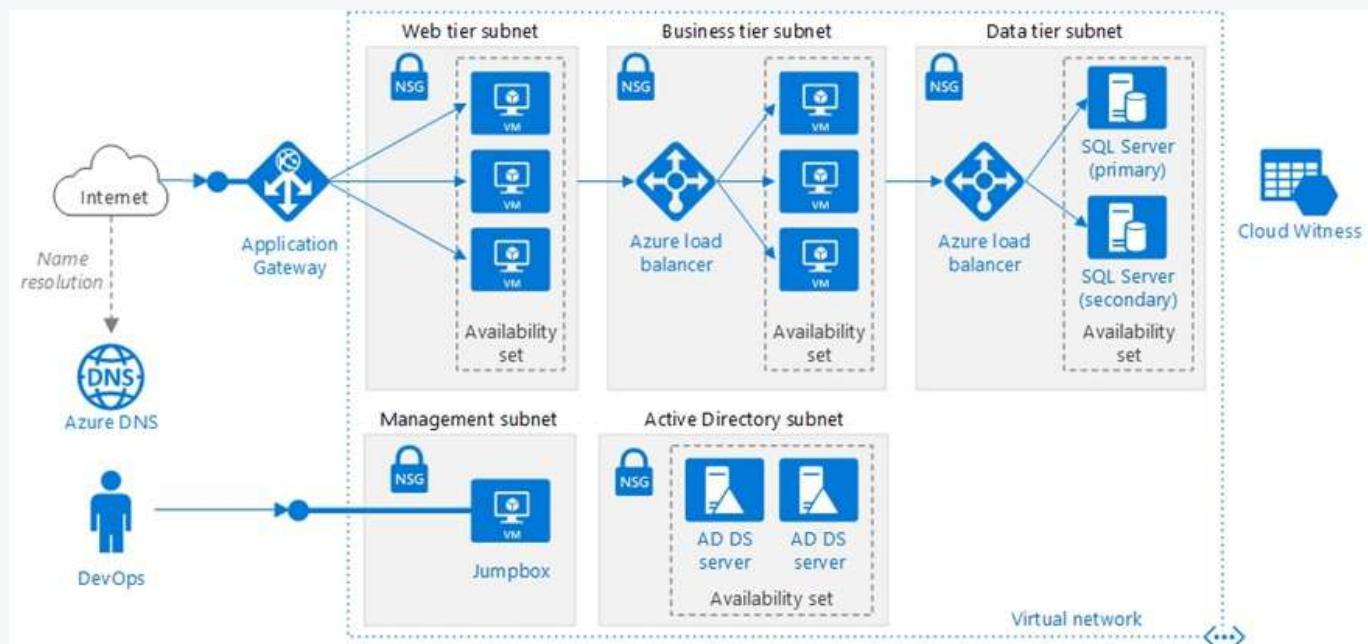
1
2
3

Number of subnets per virtual network:

1
2
3

Explanation:

This reference architecture shows how to deploy VMs and a virtual network configured for an N-tier application, using SQL Server on Windows for the data tier.



Scenario: You have a public-facing application named App1. App1 is comprised of the following three tiers:

- ⇒ A SQL database
- ⇒ A web front end
- ⇒ A processing middle tier

Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.

Technical requirements include:

- ⇒ Move all the virtual machines for App1 to Azure.

- ⇒ Minimize the number of open ports between the App1 tiers.

Reference:

<https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/n-tier/n-tier-sql-server>

Case Study Description

Contoso Ltd

Overview

Contoso, Ltd. is a manufacturing company that has offices worldwide. Contoso works with partner organizations to bring products to market.

Contoso products are manufactured by using blueprint files that the company authors and maintains.

Existing Environment

Currently, Contoso uses multiple types of servers for business operations, including the following:

- ⇒ File servers
 - ⇒ Domain controllers
 - ⇒ Microsoft SQL Server
- servers

Your network contains an Active Directory forest named contoso.com. All servers and client computers are joined to Active Directory.

