

## Question #2

Topic 1

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 **Most Voted**

[Hide Solution](#)

[Discussion 62](#)

**Correct Answer:** B 

*Community vote distribution*

B (100%)

Explanation: Conditional Access policies are configured from the Azure AD Blade under Security settings page and not from the MFA settings page.

## Question #3

Topic 1

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 **Most Voted**

[Hide Solution](#)

[Discussion 24](#)

**Correct Answer:** B 

*Community vote distribution*

B (100%)

Explanation: Correct answer - B. To enforce MFA from an untrusted location, you need to create a conditional access rule that requires MFA with Grant control.

#### Question #4 Topic 1

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 **Most Voted**
- B. No

#### Question #5 Topic 1

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. **Most Voted**

<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/tutorial-automate-vm-deployment>

## Question #6

Topic 1

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 **Most Voted**

[Hide Solution](#)

[Discussion](#) 23

**Correct Answer:** B 🏆

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/>

*Community vote distribution*

B (100%)

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

## Question #7

Topic 1

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

[Hide Solution](#)

[Discussion](#) 13

**Correct Answer:** B 🏆

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/>

*Community vote distribution*

B (100%)

## Question #8

Topic 1

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 Most Voted

B. No Most Voted

For me this question is outdated and won't show up on exam but if it showed up it would be B (No), here is why: 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

Topic 1

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 Most Voted

In the solution of this question they say "-PolicyType Initial". However you must use "-PolicyType Delta" to get only the change made and sync it immediately. So the answer is "No".

Start-ADSyncSyncCycle -PolicyType Delta. Thus answer is B, NO.

## Question #10

Topic 1

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 **Most Voted**

[Hide Solution](#)

[Discussion 20](#)

**Correct Answer: B** 

*Community vote distribution*

B (100%)

## Question #12

Topic 1

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 **Most Voted**

C. Zone-redundant storage

D. Locally redundant storage

[Hide Solution](#)

[Discussion 46](#)

**Correct Answer: B** 

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. **Most Voted**
- D. You should remove the necessary VM from the availability set.

[Hide Solution](#)[Discussion 32](#)

Correct Answer: C 

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.

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

### Question #17

Topic 1

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. **Most Voted**
- D. Delete the VM that includes the data disk.

[Hide Solution](#)

[Discussion](#) 128

**Correct Answer:** A 

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/detach-disk> <https://docs.microsoft.com/en-us/azure/lab-services/devtest-lab-attach-detach-data-disk>

*Community vote distribution*

C (82%)

Other

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

the question is for the strategy to allow for the VM to be offline for the least amount of time possible. Stopping the VM = downtime whereby detaching the DATA disk only = no downtime. So answer C is the correct answer.

### Question #18

Topic 1

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 **Most Voted**

[Hide Solution](#)

[Discussion](#) 17

**Correct Answer:** D 

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

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

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 **Most Voted**

C. 30

D. 40

[Hide Solution](#)

[Discussion](#) 57

Correct Answer: B 

Correct answer is B. 20

'Each virtual machine in your **availability set** is assigned an update domain and a fault domain by the underlying Azure platform. Each availability set can be configured with up to three fault domains and twenty update domains.' <https://docs.microsoft.com/en-us/azure/virtual-machines/availability-set-overview>

## 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 Key Vault |
| An Azure Storage account                           | An access policy   |
| Azure Active Directory (AD)<br>Identity Protection |                    |
| An access policy                                   |                    |
| An Azure policy                                    |                    |
| A backup policy                                    |                    |

Correct Answer:

Key Vault + Access Policy. Using Key Vault we create a secret containing our Password:  
<https://docs.microsoft.com/en-us/azure/key-vault/secrets/quick-create-portal> .

Using an Access Policy we allow access to the previously created secret. Documentation Guide: <https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter?tabs=azure-cli>

Key vault and the access policy, actually the access policy is set during the vault creation

**Question #21****Topic 1**

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. **Most Voted**
- 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).

**Hide Solution****Discussion 22****Correct Answer:** A 

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.

