complete your programming course about resources, doubts and more!

Microsoft

(AZ-104)

Microsoft Azure Administrator

Total: **608 Questions**

Link:

Question: 1

Your company has serval 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

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

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

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

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

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:

https://365lab.net/2015/04/11/switch-usage-model-in-azure-multi-factor-authentication-server/

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:

https://365lab.net/2015/04/11/switch-usage-model-in-azure-multi-factor-authentication-server/

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:

Effective September 1st, 2018 new auth providers may no longer be created. Existing auth providers may 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

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

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

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

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

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

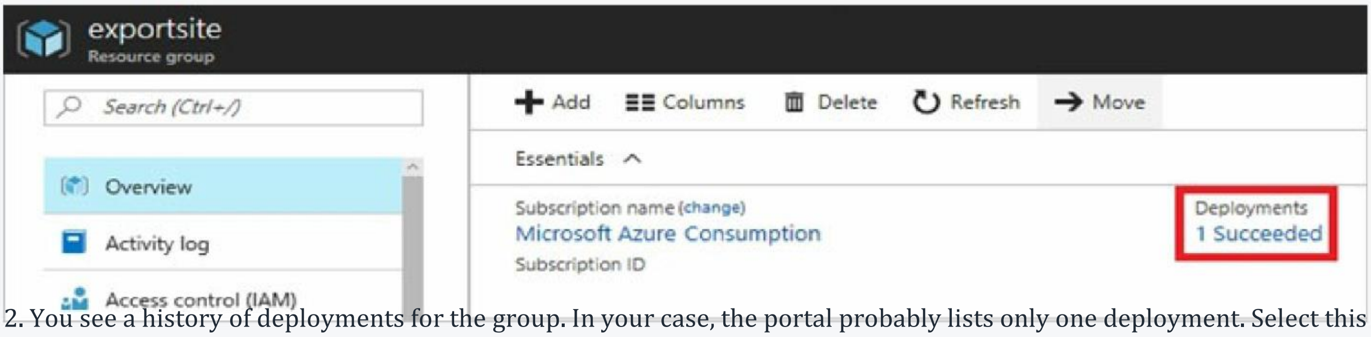
Question: 14

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?

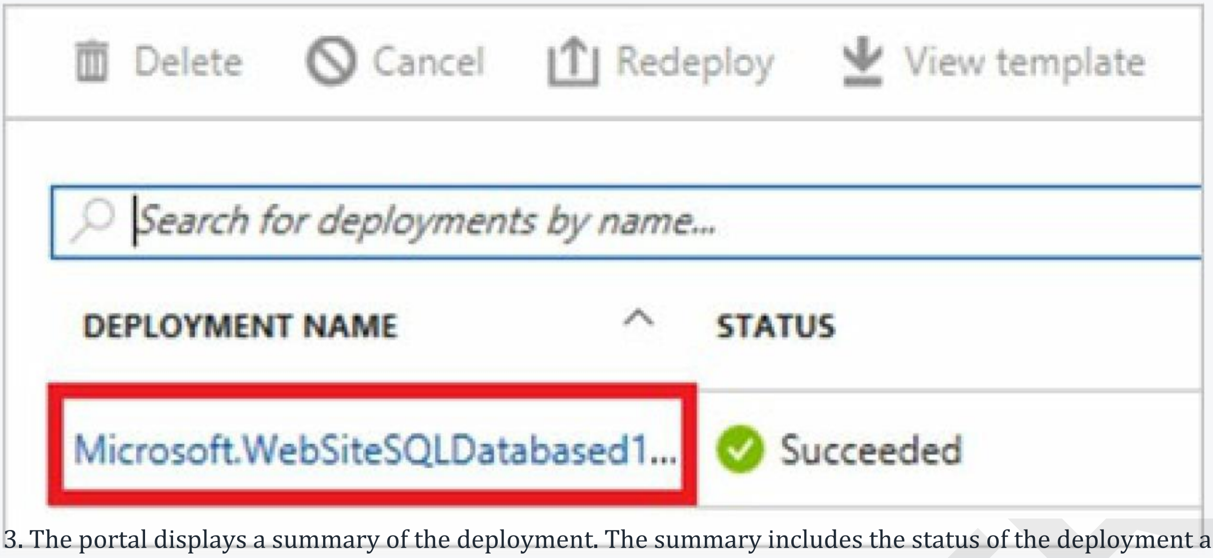
A. Yes
B. No

Answer: A

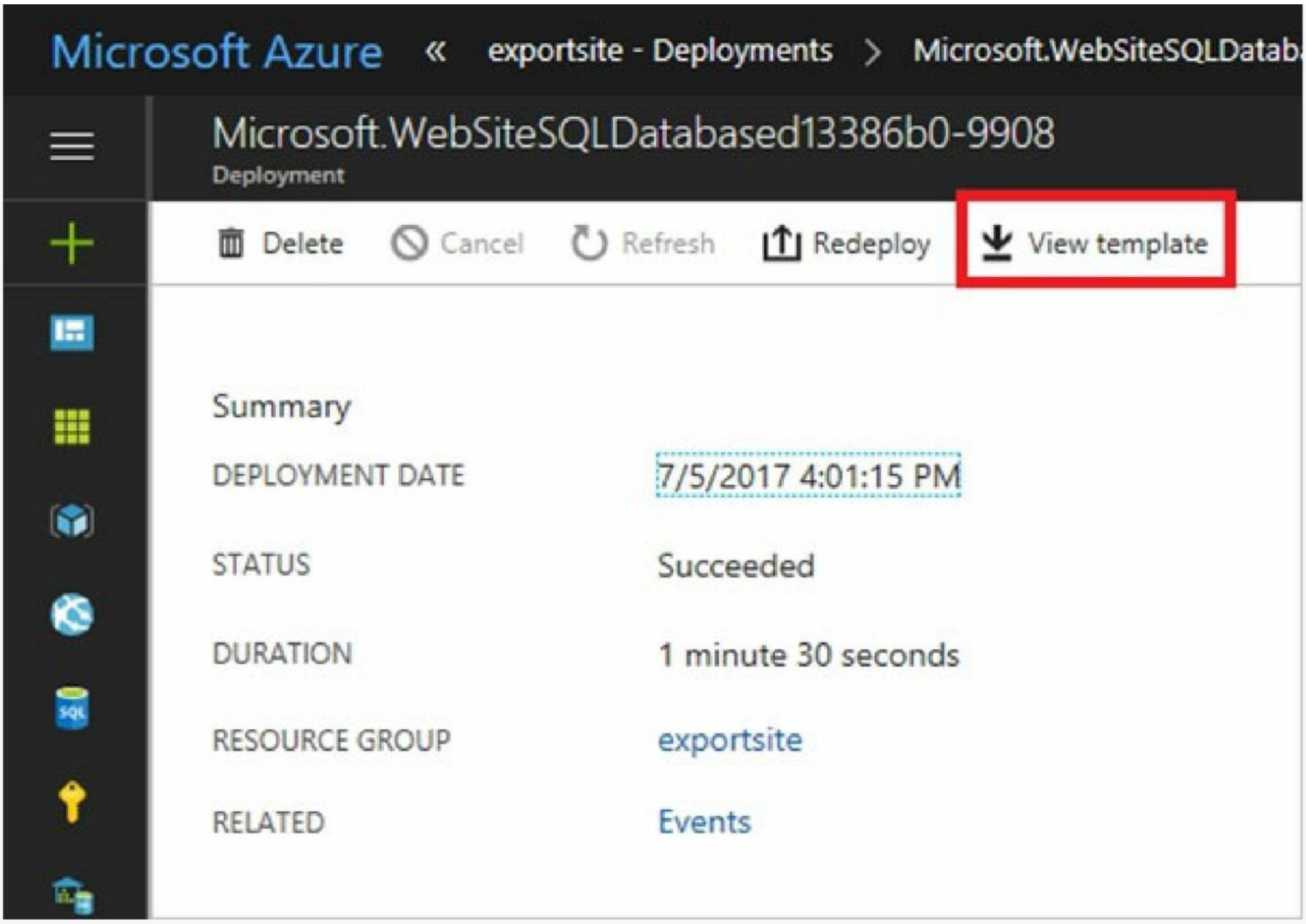
Explanation:
To view a template from deployment history:
1. Go to the resource group for your new resource group. Notice that the portal shows the result of the last deployment. Select this link.



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


Delete
Cancel
Redeploy
View template
Search for deployments by 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 Azure « exportsite - Deployments > Microsoft.WebSiteSQLDatab
Microsoft.WebSiteSQLDatabased13386b0-9908
Deployment
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

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

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

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

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

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

DRAG DROP -

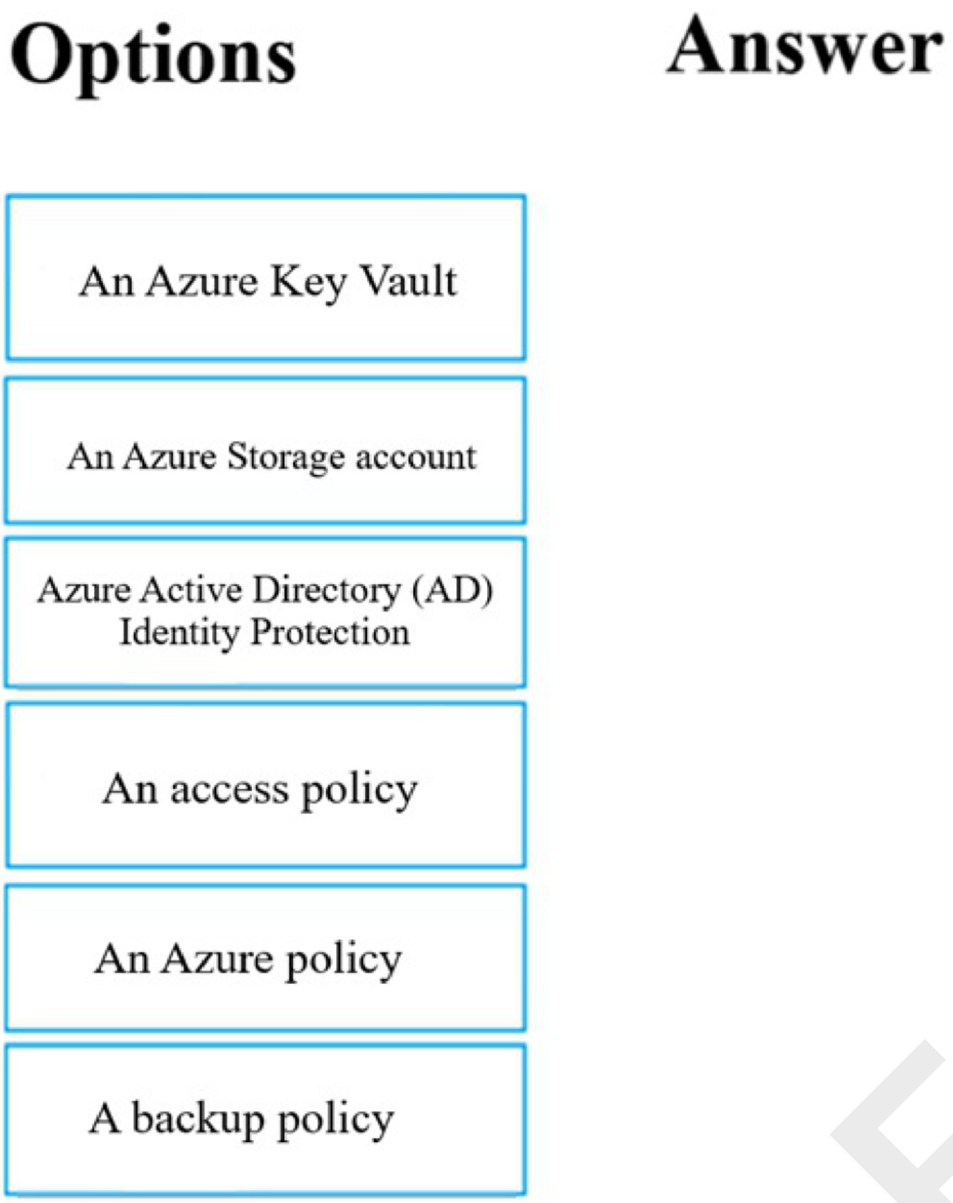
You have downloaded an Azure Resource Manager (ARM) template to deploy numerous virtual machines (VMs).

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

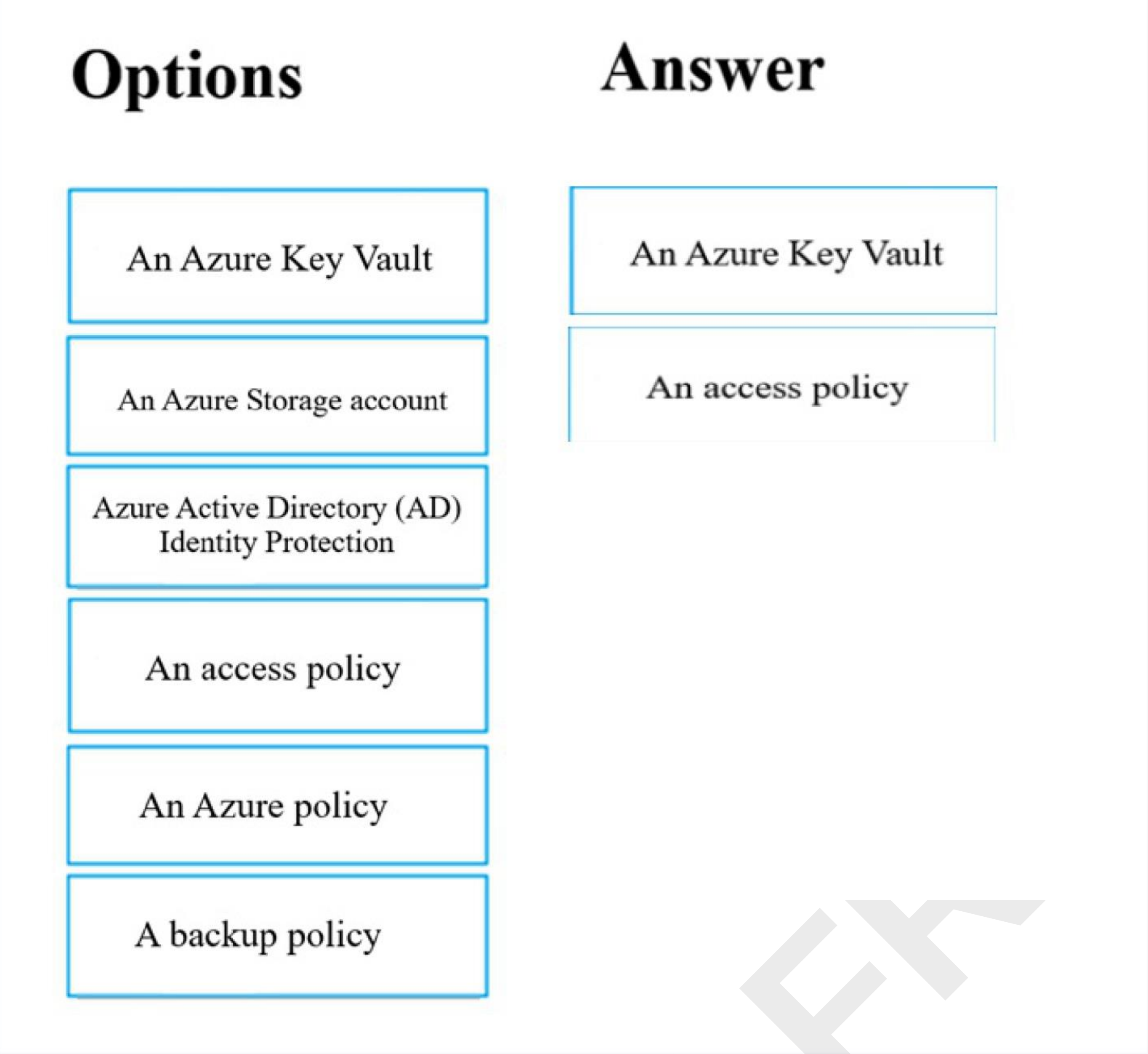
Azure Active Directory (AD) Identity Protection

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

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

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:

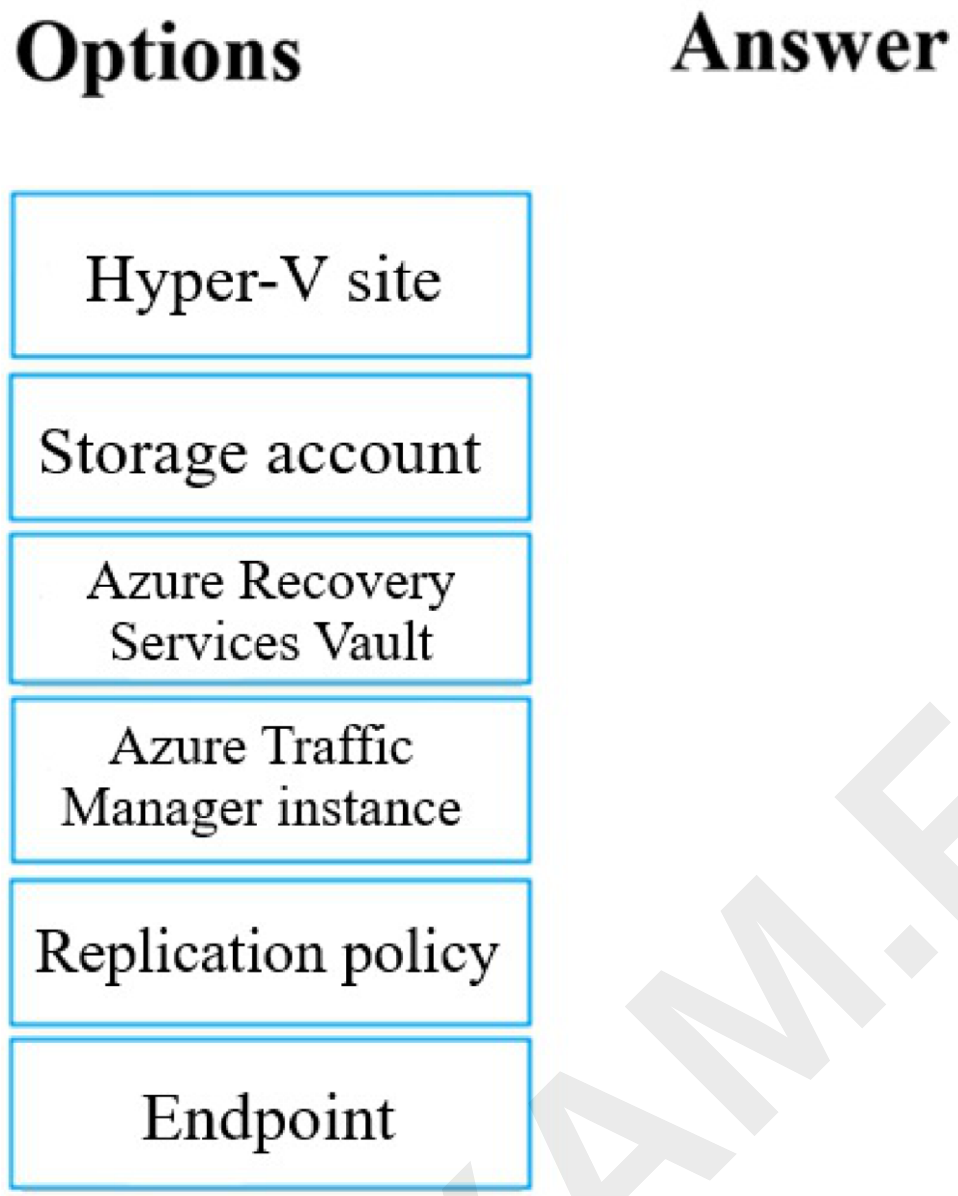
The Add-AzVhd cmdlet uploads on-premises virtual hard disks, in .vhd file format, to a blob storage account as fixed virtual hard disks.

Reference:

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

Question: 23

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

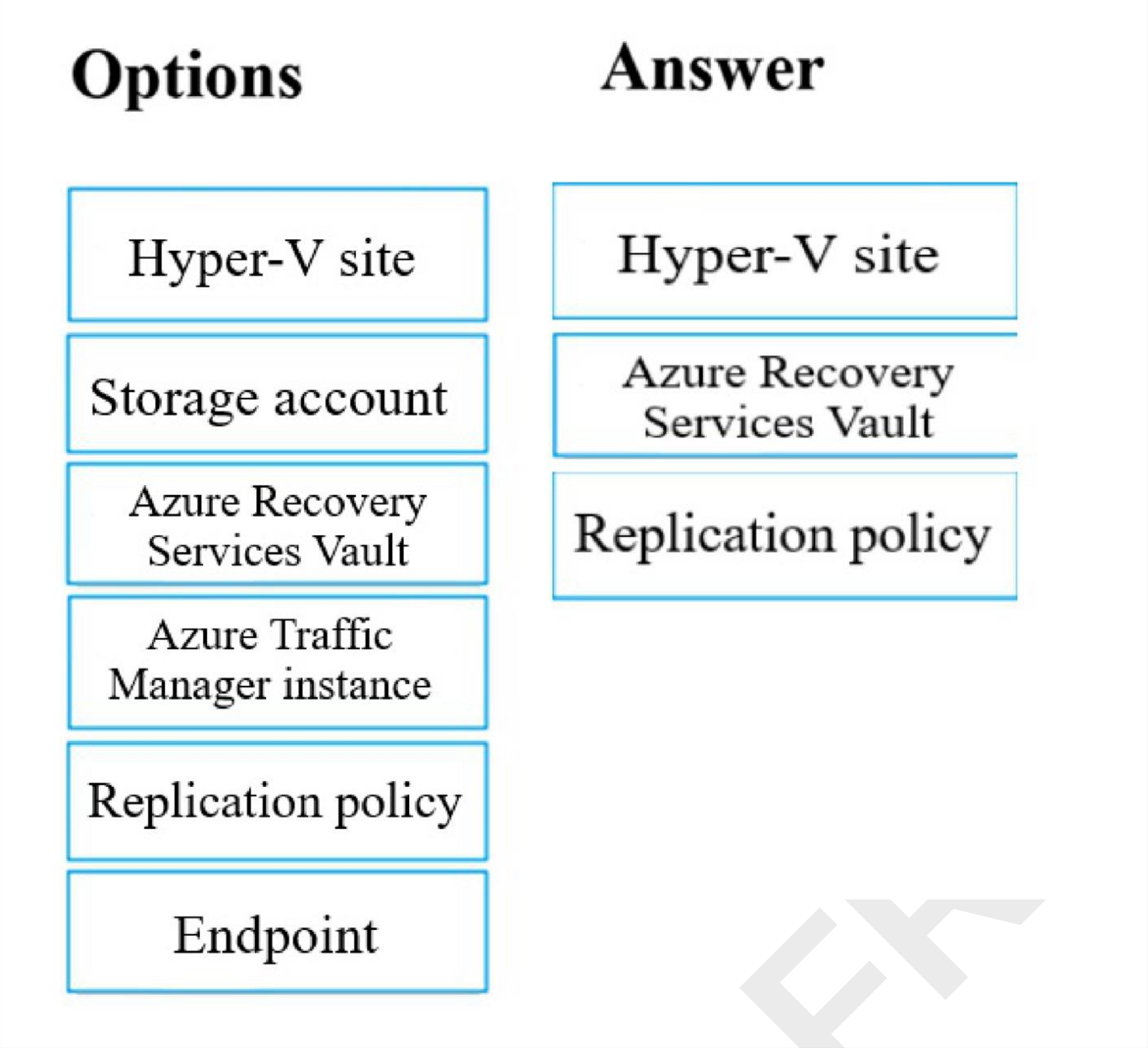
Azure Recovery Services Vault

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

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

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

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

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:

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways

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

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

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

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

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

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

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

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

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

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.

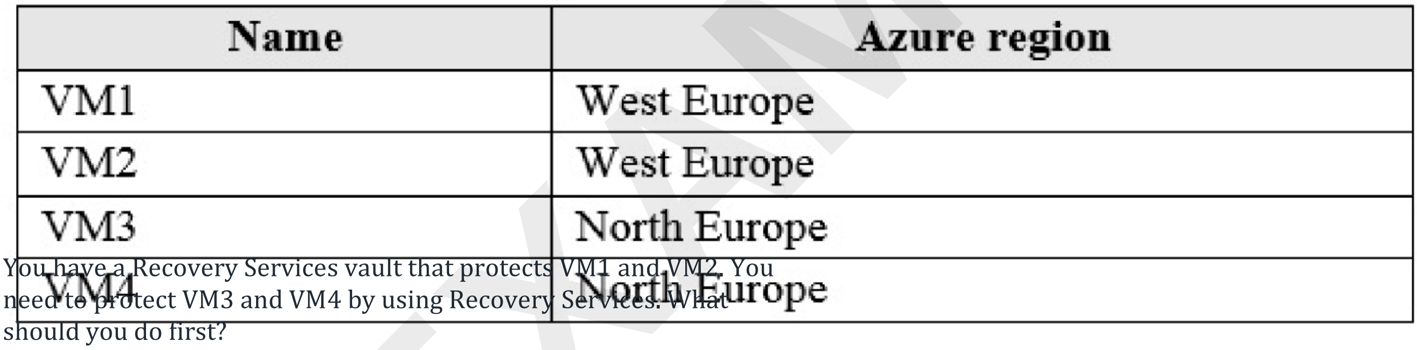
Yes, this solution should meet the goal. The New-AzureADMSInvitation cmdlet can be used to send invitations to external users to become guest users in an Azure AD tenant. By running the cmdlet for each external user listed in the CSV file, a guest user account can be created in the contoso.com Azure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

Reference:

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

Question: 41

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

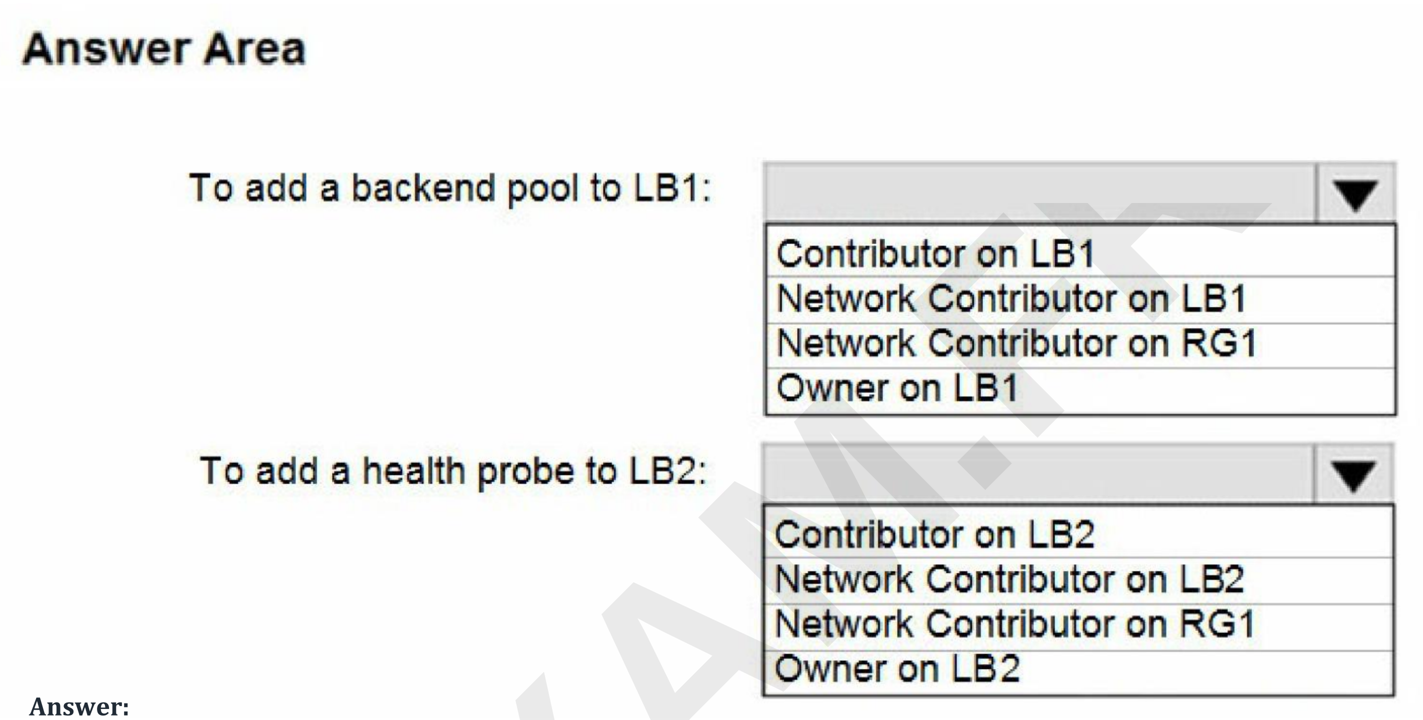
Reference:

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

Question: 42

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:

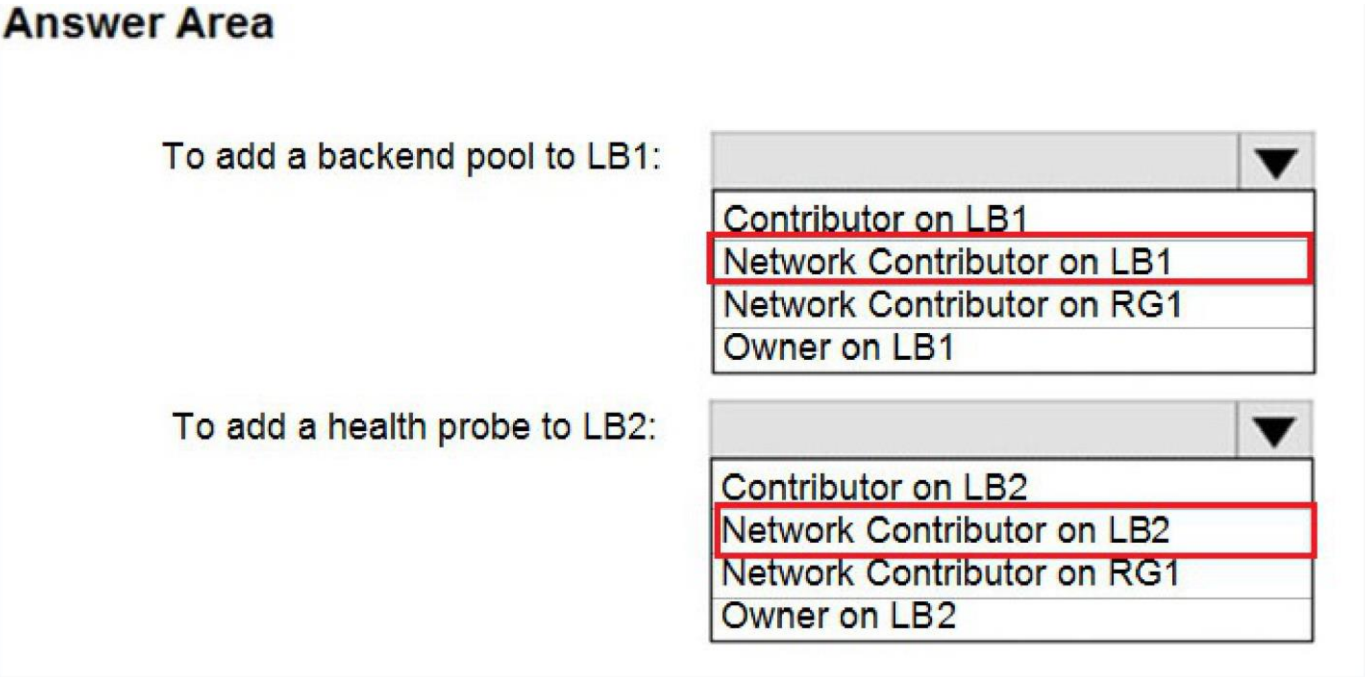


Answer Area

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

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

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:

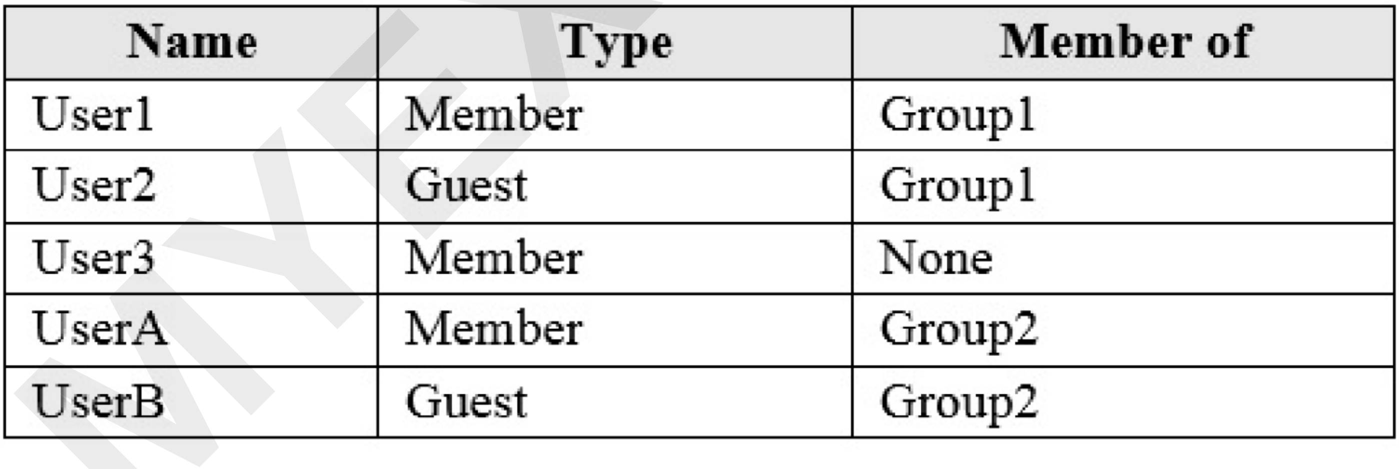
B, D, E: You can set expiration policy only for Office 365 groups in Azure Active Directory (Azure AD).