You have a public-facing application named App1.

App1 is comprised of the following three tiers:

- ⇒ A SQL database
- ⇒ A web front end
- ⇒ A processing middle tier

Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.

Requirements

Planned Changes

Contoso plans to implement the following changes to the infrastructure:

- Move all the tiers of App1 to Azure.
- Move the existing product blueprint files to Azure Blob storage.
- Create a hybrid directory to support an upcoming Microsoft Office 365 migration project.

Technical Requirements

Contoso must meet the following technical requirements:

- ⇒ Move all the virtual machines for App1 to Azure.
- ⇒ Minimize the number of open ports between the App1 tiers.
- ⇒ Ensure that all the virtual machines for App1 are protected by backups.
- ⇒ Copy the blueprint files to Azure over the Internet.
- ⇒ Ensure that the blueprint files are stored in the archive storage tier.
- ⇒ Ensure that partner access to the blueprint files is secured and temporary.

- ⇒ Prevent user passwords or hashes of passwords from being stored in Azure.
- ⇒ Use unmanaged standard storage for the hard disks of the virtual machines.
- ⇒ Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.

Minimize administrative effort whenever possible.

User Requirements

Contoso identifies the following requirements for users:

- ⇒ Ensure that only users who are part of a group named Pilot can join devices to Azure AD.
- ⇒ Designate a new user named Admin1 as the service administrator of the Azure subscription.
- ⇒ Admin1 must receive email alerts regarding service outages.
- ⇒ Ensure that a new user named User3 can create network objects for the Azure subscription.

Question: 602

CertyIQ

You are planning the move of App1 to Azure.
You create a network security group (NSG).
You need to recommend a solution to provide users with access to App1.
What should you recommend?

- A. Create an incoming security rule for port 443 from the Internet. Associate the NSG to the subnet that contains the web servers.
- B. Create an outgoing security rule for port 443 from the Internet. Associate the NSG to the subnet that contains the web servers.
- C. Create an incoming security rule for port 443 from the Internet. Associate the NSG to all the subnets.
- D. Create an outgoing security rule for port 443 from the Internet. Associate the NSG to all the subnets.

Answer: A

Explanation:

Incoming and the web server subnet only, as users access the web front end by using HTTPS only.

Note Scenario: You have a public-facing application named App1. App1 is comprised of the following three tiers:

- ⇒ A SQL database
- ⇒ A web front end
- ⇒ A processing middle tier

Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.

Case Study Description

Contoso Ltd

Overview

Contoso, Ltd. is a manufacturing company that has offices worldwide. Contoso works with partner organizations to bring products to market.

Contoso products are manufactured by using blueprint files that the company authors and maintains.

Existing Environment

Currently, Contoso uses multiple types of servers for business operations, including the following:

- ⇒ File servers
- ⇒ Domain controllers
- ⇒ Microsoft SQL Server servers

Your network contains an Active Directory forest named contoso.com. All servers and client computers are joined to Active Directory.

You have a public-facing application named App1.

App1 is comprised of the following three tiers:

- ⇒ A SQL database
- ⇒ A web front end
- ⇒ A processing middle tier

Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.

Requirements

Planned Changes

Contoso plans to implement the following changes to the infrastructure:

- Move all the tiers of App1 to Azure.

- Move the existing product blueprint files to Azure Blob storage.
- Create a hybrid directory to support an upcoming Microsoft Office 365 migration project.

Technical Requirements

Contoso must meet the following technical requirements:

- ⇒ Move all the virtual machines for App1 to Azure.
- ⇒ Minimize the number of open ports between the App1 tiers.
- ⇒ Ensure that all the virtual machines for App1 are protected by backups.
- ⇒ Copy the blueprint files to Azure over the Internet.
- ⇒ Ensure that the blueprint files are stored in the archive storage tier.
- ⇒ Ensure that partner access to the blueprint files is secured and temporary.
- ⇒ Prevent user passwords or hashes of passwords from being stored in Azure.
- ⇒ Use unmanaged standard storage for the hard disks of the virtual machines.
- ⇒ Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.