<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****Topic 1**

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 **Most Voted**
- C. Add-AzImage
- D. Add-AzImageDataDisk

**Hide Solution****Discussion 30****Correct Answer:** B 

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

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

DRAG DROP -

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

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

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

Select and Place:

| <b>Options</b>                 | <b>Answer</b>                 |
|--------------------------------|-------------------------------|
| Hyper-V site                   | Hyper-V site                  |
| Storage account                | Azure Recovery Services Vault |
| Azure Recovery Services Vault  | Replication policy            |
| Azure Traffic Manager instance |                               |
| Replication policy             |                               |
| Endpoint                       |                               |

- Correct Answer: 1. Hyper-V site 2. Azure Recovery Services Vault 3. Replication policy

<https://docs.microsoft.com/nl-nl/azure/site-recovery/hyper-v-azure-tutorial>

## Question #26

Topic 1

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 **Most Voted**

B. No

[Hide Solution](#)

[Discussion 6](#)

Correct Answer: A 

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

## Question #28

Topic 1

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 **Most Voted**

[Hide Solution](#)

[Discussion 35](#)

Correct Answer: B 

Community vote distribution

B (100%)

## Question #29

Topic 1

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

[Hide Solution](#)

[Discussion 9](#)

**Correct Answer:**  B

Reference:

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

*Community vote distribution*

B (100%)

## Question #30

Topic 1

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  Most Voted

B. No

[Hide Solution](#)

[Discussion 25](#)

**Correct Answer:**  A

*Community vote distribution*

A (90%)

10%

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

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. **Most Voted**

[Hide Solution](#)

[Discussion 49](#)

Correct Answer: E 

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 #33

Topic 1

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 Most Voted

[Hide Solution](#)

[Discussion 32](#)

**Correct Answer:** D 

*Community vote distribution*

D (100%)

### Question #34

Topic 1

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. Most Voted

C. You can only recover the files to a new VM.

D. You will not be able to recover the files.

[Hide Solution](#)

[Discussion 138](#)

**Correct Answer:** A 

*Community vote distribution*

B (89%)

11%

<https://azure.microsoft.com/en-in/blog/instantly-restore-your-azure-virtual-machines-using-azure-backup/>

### Question #35

Topic 1

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?

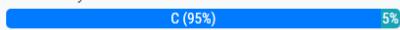
- A. You should restore the VM after deleting the infected VM.
- B. You should restore the VM to any VM within the company's subscription.
- C. You should restore the VM to a new Azure VM. **Most Voted**
- D. You should restore the VM to an on-premise Windows device.

[Hide Solution](#)

[Discussion 67](#)

**Correct Answer:** B 🎉

*Community vote distribution*



### Question #36

Topic 1

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 **Most Voted**
- C. Azure Activity Log
- D. Azure Advisor

[Hide Solution](#)

[Discussion 16](#)

**Correct Answer:** B 🎉

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

Topic 1

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. **Most Voted**

B. VMs that run Windows Server 2012 or higher. **Most Voted**

C. VMs that have NOT been shut down. **Most Voted**

D. VMs that run Debian 8.2+. **Most Voted**

E. VMs that have been shut down. **Most Voted**

[Hide Solution](#)

[Discussion 35](#)

**Correct Answer:** ABCDE 🎉

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.

### Question #38

Topic 1

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 **Most Voted**

[Hide Solution](#)

[Discussion 7](#)

**Correct Answer:** B 🎉

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.

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

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 **Most Voted**

[Hide Solution](#)

[Discussion 21](#)

**Correct Answer:** *B* 🎉

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>

*Community vote distribution*

**B (84%)**

**A (16%)**

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 **Most Voted**

B. No

**Hide Solution**

 Discussion 14

**Correct Answer:** A 🎉

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>

*Community vote distribution*

A (82%)

B (18%)

## Topic 2 ---- Question Set 2

Question #1

Topic 2

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               |

Correct Answer:

To add a health probe to LB2:

|                            |
|----------------------------|
| Contributor on LB2         |
| Network Contributor on LB2 |
| Network Contributor on RG1 |
| Owner on LB2               |

The Network Contributor role lets you manage networks, but not access them.

The Network Contributor role lets you manage networks, but not access them.

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

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

[Hide Solution](#)

[Discussion](#) 29

Correct Answer: AC 

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>

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

Description 1

\* Start date  Calendar icon

Frequency  Down arrow

Duration (in days) 0  Up/Down arrows

End 1  Never  End by Occurrences

\* Number of times

\* End date  Calendar icon

### Users

Users to review  Down arrow

Scope  Guest users only  
 Everyone

\* Group

Group1 >

### Reviewers

Reviewers  Down arrow

### Programs

Link to program

Default program >

- ✓ Upon completion settings
- ✓ Advanced settings

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

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

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

Review1 reviews access for guest users who are member of Group1. The group owner is specified as the reviewer. User3 is the owner of Group1. User2 is the only guest user in Group1.