Reference:

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

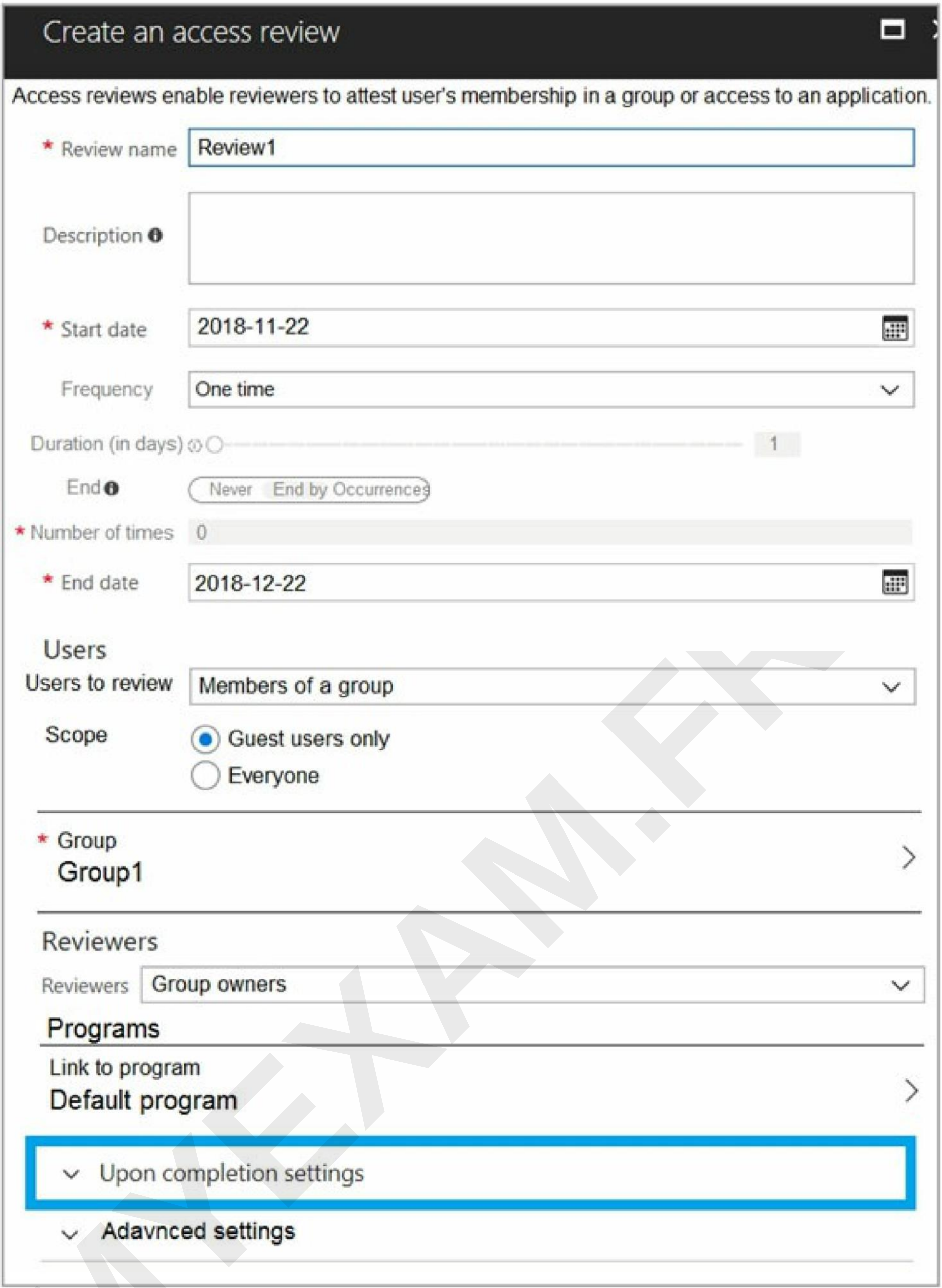
Question: 45

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:

* Start date: 2018-11-22

Frequency: One time

Duration (in days): 1

End: Never | End by Occurrences

* Number of times: 0

* End date: 2018-12-22

Users

Users to review: Members of a group

Scope: ● Guest users only ○ Everyone

* Group: Group1

Reviewers

Reviewers: Group owners

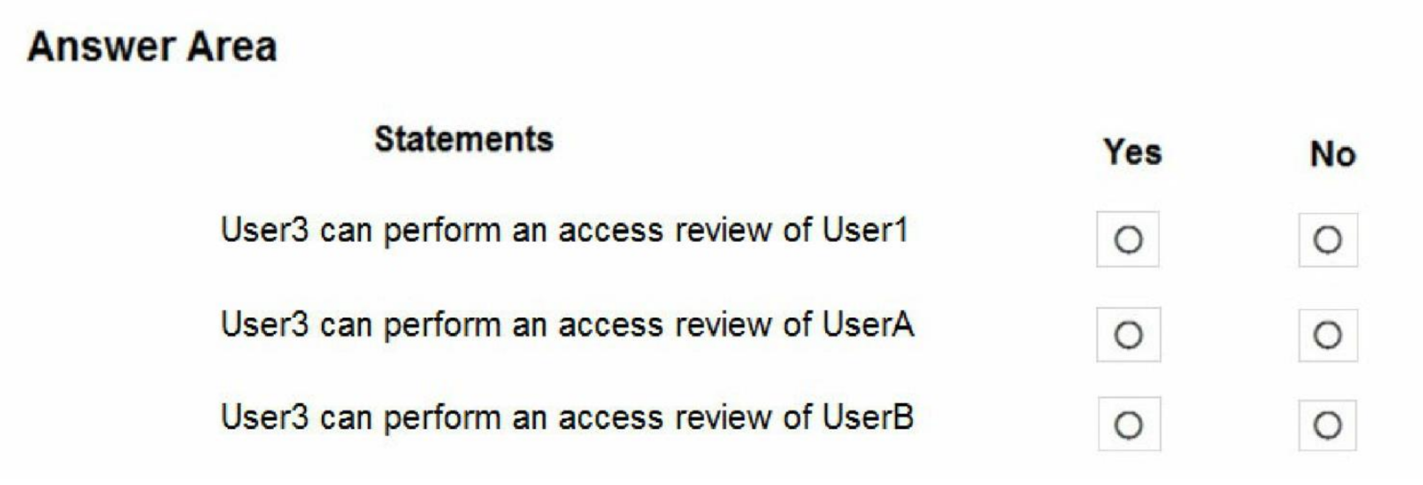
Programs

Link to program: Default program

Upon completion settings

Adavnced settings

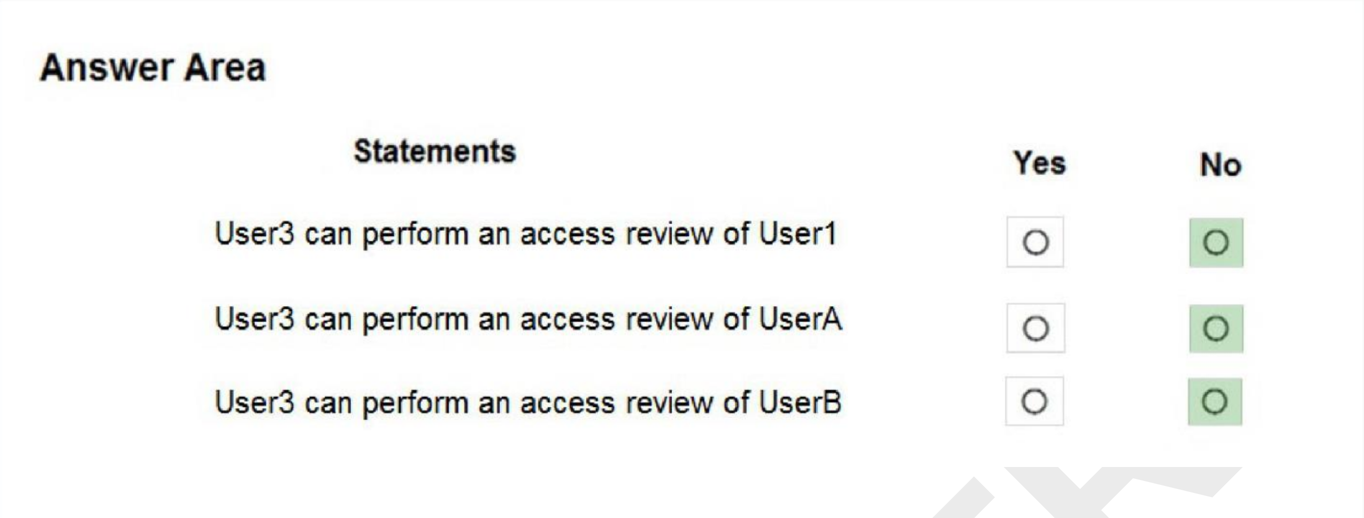
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

Statements	Yes	No
User3 can perform an access review of User1	○	○
User3 can perform an access review of UserA	○	○
User3 can perform an access review of UserB	○	○

Answer:



Answer Area

Statements	Yes	No
User3 can perform an access review of User1	○	[✓ ○]
User3 can perform an access review of UserA	○	[✓ ○]
User3 can perform an access review of UserB	○	[✓ ○]

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.

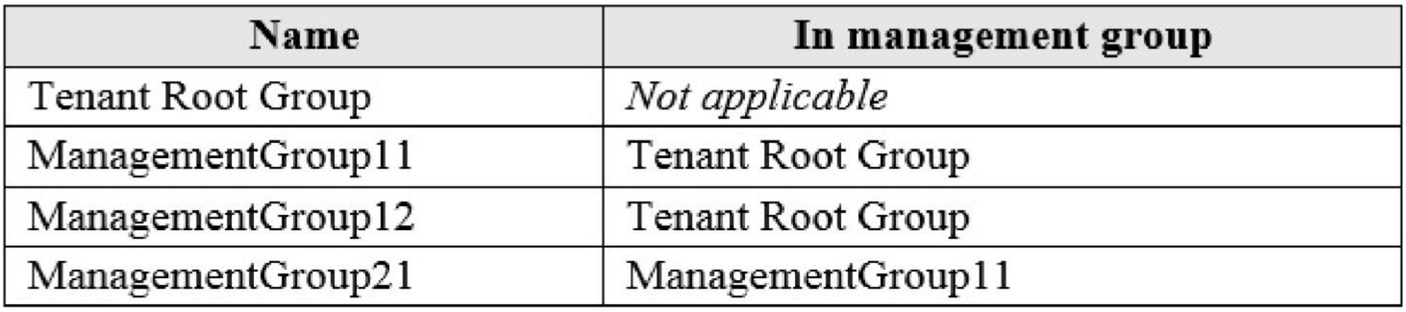
Reference:

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

Question: 46 HOTSPOT

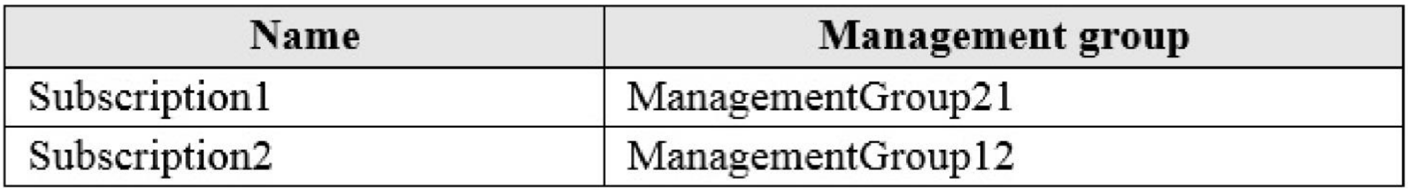
-

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



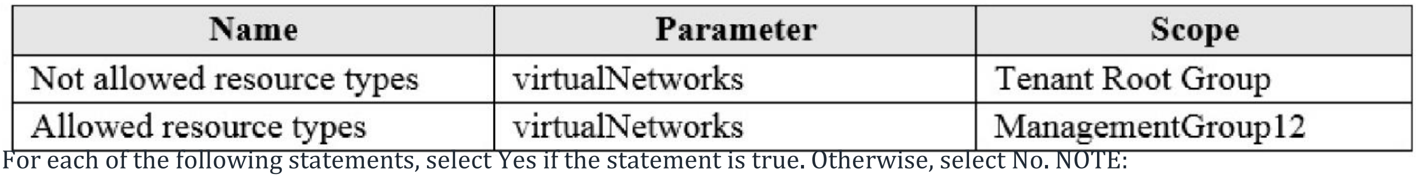
Name	In management group
Tenant Root Group	*Not applicable*
ManagementGroup11	Tenant Root Group
ManagementGroup12	Tenant Root Group
ManagementGroup21	ManagementGroup11

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



Name	Management group
Subscription1	ManagementGroup21
Subscription2	ManagementGroup12

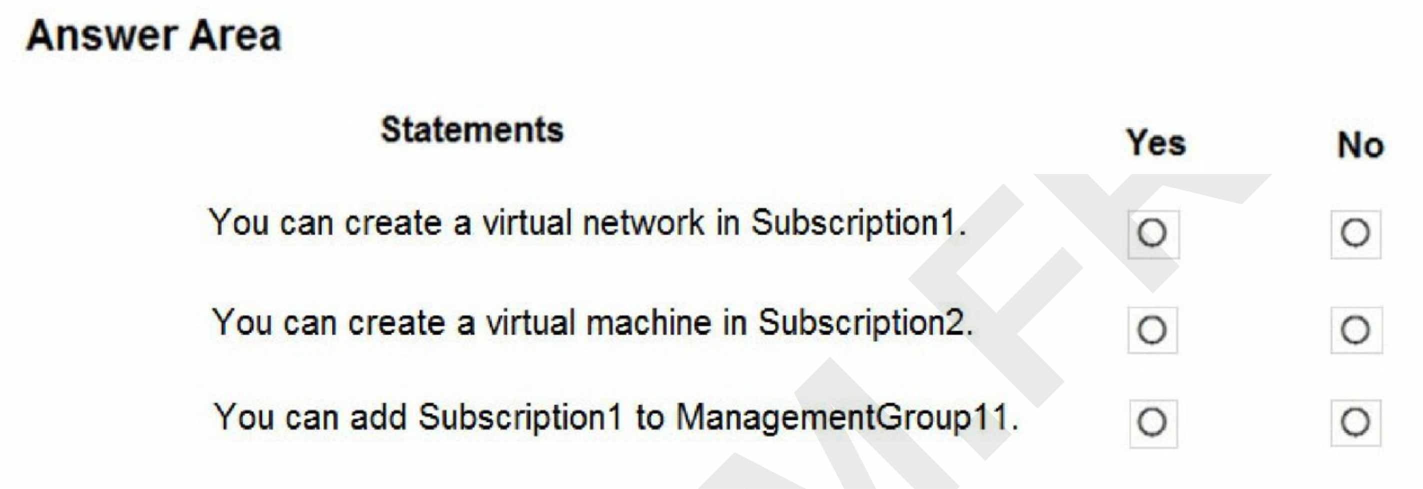
You create the Azure policies shown in the following table:



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.