Minimize administrative effort whenever possible.

User Requirements

Contoso identifies the following requirements for users:

- ⇒ Ensure that only users who are part of a group named Pilot can join devices to Azure AD.
- ⇒ Designate a new user named Admin1 as the service administrator of the Azure subscription.
- ⇒ Admin1 must receive email alerts regarding service outages.
- ⇒ Ensure that a new user named User3 can create network objects for the Azure subscription.

Question: 603

CertyIQ

HOTSPOT -

You implement the planned changes for NSG1 and NSG2.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area:

Statements	Yes	No
From VM1, you can establish a Remote Desktop session to VM2.	<input type="radio"/>	<input type="radio"/>
From VM2, you can ping VM3.	<input type="radio"/>	<input type="radio"/>
From VM2, you can establish a Remote Desktop session to VM3.	<input type="radio"/>	<input type="radio"/>

Answer:**Answer Area:**

Statements	Yes	No
From VM1, you can establish a Remote Desktop session to VM2.	<input checked="" type="radio"/>	<input type="radio"/>
From VM2, you can ping VM3.	<input checked="" type="radio"/>	<input type="radio"/>
From VM2, you can establish a Remote Desktop session to VM3.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Box 1: Yes-

The rule is configured inbound from VM1 and VM2 will allow the traffic because of stateful firewall inspection, the traffic is allowed to come in. If the traffic is initiated from VM2 then it wouldn't work.-

Box 2: Yes -

ICMP is not blocked -ping will be allowed because the vnets are already peered
traffic is initiated from VM2 and the outbound rule will block it.

Box 3: No -

NSG2 blocks RDP from VM2 -

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works>

Case Study Description:

Litware, inc.

Overview

Litware, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The Montreal office has 2,000 employees. The Seattle office has 1,000 employees. The New York office has 200 employees.

All the resources used by Litware are hosted on-premises.

Litware creates a new Azure subscription. The Azure Active Directory (Azure AD) tenant uses a domain named Litware.onmicrosoft.com. The tenant uses the P1 pricing tier.

Existing Environment

The network contains an Active Directory forest named Litware.com. All domain controllers are configured as DNS servers and host the Litware.com DNS zone.

Litware has finance, human resources, sales, research, and information technology departments. Each department has an organizational unit (OU) that contains all the accounts of that respective department. All the user accounts have the department attribute set to their respective department. New users are added frequently.

Litware.com contains a user named User1.

All the offices connect by using private links.

Litware has data centers in the Montreal and Seattle offices. Each data center has a firewall that can be configured as a VPN device.

All infrastructure servers are virtualized.

The virtualization environment contains the servers in the following table.

Name	Role	Contains virtual machine
Server1	VMWare vCenter server	VM1
Server2	Hyper-V-host	VM2

Litware uses two web applications named App1 and App2. Each instance on each web application requires 1GB of memory.

The Azure subscription contains the resources in the following table.

Name	Type
VNet1	Virtual network
VM3	Virtual machine
VM4	Virtual machine

The network security team implements several network security groups (NSGs).

Planned Changes

Litware plans to implement the following changes:

- Deploy Azure ExpressRoute to the Montreal office.
- Migrate the virtual machines hosted on Server1 and Server2 to Azure.
- Synchronize on-premises Active Directory to Azure Active Directory (Azure AD).
- Migrate App1 and App2 to two Azure web apps named webApp1 and WebApp2.