Note: Dynamic groups and nested groups are not supported with the Access review process.

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

HOTSPOT -

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

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

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

| Name          | Management group  |
|---------------|-------------------|
| Subscription1 | ManagementGroup21 |
| Subscription2 | ManagementGroup12 |

You create the Azure policies shown in the following table:

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

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

NOTE: Each correct selection is worth one point.

### Answer Area

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

Box 1: No -

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

Box 2: Yes -

Virtual Machines can be created on a Management Group provided the user has the required RBAC permissions.

Box 3: Yes -

Subscriptions can be moved between Management Groups provided the user has the required RBAC permissions.

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 #8****Topic 2**

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 **Most Voted**
- D. RVAULT1 only

[Hide Solution](#)[Discussion 64](#)

Correct Answer: C 🎉

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 #9****Topic 2**

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 **Most Voted**
- D. From the Azure portal, assign the Billing administrator role to Admin1

[Hide Solution](#)[Discussion 54](#)

Correct Answer: C 🎉

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

## Question #16

Topic 2

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. Most Voted

C. Assign User1 the Network Contributor role for VNet1.

D. Assign User1 the Network Contributor role for RG1.

[Hide Solution](#)

[Discussion](#) 35

**Correct Answer:** B 

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

## Question #18

Topic 2

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 Most Voted

[Hide Solution](#)

[Discussion](#) 40

**Correct Answer:** B 

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.

**Question #22****Topic 2**

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" **Most Voted**

C. select \* from Event where EventType == "error"

D. search in (Event) \* | where EventType -eq "error"

**Hide Solution****Discussion 23****Correct Answer:** B 🎉

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

**Question #29****Topic 2**

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 user1@outlook.com 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 user1@outlook.com ''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. **Most Voted**

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.

**Hide Solution****Discussion 46****Correct Answer:** A 🎉

## 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:

\* Name

Policy1



## Assignments

Users and groups i



0 users and groups selected

Cloud apps i



0 cloud apps selected

Conditions i



0 conditions selected

Correct Answer:

## Access controls

Grant i



0 controls selected

Session i



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. **Most Voted**
- D. Create a new management group and delegate User1 as the owner of the new management group.

[Hide Solution](#)[Discussion 98](#)

Correct Answer: **B** 🎉

Correct Answer: C

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>

**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 Area**

Correct Answer:

JobTitle:

|                             |
|-----------------------------|
| User1 only                  |
| User1 and User2 only        |
| <b>User1 and User3 only</b> |
| User1, User2, and User3     |

UsageLocation:

|                                |
|--------------------------------|
| User1 only                     |
| User1 and User2 only           |
| User1 and User3 only           |
| <b>User1, User2, and User3</b> |

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 -

**Question #33****Topic 2**

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 **Most Voted**

B. No

**Hide Solution****Discussion 41****Correct Answer: A** 🎉**Question #34****Topic 2**

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

**Hide Solution****Discussion 23****Correct Answer: A** 🎉

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>

*Community vote distribution*

A (100%)

**Question #35****Topic 2**

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 **Most Voted**

B. No **Most Voted**

**Hide Solution**

**Discussion 119**

**Correct Answer: A** 🎉

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>

*Community vote distribution*

A (58%) B (42%)

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.

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

**Question #36****Topic 2**

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 **Most Voted**

D. Virtual Machine Administrator Login

**Hide Solution**

**Discussion 194**

**Correct Answer: C** 🎉

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 admin

## HOTSPOT -

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

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

**Add** **Edit columns** **Refresh** | **Remove** | **Got feedback?**

**Check access** **Role assignments** **Deny assignments** **Classic administrators** **Roles**

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

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

1 items (1 Users)

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

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

 Save  Discard

### Directory properties

\* Name

Cont190525outlook 

Country or region

Slovenia

Location

EU Model Clause compliant datacenters

Notification language

English 

Directory ID

a93d91a6-faca-4fa6-a749-f6c25469152e 

Technical contact



Global privacy contact



Privacy statement URL



### Access management for Azure resources

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

 Yes

 No

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

NOTE: Each correct selection is worth one point.