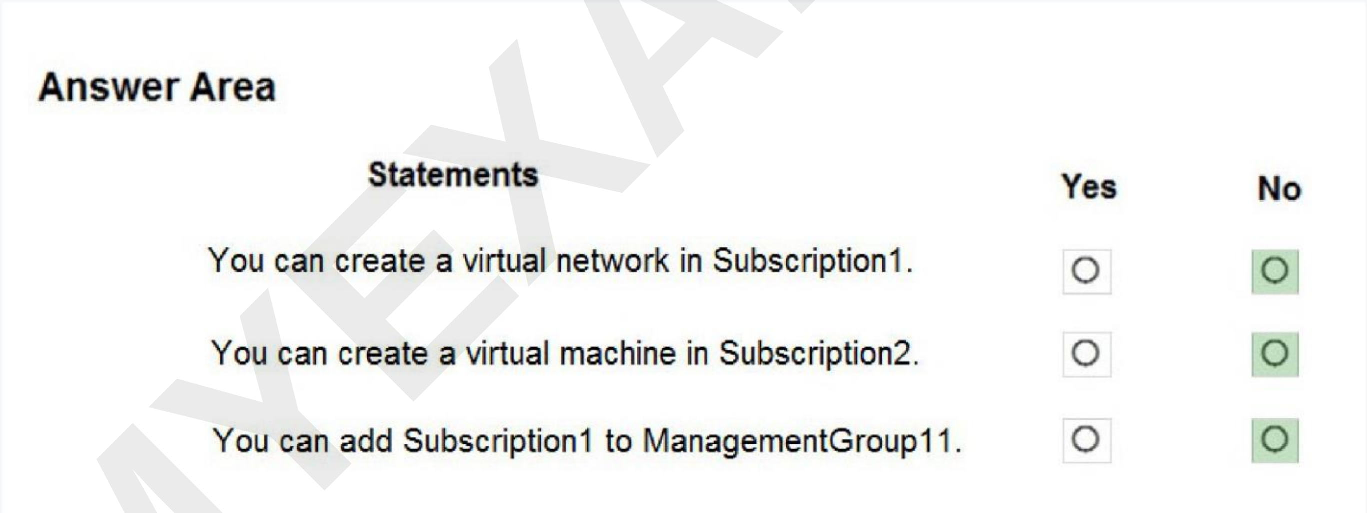
Hot Area:



Answer Area

Statements	Yes	No
You can create a virtual network in Subscription1.	○	○
You can create a virtual machine in Subscription2.	○	○
You can add Subscription1 to ManagementGroup11.	○	○

Answer:



Answer Area

Statements	Yes	No
You can create a virtual network in Subscription1.	○	●
You can create a virtual machine in Subscription2.	○	●
You can add Subscription1 to ManagementGroup11.	○	●

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 -

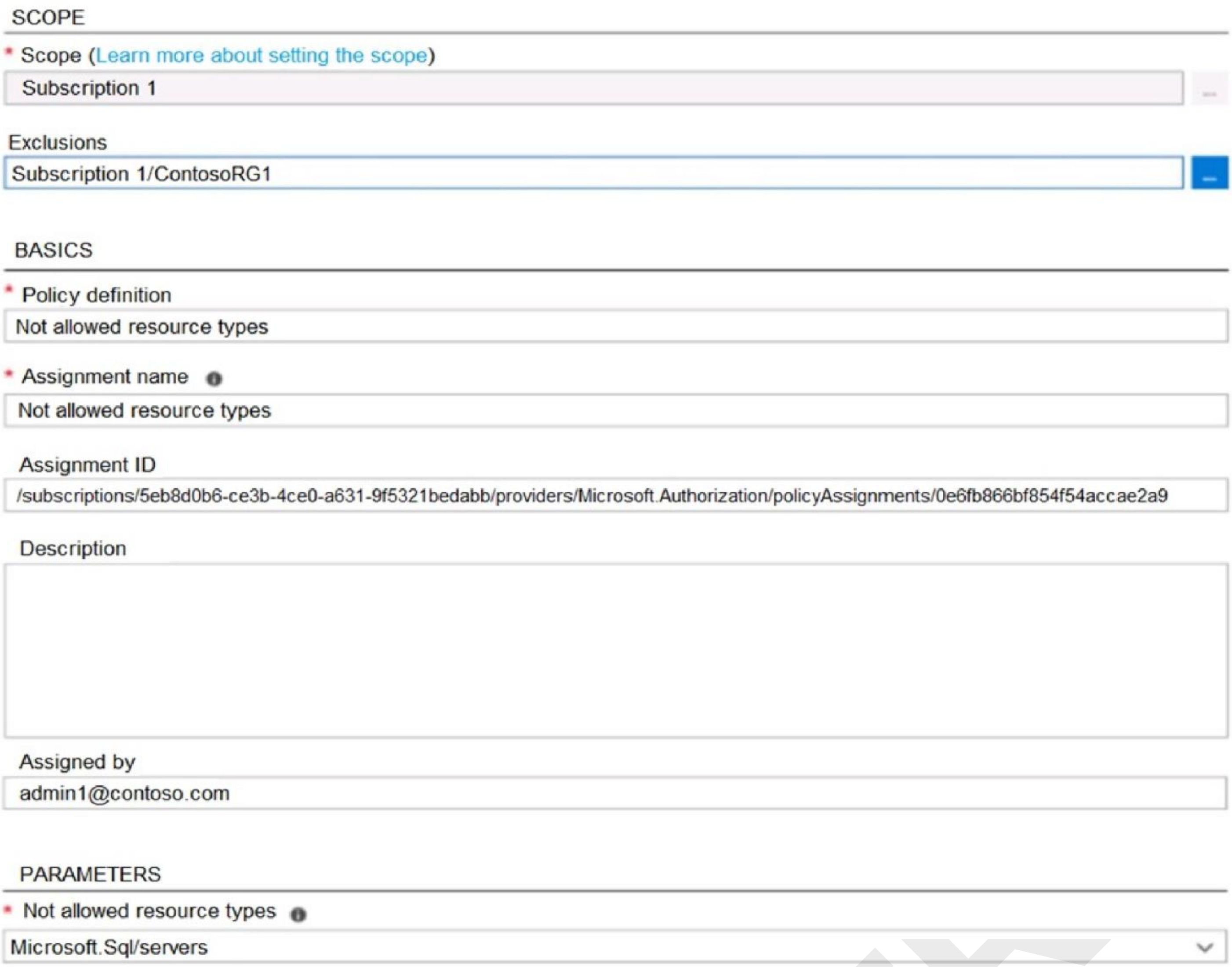
Already in one Management group called 21, so cannot add into another. A Subscription can be assigned to 1 Management Group

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

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.

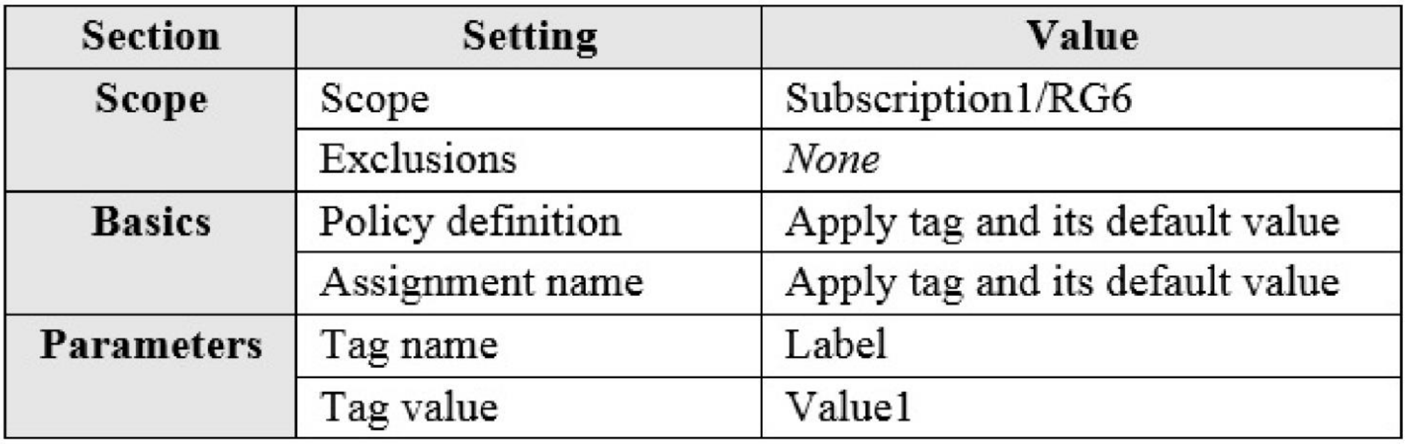
Question: 48

HOTSPOT -

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

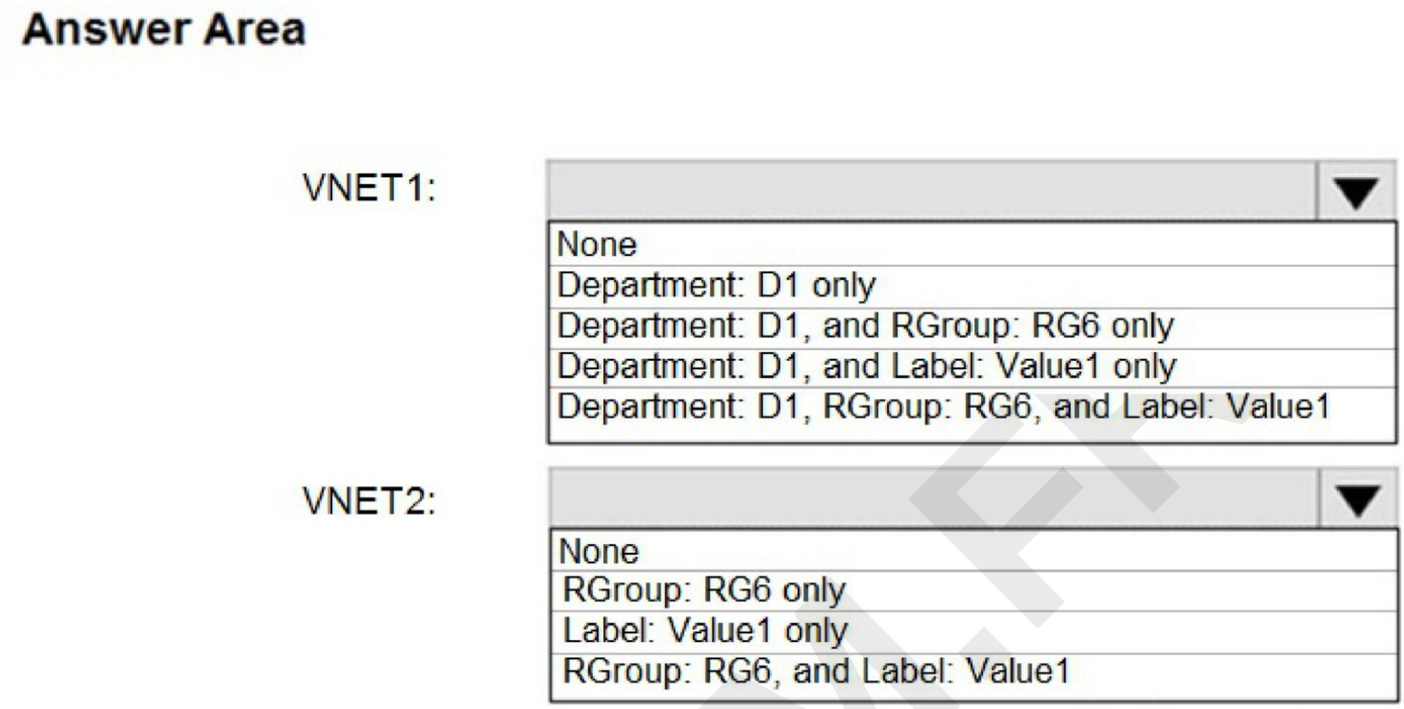
Name	Type	Resource group	Tag
RG6	Resource group	*Not applicable*	*None*
VNET1	Virtual network	RG6	Department: D1

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



Section	Setting	Value
Scope	Scope	Subscription1/RG6
	Exclusions	*None*
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:

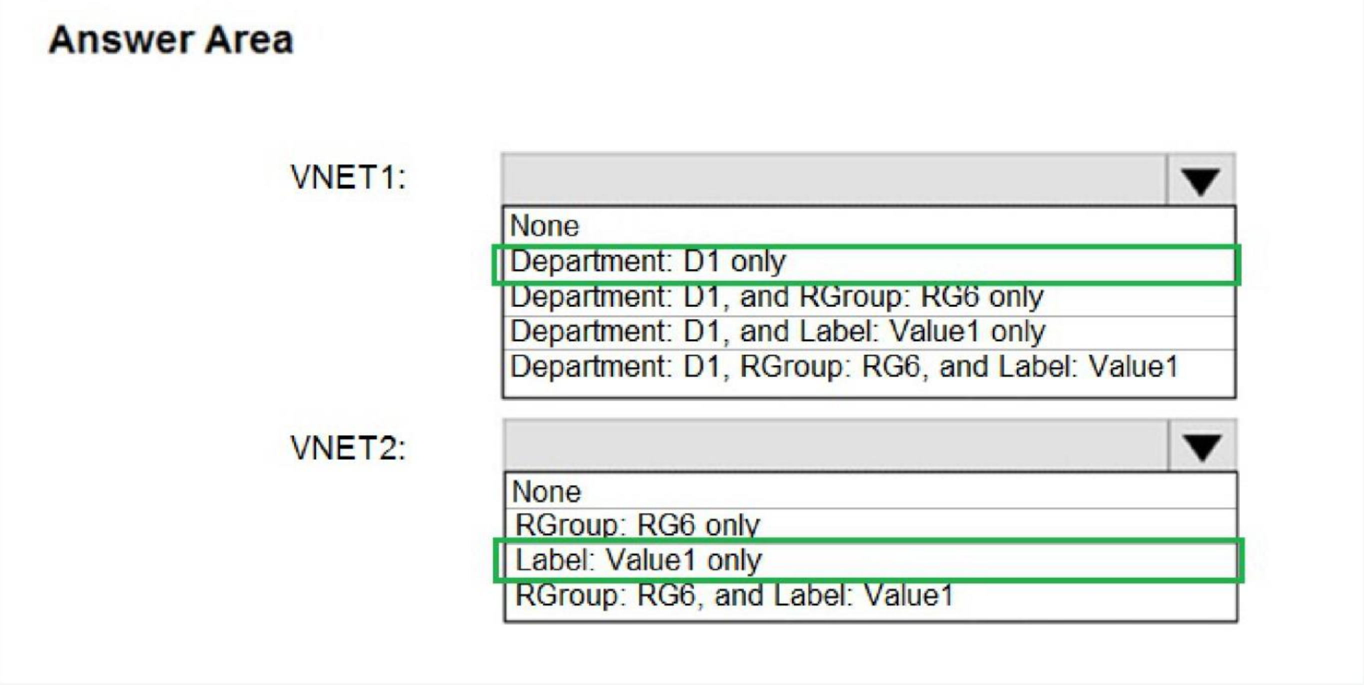


Answer Area

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:

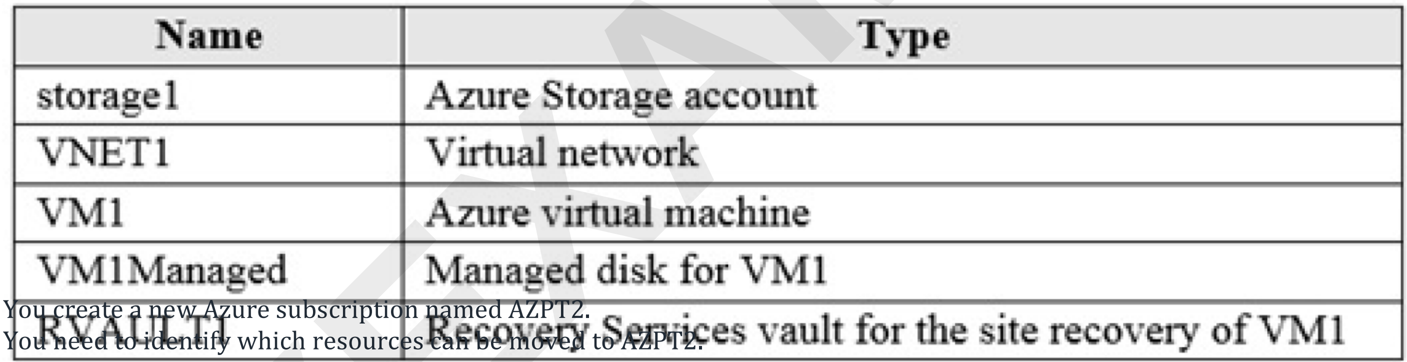
Tags are not inherited. The tag was only applied to the resource group, the VNET2 resource won't inherit it

Reference:

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

Question: 49

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

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

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-az ure-portal

Question: 52

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

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

Question: 54

You sign up for Azure Active Directory (Azure AD) Premium P2.
You need to add a user named [email protected] 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

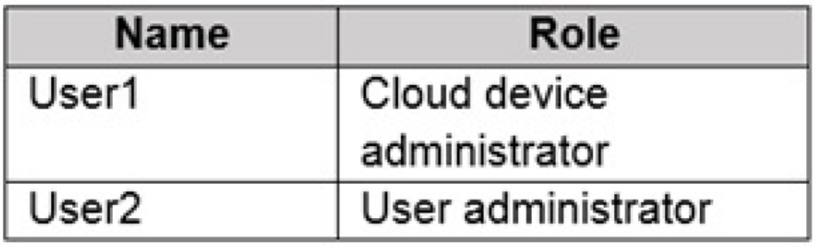
In the Azure portal, you can manage the device administrator role on the Devices page. To open the Devices page:

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

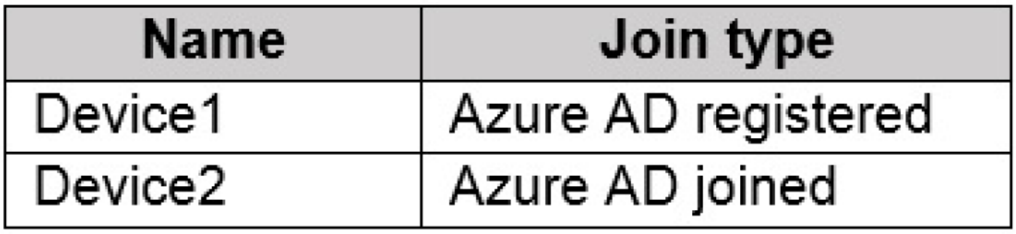
Question: 55

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



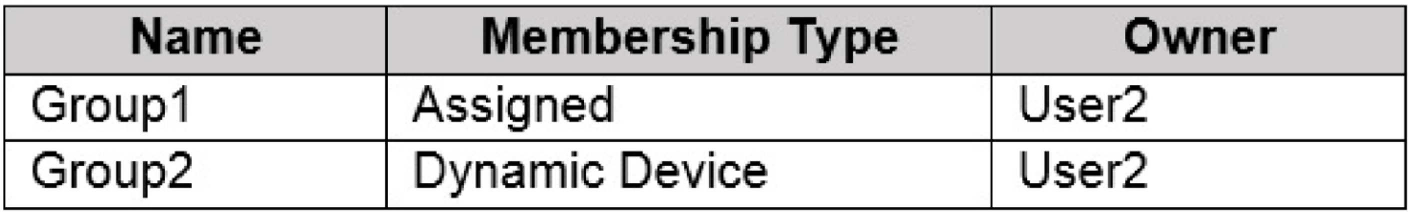
Name	Role
User1	Cloud device administrator
User2	User administrator

Contoso.com includes following Windows 10 devices:



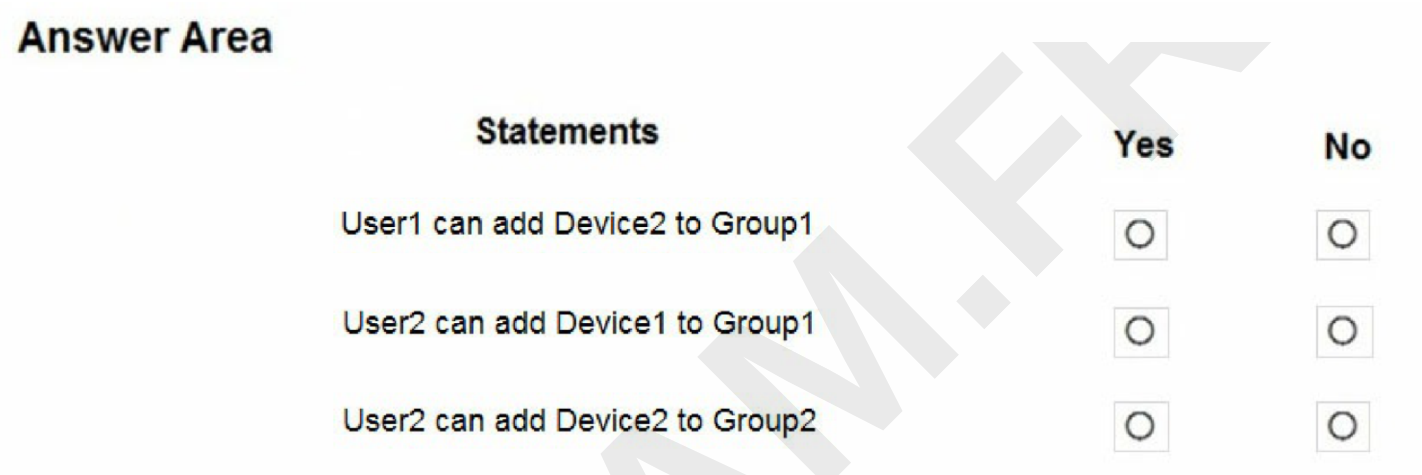
Name	Join type
Device1	Azure AD registered
Device2	Azure AD joined

You create following security groups in Contoso.com:



Name	Membership Type	Owner
Group1	Assigned	User2
Group2	Dynamic Device	User2

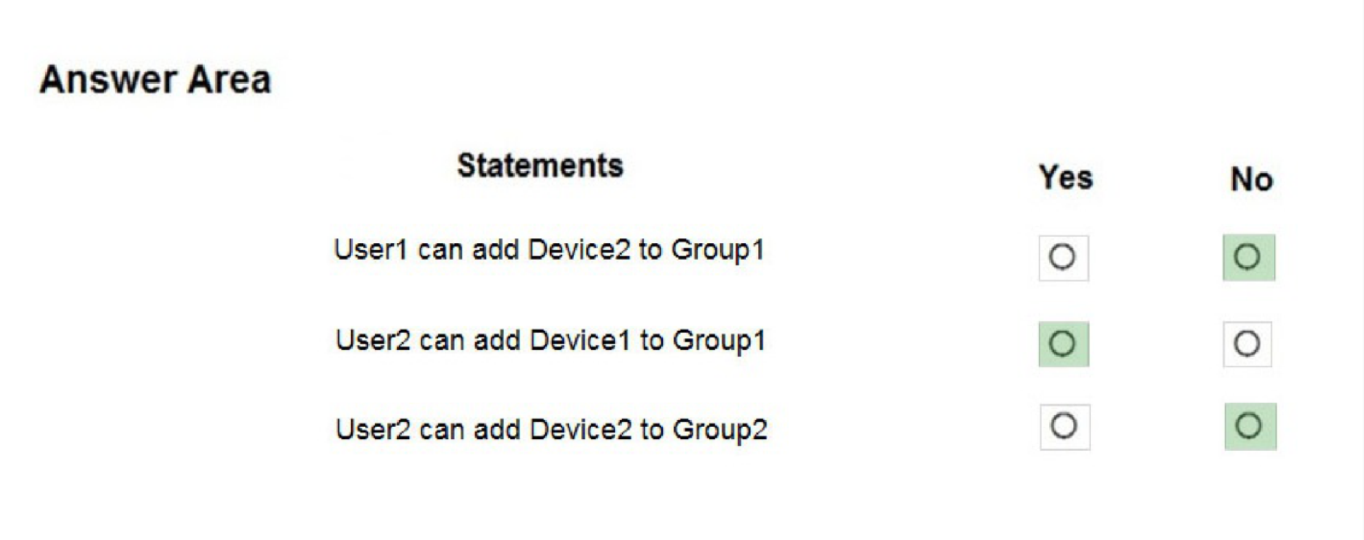
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

Statements	Yes	No
User1 can add Device2 to Group1	○	○
User2 can add Device1 to Group1	○	○
User2 can add Device2 to Group2	○	○

Answer:



Answer Area

Statements	Yes	No
User1 can add Device2 to Group1	○	[✓ ○]
User2 can add Device1 to Group1	[✓ ○]	○
User2 can add Device2 to Group2	○	[✓ ○]

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.

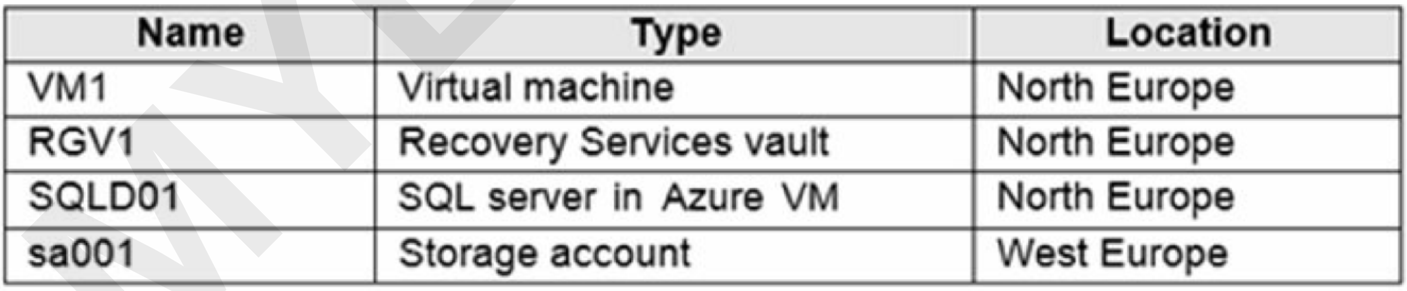
Reference:

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

Question: 56

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

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

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

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

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

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:

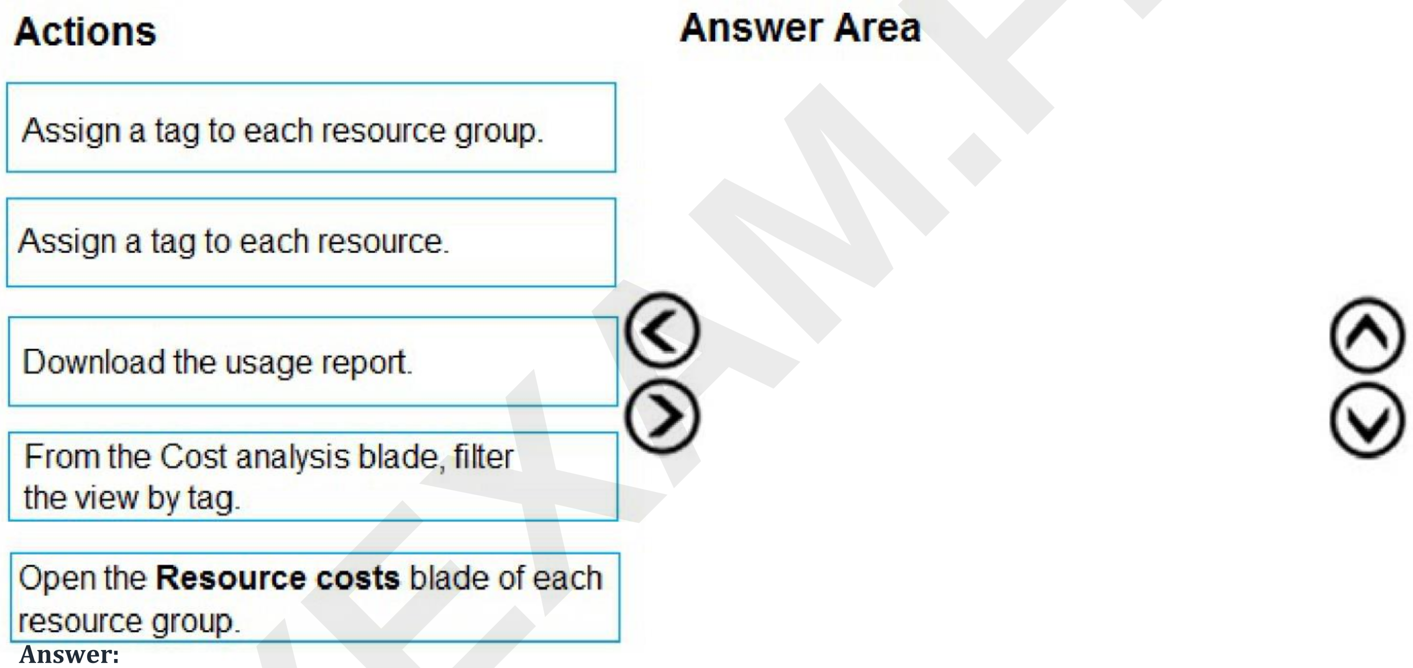
Yes, assigning the Contributor role to the Developers group on the Dev resource group would meet the goal of providing the group with the ability to create Azure logic apps in the Dev resource group.

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

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.

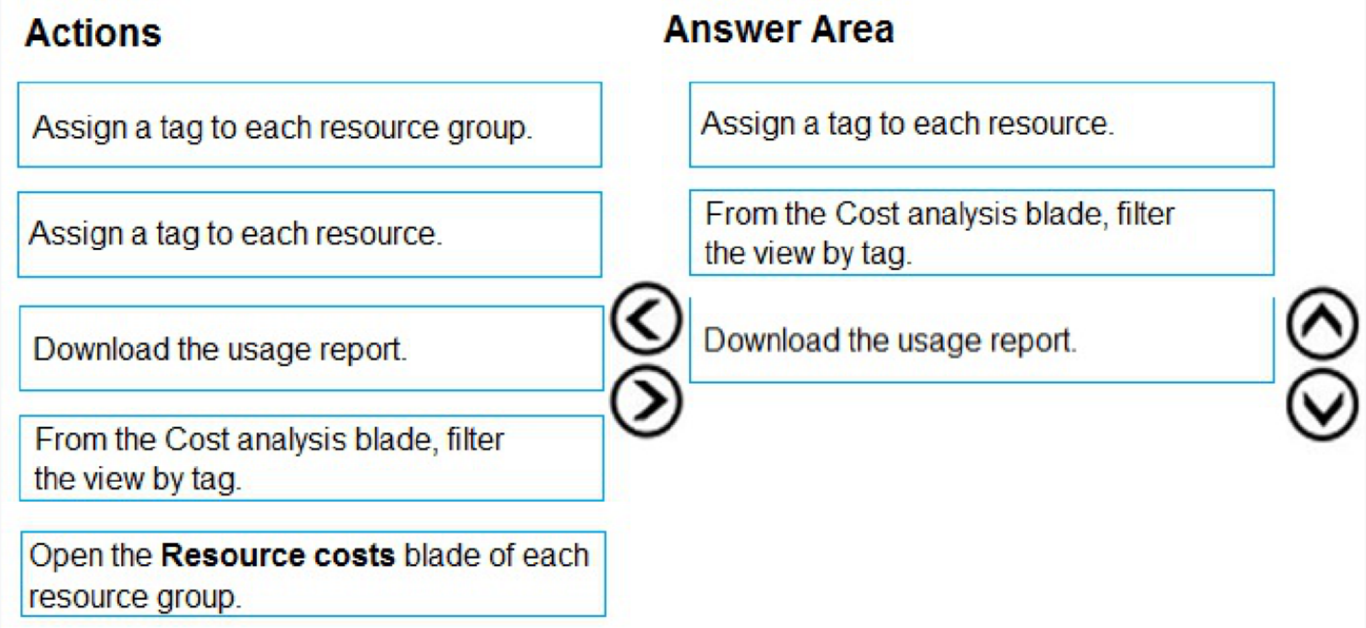
Download the usage report.

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

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

Answer Area

Answer:



Actions

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

Assign a tag to each resource.

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

Download the usage report.

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

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:

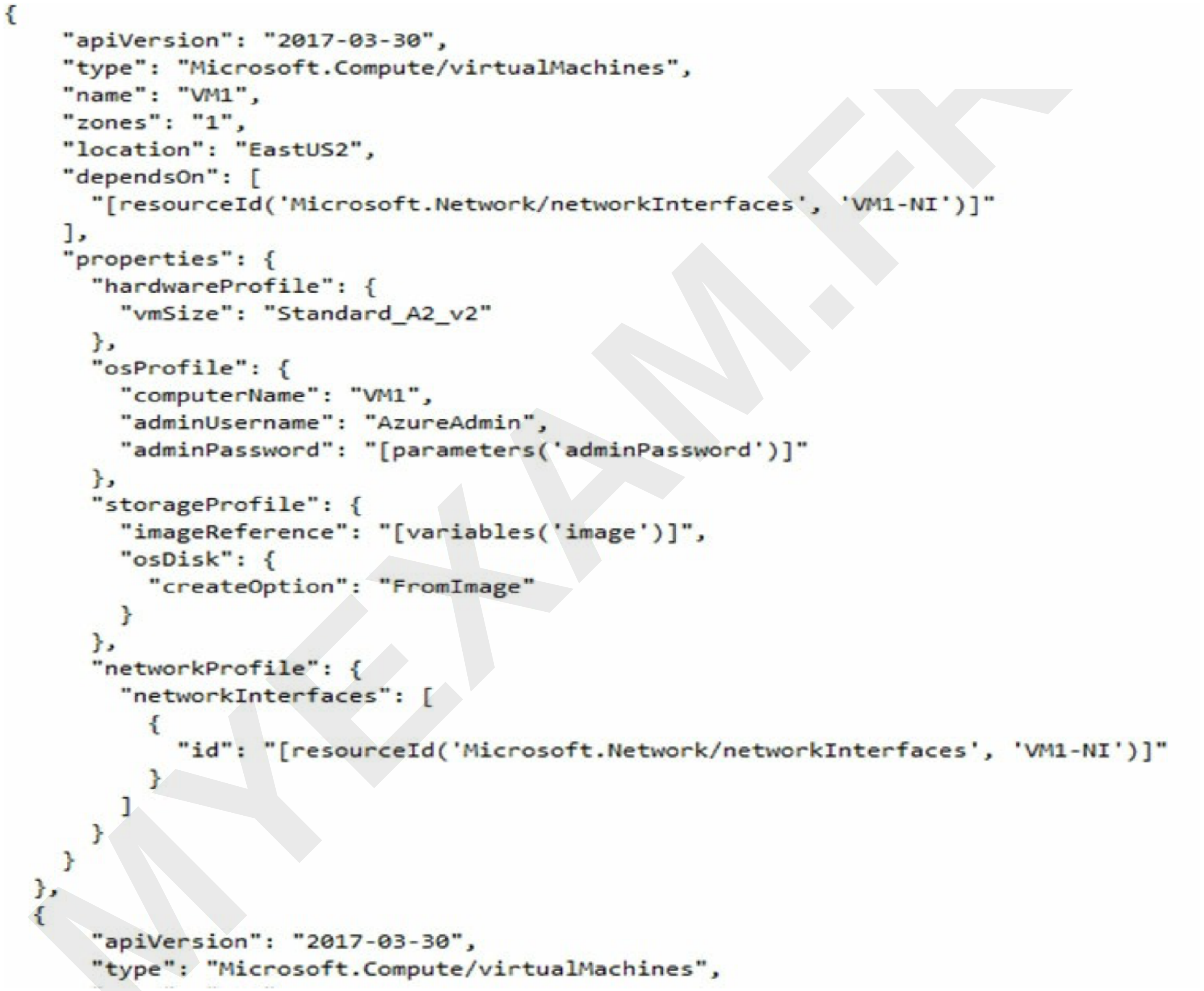
https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/search-queries https://docs.microsoft.com/e n-us/azure/azure-monitor/log-query/get-started-portal https://docs.microsoft.com/en-us/azure/data-explorer/kusto/query/searchoperator?pivots=azuredataexplorer