Technical requirements

Litware must meet the following technical requirements:

- Ensure that WebApp1 can adjust the number of instances automatically based on the load and can scale up to five instance*.
- Ensure that VM3 can establish outbound connections over TCP port 8080 to the applications servers in the Montreal office.
- Ensure that routing information is exchanged automatically between Azure and the routers in the Montreal office.
- Enable Azure Multi-Factor Authentication (MFA) for the users in the finance department only.
- Ensure that webapp2.azurewebsites.net can be accessed by using the name app2.Litware.com.
- Connect the New Your office to VNet1 over the Internet by using an encrypted connection.
- Create a workflow to send an email message when the settings of VM4 are modified.
- Create a custom Azure role named Role1 that is based on the Reader role.
- Minimize costs whenever possible.

Question: 604

CertyIQ

You need to ensure that you can add VM1 and VM2 to the backend pool of LB1. What should you do first?

- A. Redeploy VM1 and VM2 to the same availability zone.
- B. Connect VM2 to VNET1/Subnet1.
- C. Create a new NSG and associate the NSG to VNET1/Subnet1.
- D. Redeploy VM1 and VM2 to the same availability set.

Answer: D

Explanation:

Redeploy VM1 and VM2 to the same availability set.

For a LB basic it is required that the virtual machines are in a single availability set or scale set of virtual machines

"An existing VM cannot be added to an availability set after it is created."

<https://learn.microsoft.com/en-us/azure/virtual-machines/linux/tutorial-availability-sets>

A VM can only be added to an availability set when it is created.

"<https://learn.microsoft.com/en-us/azure/virtual-machines/windows/change-availability-set>"

If they are already in the same availability set , then you don't need to do B anyway, your a good little Azure admin, keep it up and create your backend pool with them in it. The fact that this question is being asked with no option of 'nothing' means they are not already in the same AS.

Case Study Description:

Contoso Ltd (Consulting Company)

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

General Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York.

Environment

Existing Environment

Contoso has an Azure subscription named Sub1 that is linked to an Azure Active Directory (Azure AD) tenant. The network contains an on-premises Active Directory domain that syncs to the Azure AD tenant.

The Azure AD tenant contains the users shown in the following table.

Name	Type	Role
User1	Member	None
User2	Guest	None
User3	Member	None
User4	Member	None

Sub1 contains two resource groups named RG1 and RG2 and the virtual networks shown in the following table.

Name	Subnet	Peered with
VNET1	Subnet1, Subnet2	VNET2
VNET2	Subnet1	VNET1, VNET3
VNET3	Subnet1	VNET2
VNET4	Subnet1	None

User1 manages the resources in RG1. User4 manages the resources in RG2.

Sub1 contains virtual machines that run Windows Server 2019 as shown in the following table

Name	IP address	Location	Connected to
VM1	10.0.1.4	West US	VNET1/Subnet1
VM2	10.0.2.4	West US	VNET1/Subnet2
VM3	172.16.1.4	Central US	VNET2/Subnet1
VM4	192.168.1.4	West US	VNET3/Subnet1
VM5	10.0.22.4	East US	VNET4/Subnet1

No network security groups (NSGs) are associated to the network interfaces or the subnets.

Sub1 contains the storage accounts shown in the following table.

Name	Kind	Location	File share	Identity-based access for file share
storage1	Storage (general purpose v1)	West US	sharea	Azure Active Directory Domain Services (Azure AD DS)
storage2	StorageV2 (general purpose v2)	East US	shareb, sharec	Disabled
storage3	BlobStorage	East US 2	Not applicable	Not applicable
storage4	FileStorage	Central US	shared	Azure Active Directory Domain Services (Azure AD DS)

Requirements

Planned Changes

Contoso plans to implement the following changes:

- ⇒ Create a blob container named container1 and a file share named share1 that will use the Cool storage tier.
- ⇒ Create a storage account named storage5 and configure storage replication for the Blob service.
- ⇒ Create an NSG named NSG1 that will have the custom inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
500	3389	TCP	10.0.2.0/24	Any	Deny
1000	Any	ICMP	Any	VirtualNetwork	Allow

- ⇒ Associate NSG1 to the network interface of VM1.
- ⇒ Create an NSG named NSG2 that will have the custom outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
200	3389	TCP	10.0.0.0/16	VirtualNetwork	Deny
400	Any	ICMP	10.0.2.0/24	10.0.1.0/24	Allow

- ⇒ Associate NSG2 to VNET1/Subnet2.