## Answer Area

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

Correct Answer: 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>

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 **Most Voted**
- B. From the Azure portal, modify the Access control (IAM) settings of RG1 **Most Voted**
- C. From the Azure portal, modify the Access control (IAM) settings of VM1
- D. From the Azure portal, modify the Policies settings of RG1

[Hide Solution](#)[Discussion 65](#)

**Correct Answer:** A 🎉

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

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

Reference:

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

*Community vote distribution*



Correct Answer: A

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. RBAC manages who has access to Azure resources, what areas they have access to and what they can do with those resources. Examples of Role Based Access Control (RBAC) include: Allowing an app to access all resources in a resource group Policies on the other hand focus on resource properties during deployment and for already existing resources. As an example, a policy can be issued to ensure users can only deploy DS series VMs within a specified resource

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

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 Most Voted
- C. Turn off VM1 and remove the resource lock from VNET1
- D. Turn off VM1 and delete all data in Vault1

**Correct Answer: B**

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.

You have an Azure DNS zone named adatum.com.

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

What should you do?

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

[Hide Solution](#)

[Discussion 51](#)

**Correct Answer: A** 

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

Reference:

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

*Community vote distribution*

A (100%)

**Question #41****Topic 2**

DRAG DROP -

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

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

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

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

Select and Place:

**Actions**

|                            |
|----------------------------|
|                            |
| Add an Azure AD tenant     |
| Configure company branding |
| Create an Azure DNS zone   |
|                            |
|                            |

**Answer Area**

|   |
|---|
| Add a custom name                               |
| Add a record to the public contoso.com DNS zone |
| Verify the domain                               |

**Question #43****Topic 2**

You have a registered DNS domain named contoso.com.

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

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

What should you do?

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

**Hide Solution****Discussion 11****Correct Answer: D**

Reference:

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

Community vote distribution

D (100%)

## HOTSPOT -

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

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

| Name      | Type     |
|-----------|----------|
| User1     | User     |
| Computer1 | Computer |

In Azure AD, you create a user named User2.

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

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

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

NOTE: Each correct selection is worth one point.

## Answer Area

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

Correct answer

Box1: Yes

Because you can assign Share-level permissions to specific Azure AD users or user groups

Box2: No

Azure AD and on-premises AD DS authentication do not support authentication against computer accounts.

Box3: No

Because User 2 is created on Azure (not in Windows Active directory) and therefore is not hybrid. To be hybrid it must be created on-prem in Windows Active Directory and then be synchronized.

**HOTSPOT -**

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

You add the users in the following table.

| User  | Role                |
|-------|---------------------|
| User1 | Owner               |
| User2 | Security Admin      |
| User3 | Network Contributor |

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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Add a subnet to VNet1:

|                             |
|-----------------------------|
| User1 only                  |
| User3 only                  |
| <b>User1 and User3 only</b> |
| User2 and User3 only        |
| User1, User2, and User3     |

Assign a user the Reader role to VNet1:

|                                |
|--------------------------------|
| <b>User1 only</b>              |
| User2 only                     |
| User3 only                     |
| User1 and User2 only           |
| User2 and User3 only           |
| <b>User1, User2, and User3</b> |

HOTSPOT -

You have the Azure resources shown on the following exhibit.



Tenant Root Group



MG1



Sub1



RG1



VM1

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Locks:

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

Tags:

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

Both Tags and Locks are available to Subscriptions, Resource Groups, and Resources.

You have an Azure Active Directory (Azure AD) tenant.  
You plan to delete multiple users by using Bulk delete in the Azure Active Directory admin center.  
You need to create and upload a file for the bulk delete.  
Which user attributes should you include in the file?

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

[Hide Solution](#)[Discussion 10](#)**Correct Answer:** B 🏆

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/users-bulk-delete>*Community vote distribution* B (100%)

HOTSPOT -

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

| Name     | Type            |
|----------|-----------------|
| RG1      | Resource group  |
| storage1 | Storage account |
| VNET1    | Virtual network |

You assign an Azure policy that has the following settings:

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

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

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

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

## Answer Area

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

Expl:

RG1 is NOT excluded. Only VNET1 is excluded

- 1) YES Policy scope's assignment is about tags on resources NOT RESOURCE GROUPS.
- 2) NO Storage1 is a recourse, it is affected by the policy and will have 2 tags. The manual input and the one from the policy Tag3:value1, Tag4:value4
- 3) NO VNET1 is a resource BUT it is excluded from the policy so it keeps only the manually assigned tag Tag3:value2

**Question #49****Topic 2**

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

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

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

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

Does this meet the goal?