Question: 64

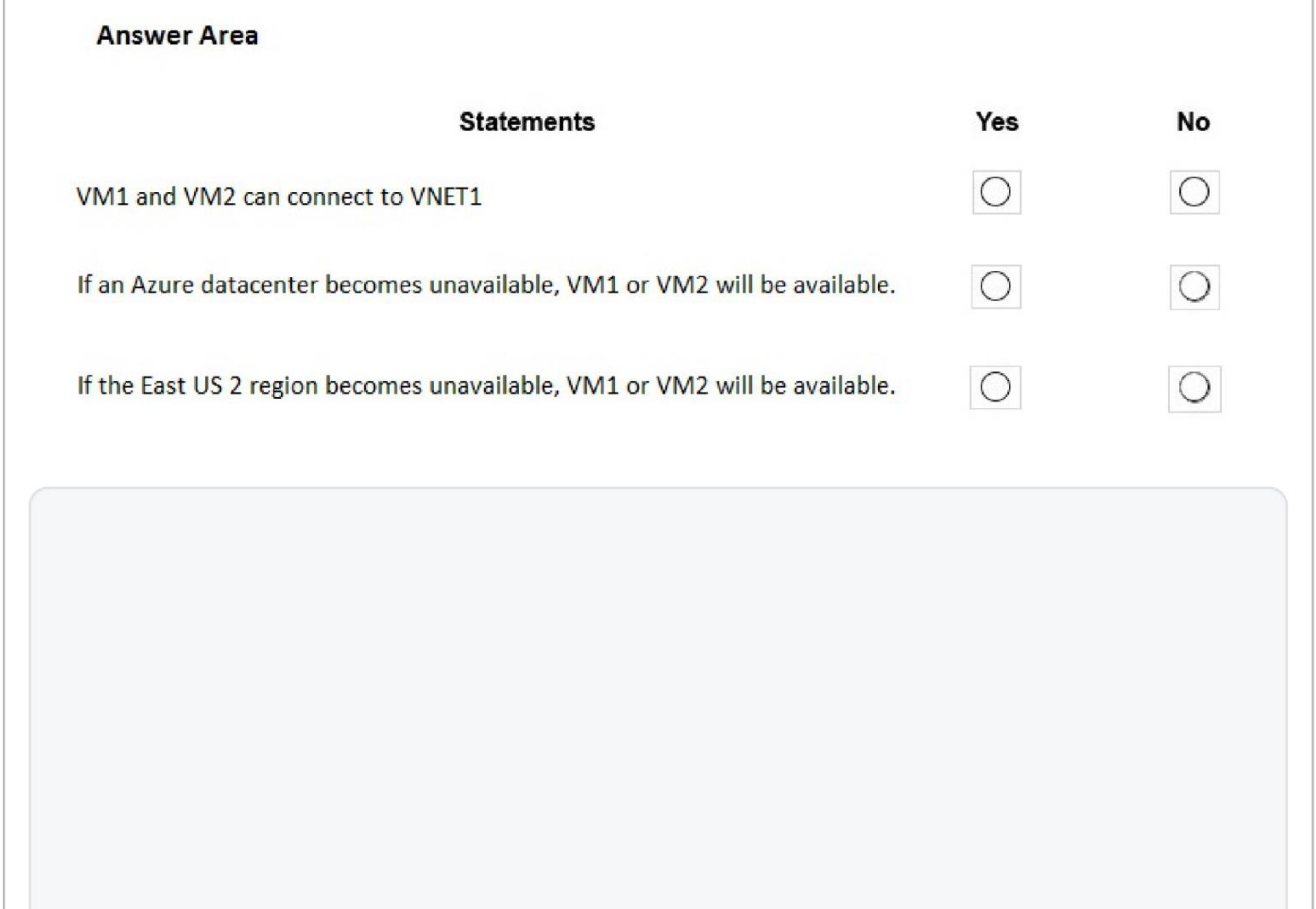
HOTSPOT -

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",
```



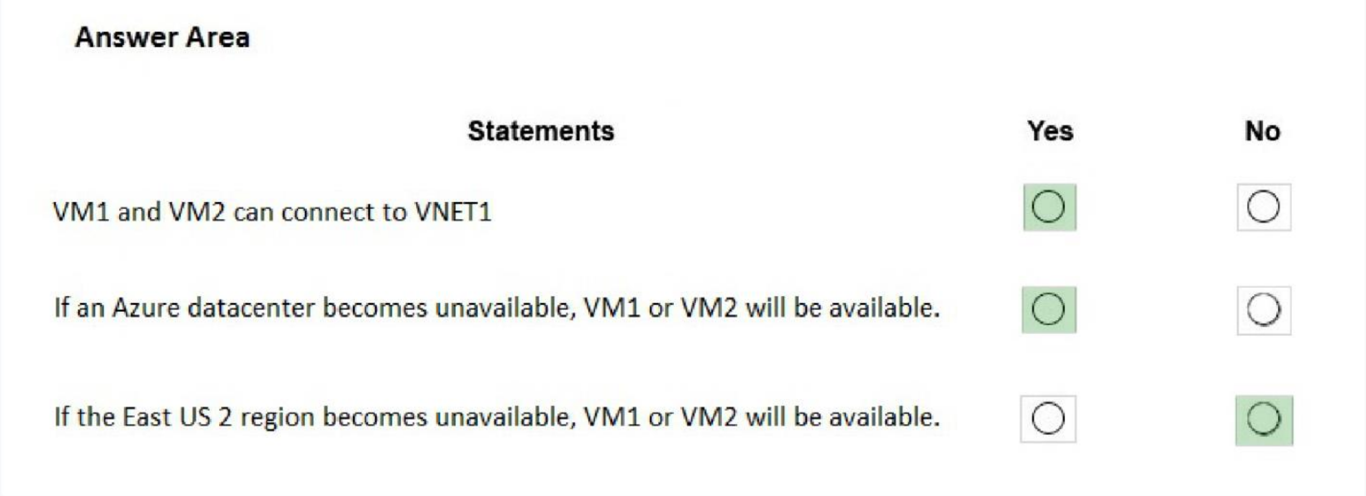
Answer Area

Statements	Yes	No
VM1 and VM2 can connect to VNET1	○	○
If an Azure datacenter becomes unavailable, VM1 or VM2 will be available.	○	○
If the East US 2 region becomes unavailable, VM1 or VM2 will be available.	○	○

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:



Answer Area

Statements	Yes	No
VM1 and VM2 can connect to VNET1	[✓ ○]	○
If an Azure datacenter becomes unavailable, VM1 or VM2 will be available.	[✓ ○]	○
If the East US 2 region becomes unavailable, VM1 or VM2 will be available.	○	[✓ ○]

Explanation:
Box 1: Yes -

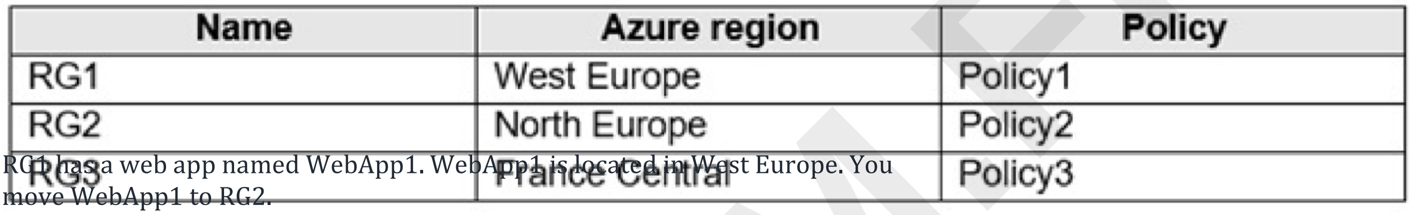
Box 2: Yes -
VM1 is in Zone1, while VM2 is on Zone2.

Box 3: No -

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

Question: 65

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

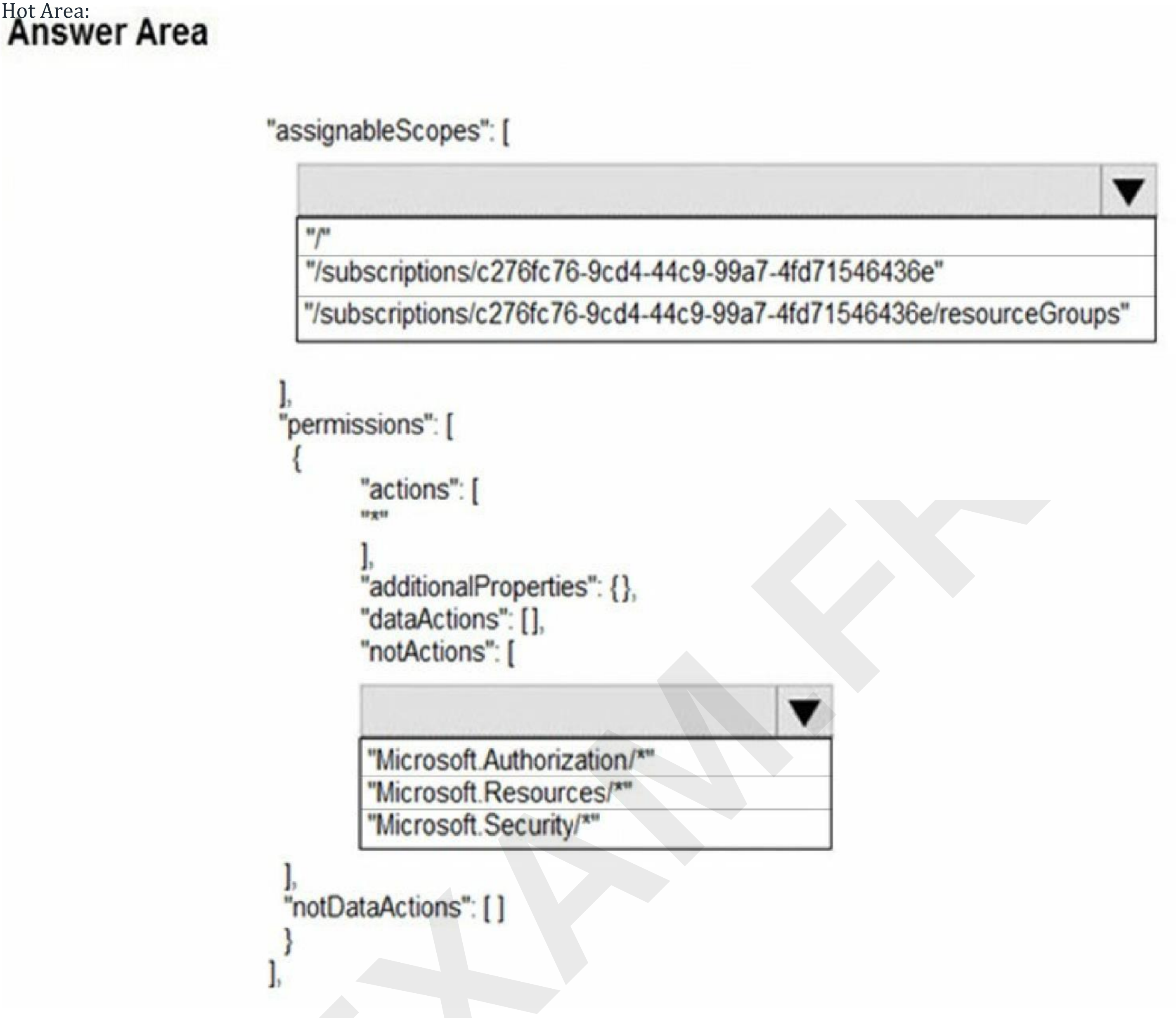
HOTSPOT -
You have an Azure subscription named Subscription1 that has a subscription ID of c276fc76-9cd4-44c9-99a7-4fd71546436e.
You need to create a custom RBAC role named CR1 that meets the following requirements:

➯ 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

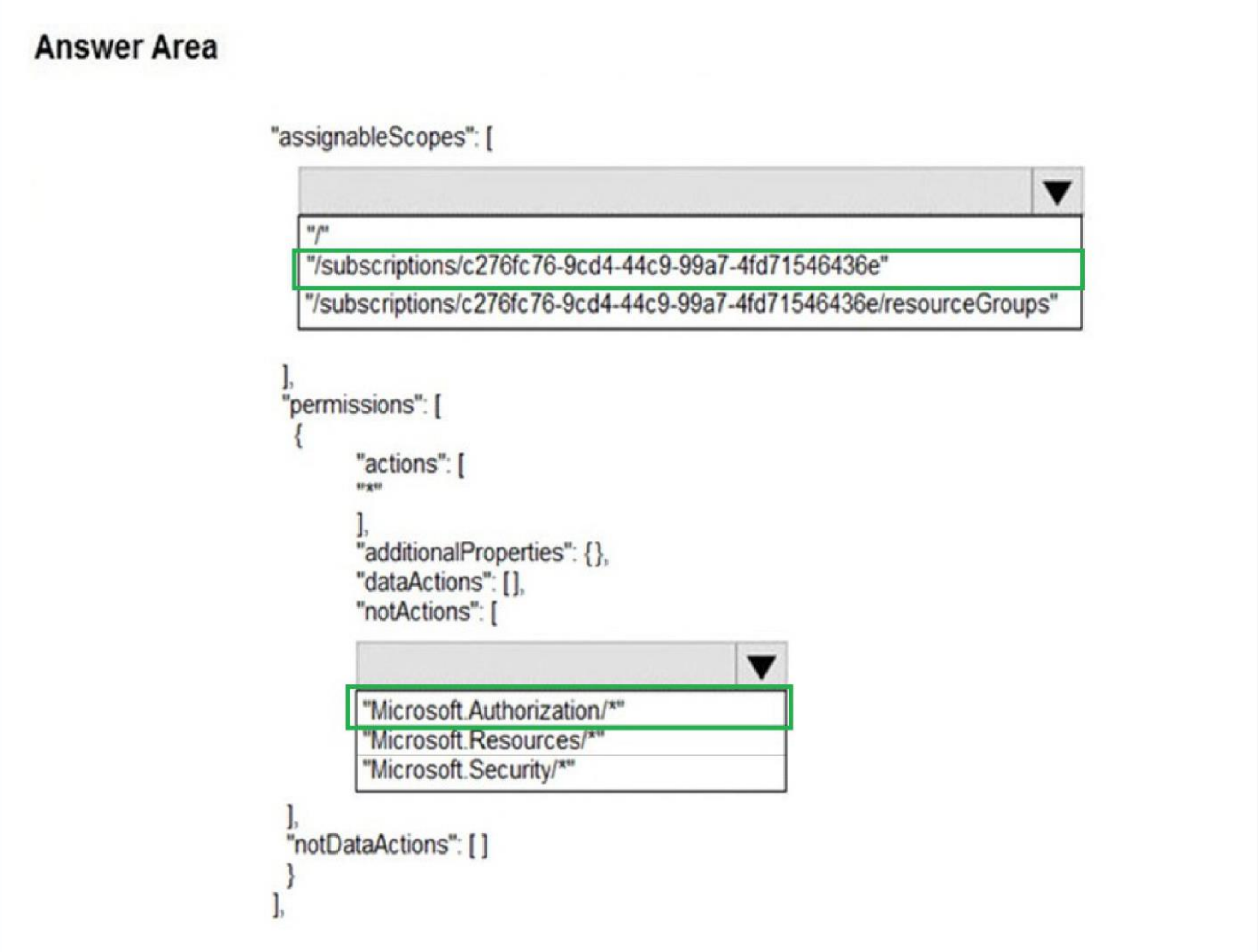
What should you specify in the assignable scopes and the permission elements of the definition of CR1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



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

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

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:

https://docs.microsoft.com/en-us/azure/advisor/advisor-cost-recommendations

Question: 69

HOTSPOT -

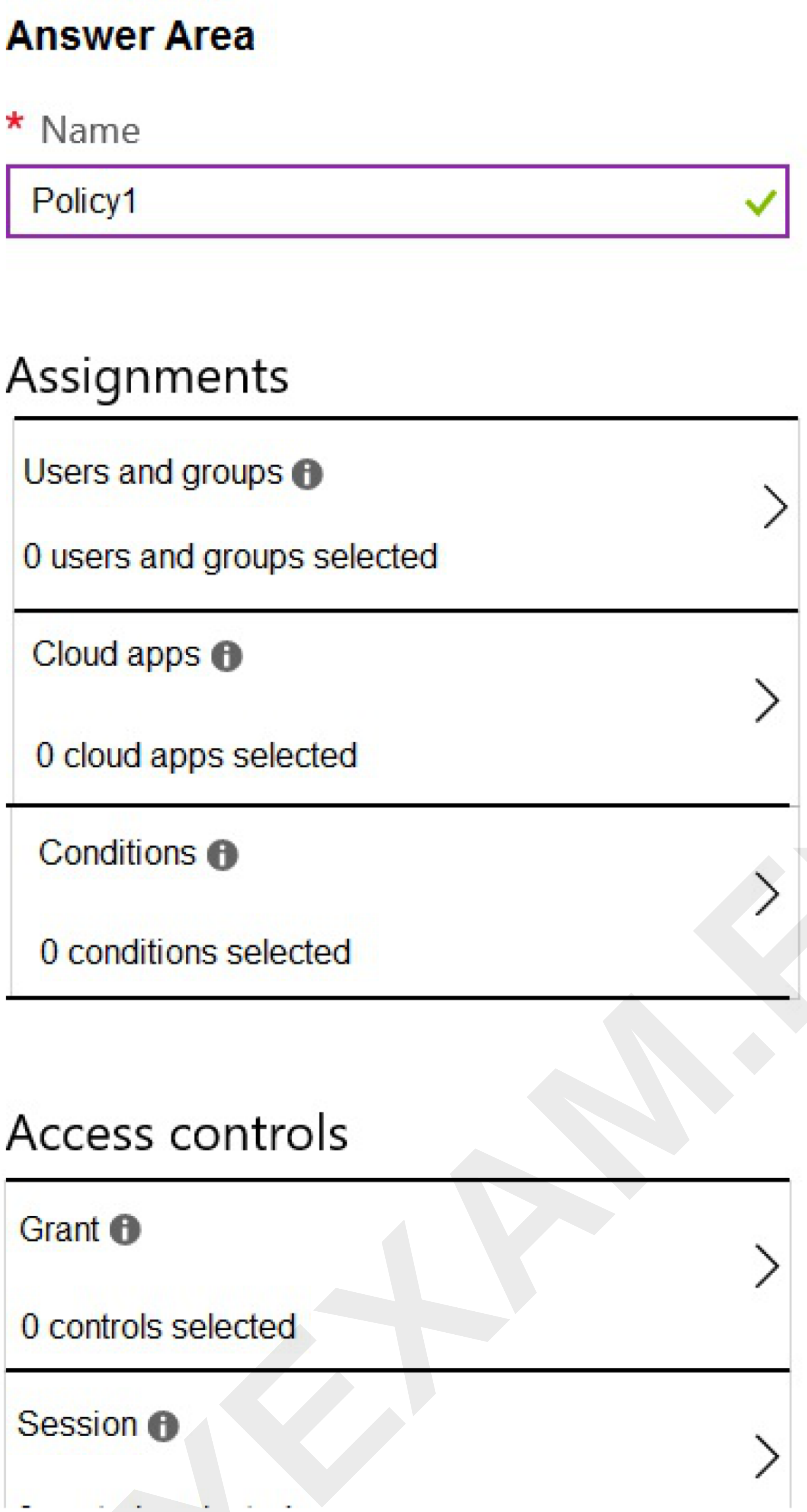