Technical Requirements

Contoso must meet the following technical requirements:

- ⇒ Create container1 and share1.
- ⇒ Use the principle of least privilege.
- ⇒ Create an Azure AD security group named Group4.
- ⇒ Back up the Azure file shares and virtual machines by using Azure Backup.
- ⇒ Trigger an alert if VM1 or VM2 has less than 20 GB of free space on volume C.
- ⇒ Enable User1 to create Azure policy definitions and User2 to assign Azure policies to RG1.

- ⇒ Create an internal Basic Azure Load Balancer named LB1 and connect the load balancer to VNET1/Subnet1
- ⇒ Enable flow logging for IP traffic from VM5 and retain the flow logs for a period of eight months.
- ⇒ Whenever possible, grant Group4 Azure role-based access control (Azure RBAC) read-only permissions to the Azure file shares.

Question: 605

CertyIQ

You need to add VM1 and VM2 to the backend pool of LB1.
What should you do first?

- A. Connect VM2 to VNET1/Subnet1.
- B. Redeploy VM1 and VM2 to the same availability zone.
- C. Redeploy VM1 and VM2 to the same availability set.
- D. Create a new NSG and associate the NSG to VNET1/Subnet1.

Answer: C

Explanation:

No point in Connecting VM2 to VNET1/Subnet1 as you are going to have to redeploy it anyway.

"An existing VM cannot be added to an availability set after it is created."

<https://learn.microsoft.com/en-us/azure/virtual-machines/linux/tutorial-availability-sets>

A VM can only be added to an availability set when it is created.

"<https://learn.microsoft.com/en-us/azure/virtual-machines/windows/change-availability-set>"

If they are already in the same availability set , then you don't need to do B anyway, your a good little Azure admin, keep it up and create your backend pool with them in it. The fact that this question is being asked with no option of 'nothing' means they are not already in the same AS.

Case Study Description:

Contoso Ltd (Consulting Company)

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

General Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York.

Environment

Existing Environment

Contoso has an Azure subscription named Sub1 that is linked to an Azure Active Directory (Azure AD) tenant. The network contains an on-premises Active Directory domain that syncs to the Azure AD tenant.

The Azure AD tenant contains the users shown in the following table.

Name	Type	Role
User1	Member	None
User2	Guest	None
User3	Member	None
User4	Member	None

Sub1 contains two resource groups named RG1 and RG2 and the virtual networks shown in the following table.

Name	Subnet	Peered with
VNET1	Subnet1, Subnet2	VNET2
VNET2	Subnet1	VNET1, VNET3
VNET3	Subnet1	VNET2
VNET4	Subnet1	None

User1 manages the resources in RG1. User4 manages the resources in RG2.

Sub1 contains virtual machines that run Windows Server 2019 as shown in the following table

Name	IP address	Location	Connected to
VM1	10.0.1.4	West US	VNET1/Subnet1
VM2	10.0.2.4	West US	VNET1/Subnet2
VM3	172.16.1.4	Central US	VNET2/Subnet1
VM4	192.168.1.4	West US	VNET3/Subnet1
VM5	10.0.22.4	East US	VNET4/Subnet1

No network security groups (NSGs) are associated to the network interfaces or the subnets.

Sub1 contains the storage accounts shown in the following table.