A. Yes

B. No **Most Voted**

[Hide Solution](#)[Discussion 28](#)

**Correct Answer:** B 🎉

B) "No" One of the following Azure built-in roles needs to be assigned to your account:

- Owner
- Contributor
- Reader
- Network Contributor

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

**Question #50****Topic 2**

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

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

What should you use?

A. Azure AD roles

B. administrative units **Most Voted**

C. access packages in Azure AD entitlement management

D. Azure roles

[Hide Solution](#)[Discussion 13](#)

**Correct Answer:** B 🎉

Reference:

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

*Community vote distribution*

B (100%)

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

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

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

Subscription1 contains a resource group named Dev.

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

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

Does this meet the goal?

A. Yes **Most Voted**

B. No

[Hide Solution](#)

[Discussion \*\*46\*\*](#)

**Correct Answer:** A 🎉

Reference:

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

*Community vote distribution*

A (61%)

B (35%)

HOTSPOT -

You configure the custom role shown in the following exhibit.

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

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

|                  |   |
|------------------|---|
|                  | ▼ |
| actions          |   |
| roletype         |   |
| notActions       |   |
| dataActions      |   |
| notDataActions   |   |
| assignableScopes |   |

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

|                  |   |
|------------------|---|
|                  | ▼ |
| actions          |   |
| roletype         |   |
| notActions       |   |
| dataActions      |   |
| notDataActions   |   |
| assignableScopes |   |

You need to provide either of the following in DataActions:

Microsoft.Compute/virtualMachines/login/action

Microsoft.Compute/virtualMachines/loginAsAdmin/action

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles?source=recommendations#virtual-machine-administrator-login>

Correct answer is dataActions and assignableScopes

You have an Azure subscription that contains a storage account named storage1. The storage1 account contains a file share named share1. The subscription is linked to a hybrid Azure Active Directory (Azure AD) tenant that contains a security group named Group1. You need to grant Group1 the Storage File Data SMB Share Elevated Contributor role for share1. What should you do first?

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

[Hide Solution](#)[Discussion 5](#)**Correct Answer:** A 

HOTSPOT -

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



You create an Azure Policy definition named Policy1.

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

NOTE: Each correct selection is worth one point.

## Answer Area

You can assign Policy1 to:

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



You can exclude Policy1 from:

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



From Azure Portal you can only assign to TRGrp, MGrp, Subs1, RG1 only . there is not option to assign to individual resources like VM or NIC etc. if you want a policy to apply to resources under an RG. you have to make sure the scope covers the RG, then from exclusions you can exclude a particular resource under that RG

[https://www.youtube.com/watch?v=XxeSn\\_IWz6I&ab\\_channel=kudvenkat](https://www.youtube.com/watch?v=XxeSn_IWz6I&ab_channel=kudvenkat)

Question #58

Topic 2

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

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

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

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

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

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

Solution: You instruct User2 to create the user accounts.

Does that meet the goal?

A. Yes

B. No

User 1 can but User 2 has nothing to do with the new directory so he/she will not be able to create users in the new tenant. Answer should be **B** in my opinion.

Correct answer is **B**. User 2 is not Global Admin on external tenant.

**Question #59****Topic 2**

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

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

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

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

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

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

Solution: You instruct User4 to create the user accounts.

Does that meet the goal?

A. Yes

B. No **Most Voted**

[Hide Solution](#)[Discussion 28](#)

Correct Answer: B 🎉

**Question #61****Topic 2**

You have two Azure subscriptions named Sub1 and Sub2.

An administrator creates a custom role that has an assignable scope to a resource group named RG1 in Sub1.

You need to ensure that you can apply the custom role to any resource group in Sub1 and Sub2. The solution must minimize administrative effort.

What should you do?

- A. Select the custom role and add Sub1 and Sub2 to the assignable scopes. Remove RG1 from the assignable scopes. **Most Voted**
- B. Create a new custom role for Sub1. Create a new custom role for Sub2. Remove the role from RG1.
- C. Create a new custom role for Sub1 and add Sub2 to the assignable scopes. Remove the role from RG1.
- D. Select the custom role and add Sub1 to the assignable scopes. Remove RG1 from the assignable scopes. Create a new custom role for Sub2.