You have an Azure Active Directory (Azure AD) tenant.

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

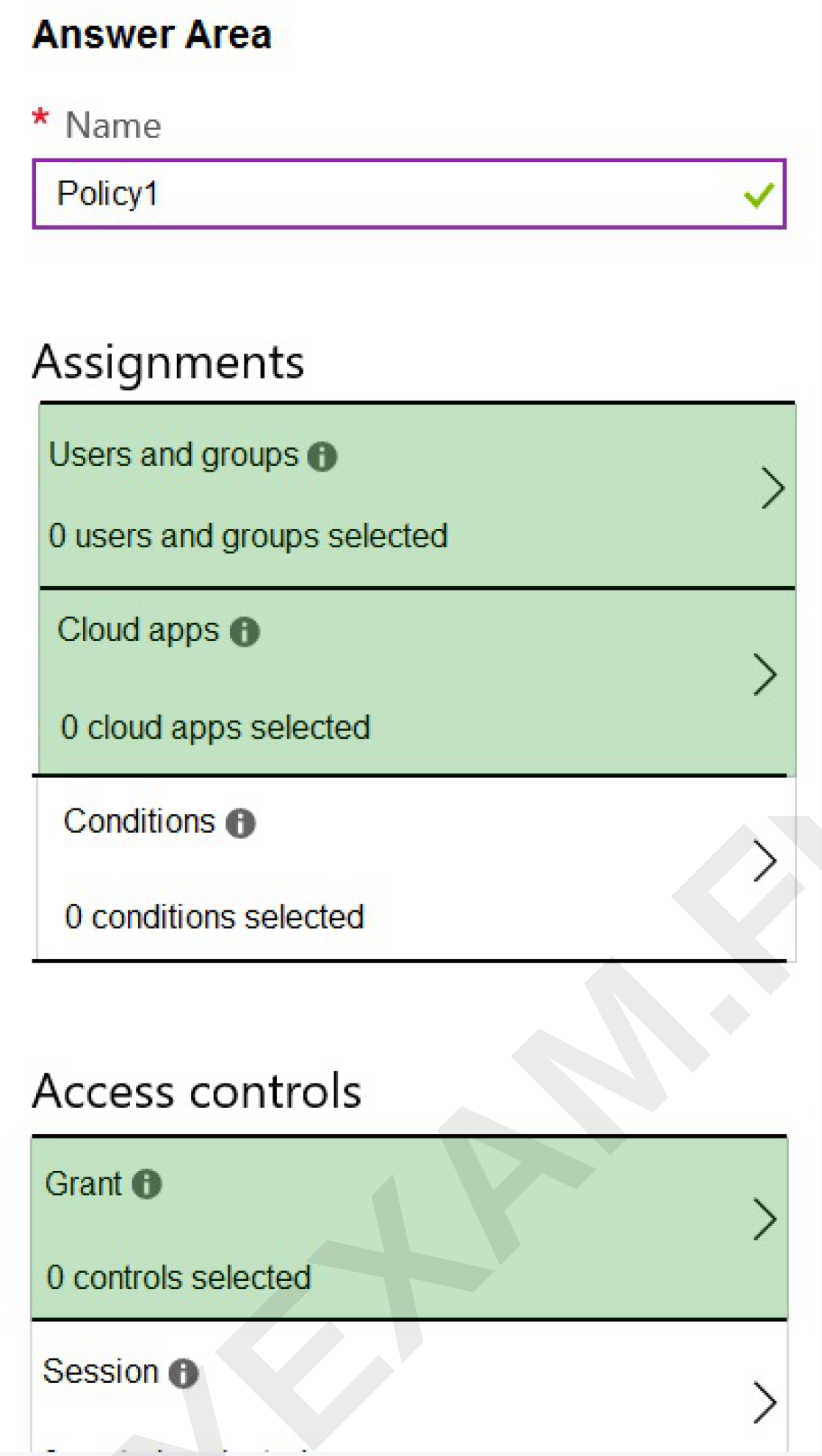
Access controls

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

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 [email protected] 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 [email protected] `" 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

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:

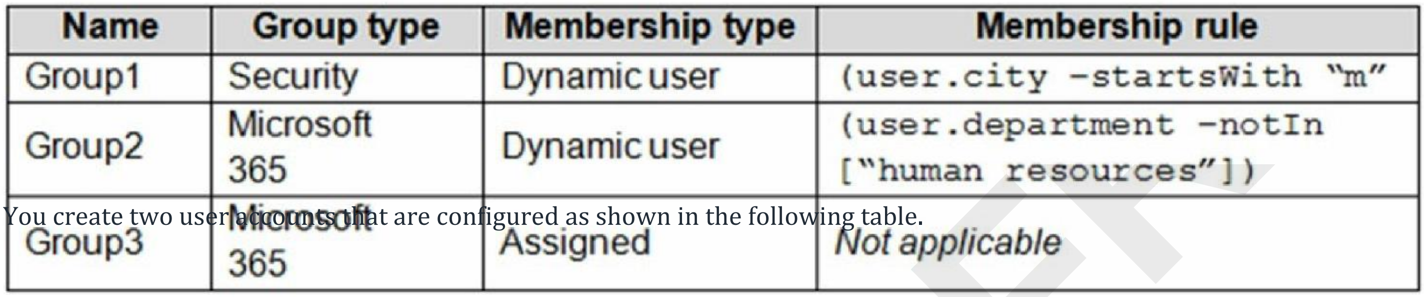
https://docs.microsoft.com/en-us/azure/governance/management-groups/overview#important-facts-about-the-root-management-group

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

Question: 72 HOTSPOT

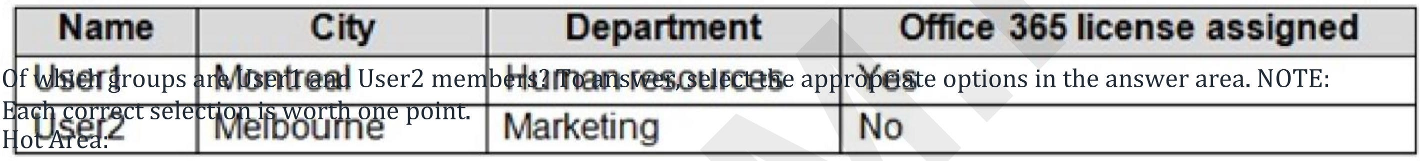
-

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	*Not applicable*

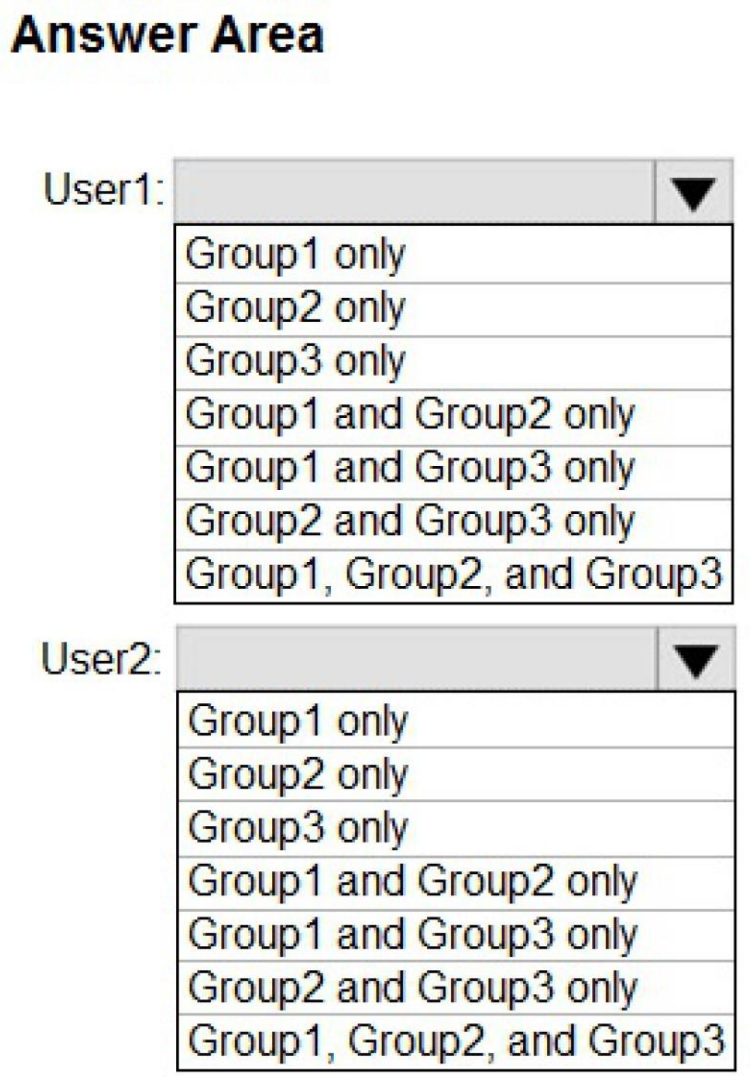
You create two user accounts that are configured as shown in the following table.



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

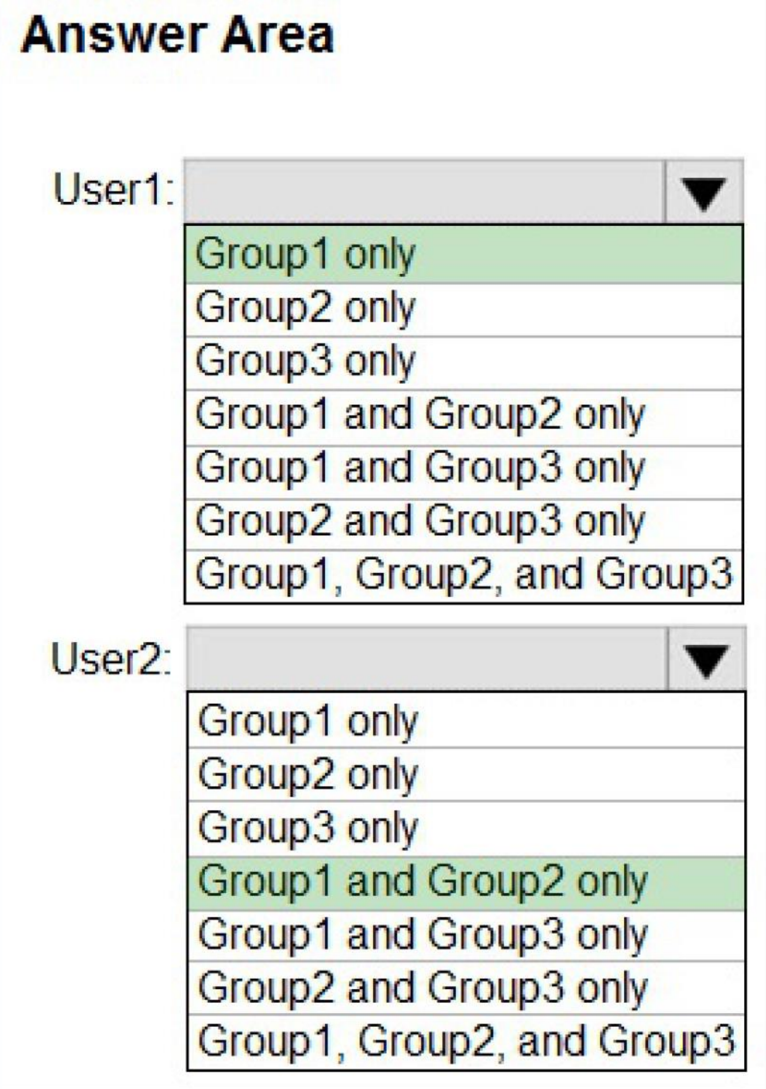
User1:

- 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:

- [✓ 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

Explanation:

Box 1: Group 1 only .

First rule applies -

Box 2: Group1 and Group2 only .

Both membership rules apply.

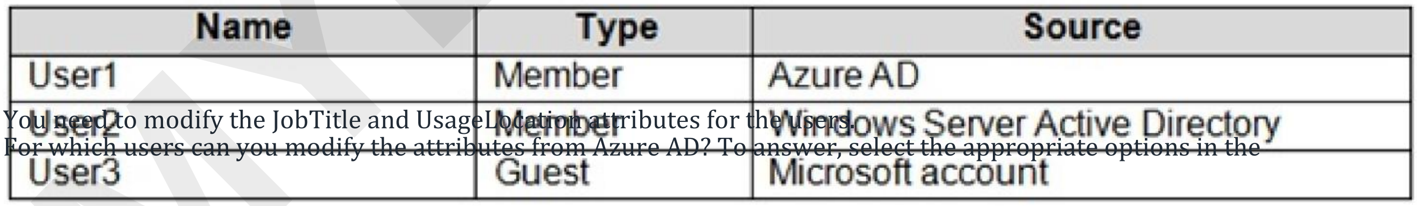
Reference:

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

Question: 73 HOTSPOT

-

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

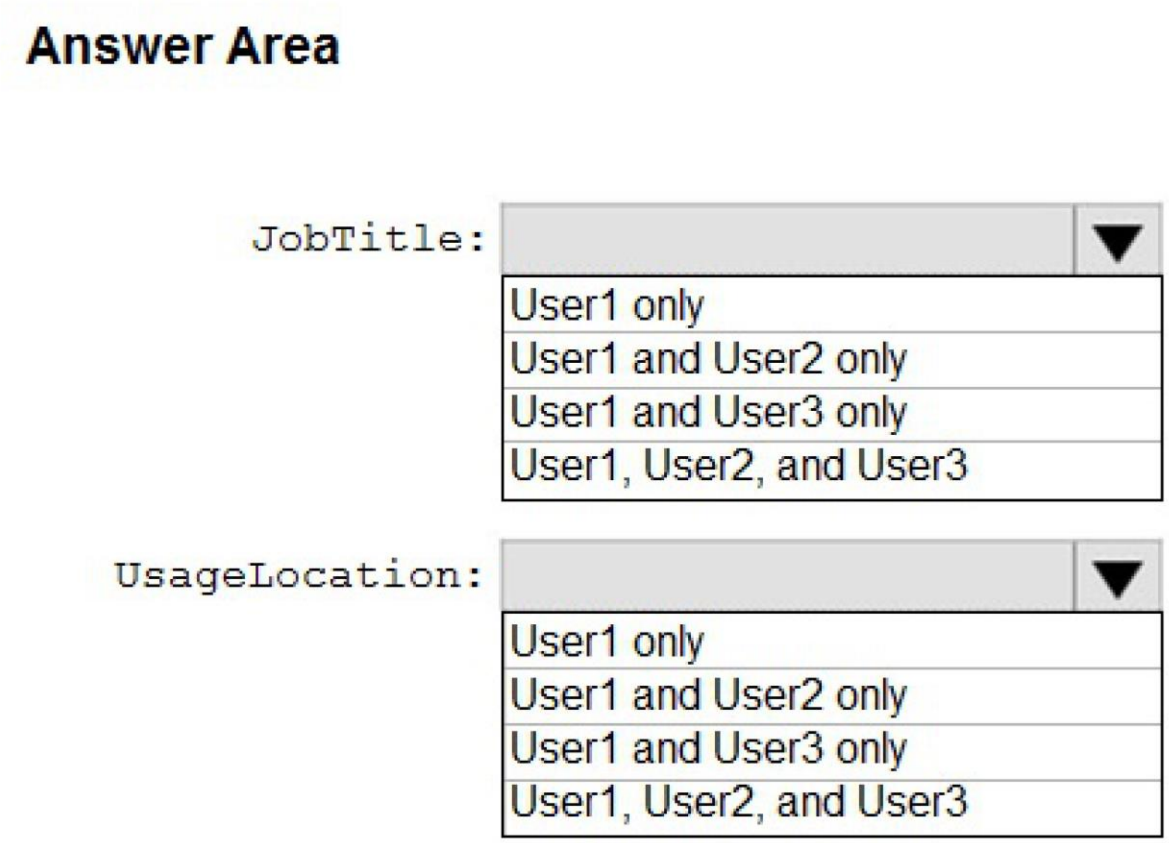


Name	Type	Source
User1	Member	Azure AD
User2	Member	Windows Server Active Directory
User3	Guest	Microsoft account

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

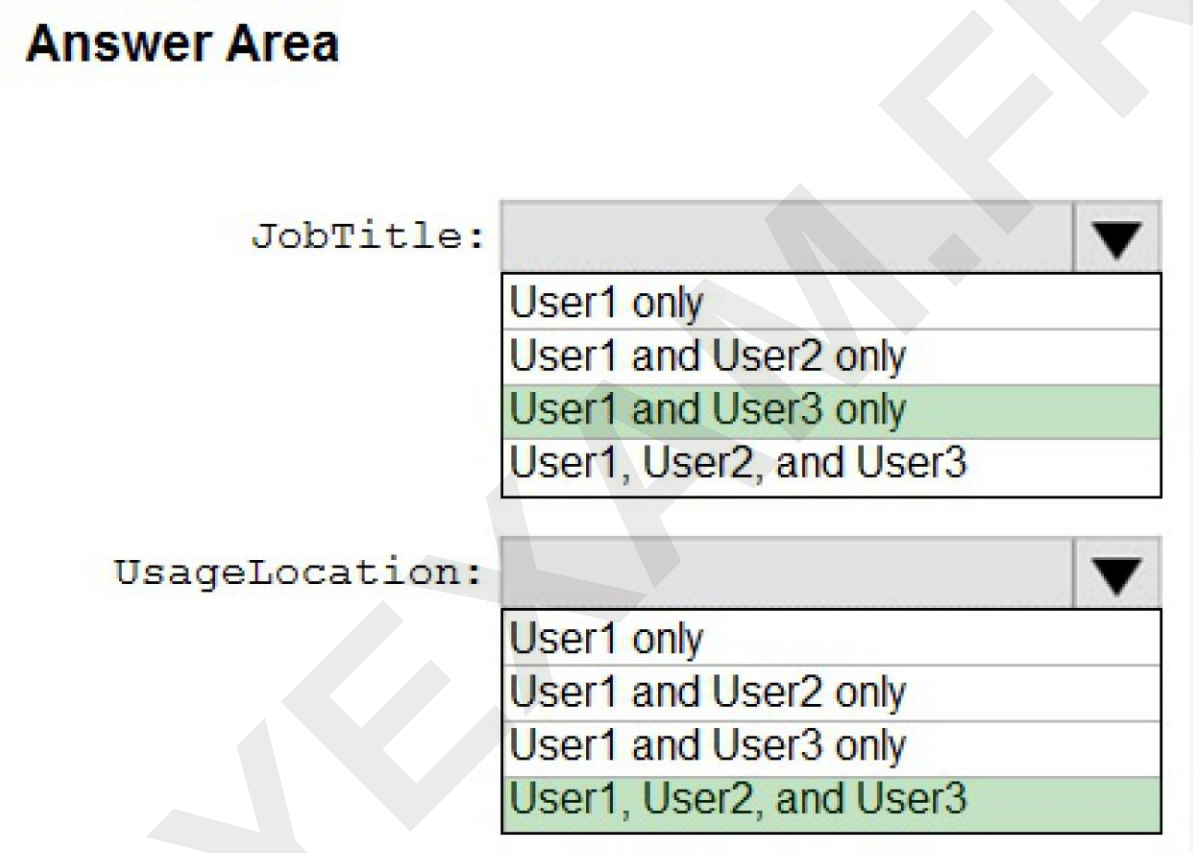
JobTitle: ▼

- 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