Name	Kind	Location	File share	Identity-based access for file share
storage1	Storage (general purpose v1)	West US	sharea	Azure Active Directory Domain Services (Azure AD DS)
storage2	StorageV2 (general purpose v2)	East US	shareb, sharec	Disabled
storage3	BlobStorage	East US 2	Not applicable	Not applicable
storage4	FileStorage	Central US	shared	Azure Active Directory Domain Services (Azure AD DS)

Requirements

Planned Changes

Contoso plans to implement the following changes:

- ⇒ Create a blob container named container1 and a file share named share1 that will use the Cool storage tier.
- ⇒ Create a storage account named storage5 and configure storage replication for the Blob service.
- ⇒ Create an NSG named NSG1 that will have the custom inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
500	3389	TCP	10.0.2.0/24	Any	Deny
1000	Any	ICMP	Any	VirtualNetwork	Allow

- ⇒ Associate NSG1 to the network interface of VM1.

- ⇒ Create an NSG named NSG2 that will have the custom outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
200	3389	TCP	10.0.0.0/16	VirtualNetwork	Deny
400	Any	ICMP	10.0.2.0/24	10.0.1.0/24	Allow

- ⇒ Associate NSG2 to VNET1/Subnet2.

Technical Requirements

Contoso must meet the following technical requirements:

- ⇒ Create container1 and share1.
- ⇒ Use the principle of least privilege.
- ⇒ Create an Azure AD security group named Group4.
- ⇒ Back up the Azure file shares and virtual machines by using Azure Backup.
- ⇒ Trigger an alert if VM1 or VM2 has less than 20 GB of free space on volume C.
- ⇒ Enable User1 to create Azure policy definitions and User2 to assign Azure policies to RG1.
- ⇒ Create an internal Basic Azure Load Balancer named LB1 and connect the load balancer to VNET1/Subnet1
- ⇒ Enable flow logging for IP traffic from VM5 and retain the flow logs for a period of eight months.
- ⇒ Whenever possible, grant Group4 Azure role-based access control (Azure RBAC) read-only permissions to the Azure file shares.

Question: 606

CertyIQ

You need to ensure that VM1 can communicate with VM4. The solution must minimize administrative effort.

What should you do?

- A. Create a user-defined route from VNET1 to VNET3.
- B. Create an NSG and associate the NSG to VM1 and VM4.
- C. Assign VM4 an IP address of 10.0.1.5/24.
- D. Establish peering between VNET1 and VNET3.

Answer: D

Explanation:

Correct Answer = D

Establish peering between VNET1 and VNET3.

Case Study Description

Case study

This is a case study. **Case studies are not timed separately. You can use as much exam time as you would like to complete each case.** However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the

case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the **Next** button. Use the buttons in the left pane to explore

the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an **All Information** tab, note that the information displayed is identical to the information displayed on the subsequent

tabs. When you are ready to answer a question, click the **Question** button to return to the question.

Overview

Contoso, Ltd. is a manufacturing company that has offices worldwide. Contoso works with partner organizations to bring products to market.

Contoso products are manufactured by using blueprint files that the company authors and maintains.

Existing Environment

Currently, Contoso uses multiple types of servers for business operations, including the following:

- File servers
- Domain controllers
- Microsoft SQL Server servers

Your network contains an Active Directory forest named contoso.com. All servers and client computers are joined to Active Directory.

You have a public-facing application named App1. App1 is comprised of the following three tiers:

- A SQL database
- A web front end
- A processing middle tier

Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.

Requirements

Planned Changes

Contoso plans to implement the following changes to the infrastructure:

- Move all the tiers of App1 to Azure.
- Move the existing product blueprint files to Azure Blob storage.
- Create a hybrid directory to support an upcoming Microsoft Office 365 migration project.