[Hide Solution](#)[Discussion 8](#)

Correct Answer: A 🎉

You have an Azure Subscription that contains a storage account named storageacct1234 and two users named User1 and User2. You assign User1 the roles shown in the following exhibit.

**User1 assignments – storageacct1234**

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

Search by assignment name or description

Role assignments (2) ①

| Role                          | Scope                      | Group assignment | Condition |
|-------------------------------|----------------------------|------------------|-----------|
| Reader                        | Resource group (inherited) | --               | None      |
| Storage Blob Data Contributor | This resource              | --               | Add       |

Deny assignments (0) ①

Classic administrators (0) ①

Which two actions can User1 perform? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Assign roles to User2 for storageacct1234.

B. Upload blob data to storageacct1234. Most Voted

C. Modify the firewall of storageacct1234.

D. View blob data in storageacct1234. Most Voted

E. View file shares in storageacct1234.

[Hide Solution](#)

[Discussion](#) 39

Correct Answer: AE 🏆

Community vote distribution

BD (98%)

You have an Azure App Services web app named App1. You plan to deploy App1 by using Web Deploy. You need to ensure that the developers of App1 can use their Azure AD credentials to deploy content to App1. The solution must use the principle of least privilege.  
What should you do?

- A. Assign the Owner role to the developers
- B. Configure app-level credentials for FTPS
- C. Assign the Website Contributor role to the developers **Most Voted**
- D. Configure user-level credentials for FTPS

[Hide Solution](#)[Discussion 7](#)

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

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

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

Solution: From Azure AD in the Azure portal, you use the Bulk invite users operation.

Does this meet the goal?

- A. Yes **Most Voted**

- B. No

[Hide Solution](#)[Discussion 5](#)

**Correct Answer:** B 

*Community vote distribution*

A (86%)

14%

You have an Azure subscription that is linked to an Azure AD tenant. The tenant contains the custom role-based access control (RBAC) roles shown in the following table.

| Name  | Description             |
|-------|-------------------------|
| Role1 | Azure subscription role |
| Role2 | Azure AD role           |

From the Azure portal, you need to create two custom roles named Role3 and Role4. Role3 will be an Azure subscription role. Role4 will be an Azure AD role.

Which roles can you clone to create the new roles? To answer, select the appropriate options in the answer area.

#### Answer Area

Role3:

- Role1 only
- Built-in Azure subscription roles only
- Role1 and built-in Azure subscription roles only 
- Built-in Azure subscription roles and built-in Azure AD roles only
- Role1, Role2, built-in Azure subscription roles, and built-in Azure AD roles

Role4:

- Role2 only 
- Built-in Azure AD roles only
- Role2 and built-in Azure AD roles only
- Built-in Azure AD roles and built-in Azure subscription roles only
- Role1, Role2, built-in Azure AD, and built-in Azure subscription roles

You can clone only custom azure ad role or create from scratch.

You have an Azure subscription named Sub1 that contains two users named User1 and User2.

You need to assign role-based access control (RBAC) roles to User1 and User2. The users must be able to perform the following tasks in Sub1:

- User1 must view the data in any storage account.
- User2 must assign users the Contributor role for storage accounts.

The solution must use the principle of least privilege.

Which RBAC role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

## Answer Area

User1: Reader and Data Access

User2: Owner

You have an Azure subscription that contains 10 virtual machines, a key vault named Vault1, and a network security group (NSG) named NSG1. All the resources are deployed to the East US Azure region.

The virtual machines are protected by using NSG1. NSG1 is configured to block all outbound traffic to the internet.

You need to ensure that the virtual machines can access Vault1. The solution must use the principle of least privilege and minimize administrative effort

what should you configure as the destination of the outbound security rule for NSG1?

A. an application security group

B. a service tag

C. an IP address range

[Hide Solution](#)

[Discussion](#) 3

**Correct Answer:** B 

*Community vote distribution*

B (100%)

B - Service Tag is correct.

<https://learn.microsoft.com/en-us/azure/virtual-network/service-tags-overview#available-service-tags>

"AzureKeyVault" tag can be used in outbound NSGs.