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

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

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.

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

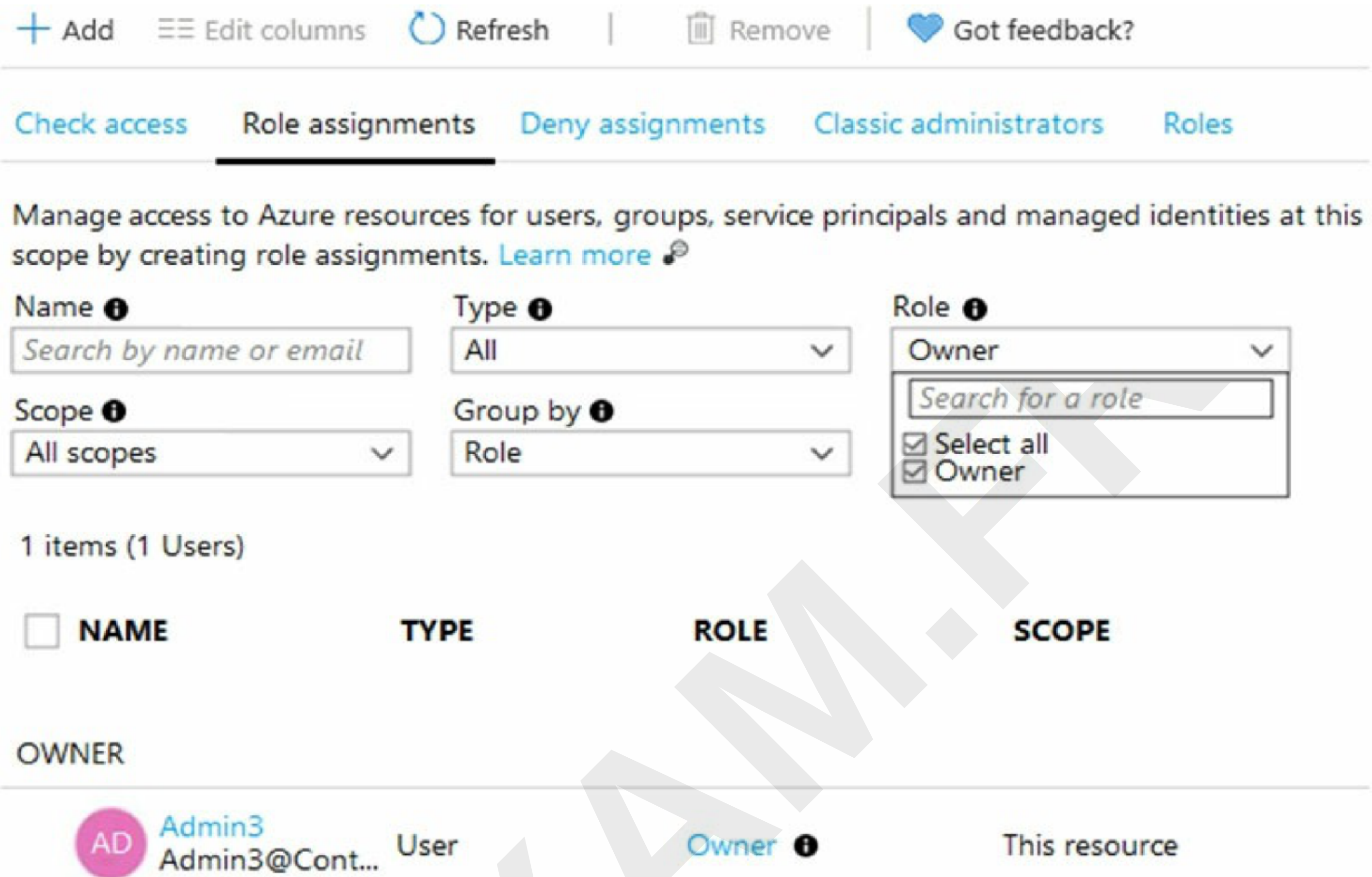
Explanation:
Contributor: Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC

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

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.)



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

Name: Search by name or email

Type: All

Role: Owner

Search for a role
☑ Select all
☑ Owner

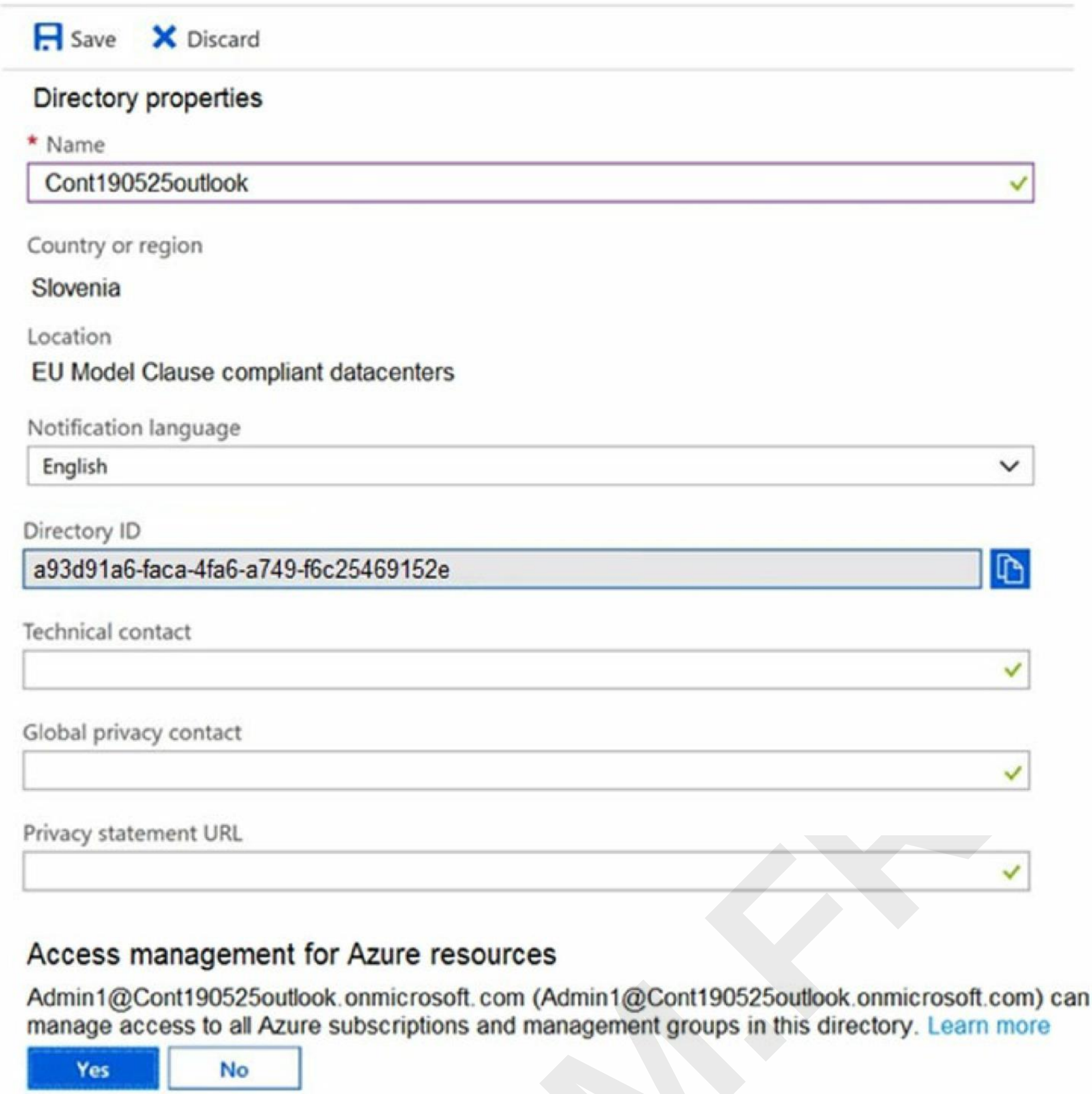
Scope: All scopes

Group by: Role

1 items (1 Users)

□ NAME	TYPE	ROLE	SCOPE
OWNER			
AD 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.)



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

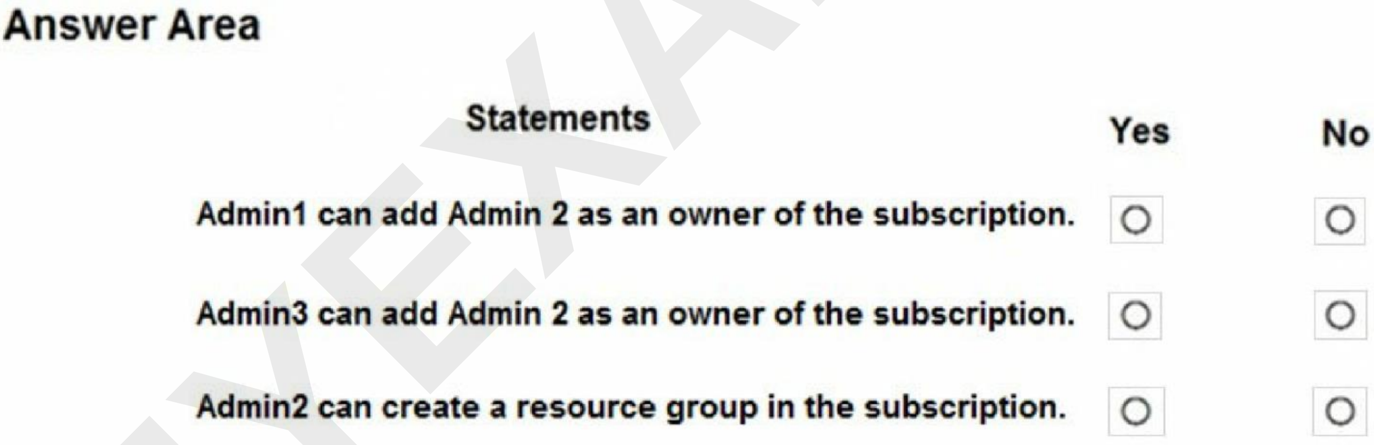
Global privacy contact

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

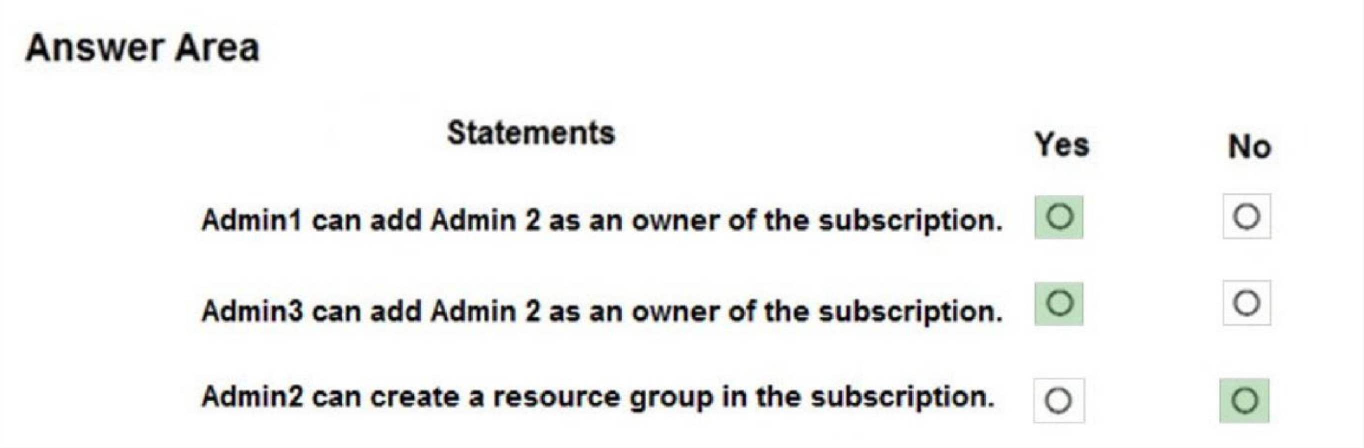
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

Statements	Yes	No
Admin1 can add Admin 2 as an owner of the subscription.	○	○
Admin3 can add Admin 2 as an owner of the subscription.	○	○
Admin2 can create a resource group in the subscription.	○	○

Answer:



Answer Area

Statements	Yes	No
Admin1 can add Admin 2 as an owner of the subscription.	[✓ ○]	○
Admin3 can add Admin 2 as an owner of the subscription.	[✓ ○]	○
Admin2 can create a resource group in the subscription.	○	[✓ ○]

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

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

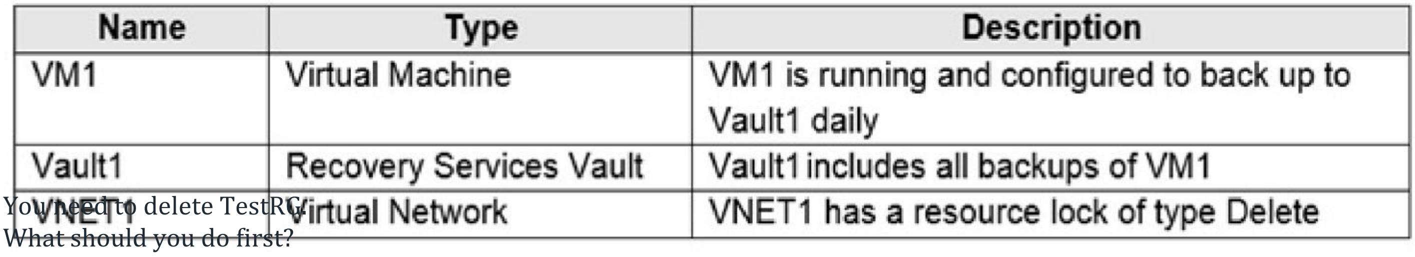
Answer: A

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-p ortal-windows-vm

Question: 80

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