Technical Requirements

Contoso must meet the following technical requirements:

- Move all the virtual machines for App1 to Azure.
- Minimize the number of open ports between the App1 tiers.
- Ensure that all the virtual machines for App1 are protected by backups.
- Copy the blueprint files to Azure over the Internet.
- Ensure that the blueprint files are stored in the archive storage tier.
- Ensure that partner access to the blueprint files is secured and temporary.
- Prevent user passwords or hashes of passwords from being stored in Azure.
- Use unmanaged standard storage for the hard disks of the virtual machines.
- Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.
- Minimize administrative effort whenever possible.

User Requirements

Contoso identifies the following requirements for users:

- Ensure that only users who are part of a group named Pilot can join devices to Azure AD.
- Designate a new user named Admin1 as the service admin for the Azure subscription.
- Admin1 must receive email alerts regarding service outages.
- Ensure that a new user named User3 can create network objects for the Azure subscription.

You need to implement Role1.

Which command should you run before you create Role1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Find-RoleCapability
Get-AzureADDirectoryRole
Get-AzRoleDefinition
Get-AzResourceProvider

-Name "Reader" |

ConvertFrom-Json
ConvertFrom-String
ConvertTo-Json
ConvertTo-Xml

Answer:

Answer Area

Find-RoleCapability
Get-AzureADDirectoryRole
Get-AzRoleDefinition
Get-AzResourceProvider

-Name "Reader" |

ConvertFrom-Json
ConvertFrom-String
ConvertTo-Json
ConvertTo-Xml

Explanation:

Get-AzRoleDefinition -name "Reader" |ConvertTo-Json

<https://docs.microsoft.com/en-us/azure/role-based-access-control/role-definitions-list?tabs=roles>

Case Study Description:

Overview

Litware, Inc. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The Montreal office has 2,000 employees. The Seattle office has 1,000 employees. The New York office has 200 employees.

All the resources used by Litware are hosted on-premises.

Litware creates a new Azure subscription. The Azure Active Directory (Azure AD) tenant uses a domain named litware.onmicrosoft.com. The tenant uses the Premium P1 pricing tier.

Existing Environment

The network contains an Active Directory forest named litware.com. All domain controllers are configured as DNS servers and host the litware.com DNS zone.

Litware has finance, human resources, sales, research, and information technology departments. Each department has an organizational unit (OU) that contains all the accounts of that respective department. All the user accounts have the department attribute set to their respective department. New users are added frequently.

Litware.com contains a user named User1.

All the offices connect by using private connections.

Litware has data centers in the Montreal and Seattle offices. Each office has a firewall that can be configured as a VPN device.

All infrastructure servers are virtualized. The virtualization environment contains the servers in the following table.

Name	Role	Contains virtual machine
Server1	VMware vCenter server	VM1
Server2	Hyper-V host	VM2

Litware uses two web applications named App1 and App2. Each instance on each web application requires 1 GB of memory.

The Azure subscription contains the resources in the following table.

Name	Type
VNet1	Virtual network
VM3	Virtual machine
VM4	Virtual machine

The network security team implements several network security groups (NSGs)

Requirements

Planned Changes

Litware plans to implement the following changes:

- Deploy Azure ExpressRoute to the Montreal office.
- Migrate the virtual machines hosted on Server1 and Server2 to Azure.
- Synchronize on-premises Active Directory to Azure Active Directory (Azure AD).
- Migrate App1 and App2 to two Azure web apps named WebApp1 and WebApp2.

Technical Requirements

Litware must meet the following technical requirements:

- Ensure that WebApp1 can adjust the number of instances automatically based on the load and can scale up to five instances.
- Ensure that VM3 can establish outbound connections over TCP port 8080 to the applications servers in the Montreal office.
- Ensure that routing information is exchanged automatically between Azure and the routers in the Montreal office.
- Enable Azure Multi-Factor Authentication (MFA) for the users in the finance department only.
- Ensure that webapp2.azurewebsites.net can be accessed by using the name app2.litware.com.
- Connect the New York office to VNet1 over the Internet by using an encrypted connection.
- Create a workflow to send an email message when the settings of VM4 are modified.
- Create a custom Azure role named Role1 that is based on the Reader role.
- Minimize costs whenever possible.

Question: 608

CertyIQ

You need to recommend a solution to automate the configuration for the finance department users. The solution must meet the technical requirements.

What should you include in the recommendation?

- A. Azure AD B2C
- B. dynamic groups and conditional access policies
- C. Azure AD Identity Protection
- D. an Azure logic app and the Microsoft Identity Management (MIM) client

Answer: B

Explanation:

Scenario:

Ensure Azure Multi-Factor Authentication (MFA) for the users in the finance department only.

The recommendation is to use conditional access policies that can then be targeted to groups of users, specific applications, or other conditions.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates>

Case Study Description:

Overview

Litware, Inc. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The Montreal office has 2,000 employees. The Seattle office has 1,000 employees. The New York office has 200 employees.

All the resources used by Litware are hosted on-premises.

Litware creates a new Azure subscription. The Azure Active Directory (Azure AD) tenant uses a domain named litware.onmicrosoft.com. The tenant uses the Premium P1 pricing tier.

Existing Environment

The network contains an Active Directory forest named litware.com. All domain controllers are configured as DNS servers and host the litware.com DNS zone.

Litware has finance, human resources, sales, research, and information technology departments. Each department has an organizational unit (OU) that contains all the accounts of that respective department. All the

user accounts have the department attribute set to their respective department. New users are added frequently.

Litware.com contains a user named User1.

All the offices connect by using private connections.

Litware has data centers in the Montreal and Seattle offices. Each office has a firewall that can be configured as a VPN device.

All infrastructure servers are virtualized. The virtualization environment contains the servers in the following table.

Name	Role	Contains virtual machine
Server1	VMware vCenter server	VM1
Server2	Hyper-V host	VM2

Litware uses two web applications named App1 and App2. Each instance on each web application requires 1 GB of memory.

The Azure subscription contains the resources in the following table.

Name	Type
VNet1	Virtual network
VM3	Virtual machine
VM4	Virtual machine

The network security team implements several network security groups (NSGs)

Requirements

Planned Changes

Litware plans to implement the following changes:

- Deploy Azure ExpressRoute to the Montreal office.
- Migrate the virtual machines hosted on Server1 and Server2 to Azure.
- Synchronize on-premises Active Directory to Azure Active Directory (Azure AD).
- Migrate App1 and App2 to two Azure web apps named WebApp1 and WebApp2.

Technical Requirements

Litware must meet the following technical requirements:

- Ensure that WebApp1 can adjust the number of instances automatically based on the load and can scale up to five instances.
- Ensure that VM3 can establish outbound connections over TCP port 8080 to the applications servers in the Montreal office.
- Ensure that routing information is exchanged automatically between Azure and the routers in the Montreal office.
- Enable Azure Multi-Factor Authentication (MFA) for the users in the finance department only.
- Ensure that webapp2.azurewebsites.net can be accessed by using the name app2.litware.com.
- Connect the New York office to VNet1 over the Internet by using an encrypted connection.
- Create a workflow to send an email message when the settings of VM4 are modified.
- Create a custom Azure role named Role1 that is based on the Reader role.
- Minimize costs whenever possible.

Thank you

Thank you for being so interested in the premium exam material.

I'm glad to hear that you found it informative and helpful.

If you have any feedback or thoughts on the bumps, I would love to hear them.
Your insights can help me improve our writing and better understand our readers.

Best of Luck

You have worked hard to get to this point, and you are well-prepared for the exam
Keep your head up, stay positive, and go show that exam what you're made of!

[Feedback](#)

[More Papers](#)



Future is Secured
100% Pass Guarantee



24/7 Customer Support
Mail us - certyiqofficial@gmail.com



Free Updates
Lifetime Free Updates!

Total: **608 Questions**

Link: <https://certyiq.com/papers/microsoft/az-104>