You have an Azure AD tenant named adatum.com that contains the groups shown in the following table.

| Name   | Member of   |
|--------|-------------|
| Group1 | <i>None</i> |
| Group2 | Group1      |
| Group3 | Group2      |

Adatum.com contains the users shown in the following table.

| Name  | Member of   |
|-------|-------------|
| User1 | Group1      |
| User2 | Group2      |
| User3 | Group3      |
| User4 | <i>None</i> |

You assign the Azure Active Directory Premium Plan 2 license to Group1 and User4.

Which users are assigned the Azure Active Directory Premium Plan 2 license?

- A. User4 only
- B. User1 and User4 only **Most Voted**
- C. User1, User2, and User4 only
- D. User1, User2, User3, and User4

[Hide Solution](#)[Discussion 7](#)

Correct Answer: B 

Community vote distribution

B (53%) C (20%) 13% 13%

- Group-based licensing currently does not support groups that contain other groups (nested groups). If you apply a license to a nested group, only the immediate first-level user members of the group have the licenses applied.

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced>

You have an Azure AD tenant named contoso.com.

You have two external partner organizations named fabrikam.com and litwareinc.com. Fabrikam.com is configured as a connected organization.

You create an access package as shown in the Access package exhibit. (Click the Access package tab.)

### New access package ...

\* Basics    Resource roles    \* Requests    Requestor information    \*Lifecycle    Review + Create

Summary of access package configuration

Basics

|              |             |
|--------------|-------------|
| Name         | package1    |
| Description  | Guest users |
| Catalog name | General     |

Resource roles

| Resource | Type           | Sub Type       | Role   |
|----------|----------------|----------------|--------|
| Group1   | Group and Team | Security Group | Member |

Requests

|                              |  |
|------------------------------|--|
| Users who can request access | All configured connected organizations |
| Require approval             | No                                     |
| Enabled                      | Yes                                    |

Requestor information

Questions

| Question | Answer format | Multiple choice optio... | Required |
|----------|---------------|--------------------------|----------|
|----------|---------------|--------------------------|----------|

Attributes (Preview)

| Attribute type | Attribute | Default display string | Answer format | Multi |
|----------------|-----------|------------------------|---------------|-------|
|----------------|-----------|------------------------|---------------|-------|

Lifecycle

|                                   |                |
|-----------------------------------|----------------|
| Access package assignments expire | After 365 days |
| Require access reviews            | No             |

You configure the external user lifecycle settings as shown in the Lifecycle exhibit. (Click the Lifecycle tab.)

## Manage the lifecycle of external users

Select what happens when an external user, who was added to your directory through an access package request, loses their last assignment to any access package.

Block external user from signing in to this directory

Yes

No

Remove external user

Yes

No

Number of days before removing external user from this directory

30

## Delegate entitlement management

By default, only Global Administrators and User Administrators can create and manage catalogs, and can manage all catalogs. Users added to entitlement management as Catalog creators can also create catalogs and will become the owner of any catalogs they create.

Catalog creators (1)

0 selected

Add catalog creators

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

### Statements

**Yes**

**No**

Litwareinc.com users can be assigned to package1.

After 365 days, fabrikam.com users will be removed from Group1.

After 395 days, fabrikam.com users will be removed from the contoso.com tenant.

N not a connected organization

N expires not remove

Y  $365 + 30 = 395$  removed



## Question #4

## Topic 3

HOTSPOT -

You have an Azure Storage account named storage1.

You have an Azure App Service app named App1 and an app named App2 that runs in an Azure container instance. Each app uses a managed identity.

You need to ensure that App1 and App2 can read blobs from storage1. The solution must meet the following requirements:

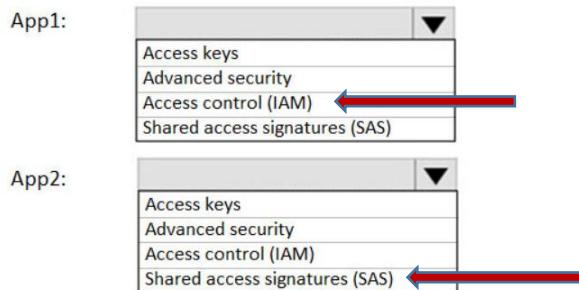
- Minimize the number of secrets used.
- Ensure that App2 can only read from storage1 for the next 30 days.

What should you configure in storage1 for each app? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area



Correct Answer: Box 1: Access Control (IAM) Since the App1 uses Managed Identity, App1 can access the Storage Account via IAM. As per requirement, we need to minimize the number of secrets used, so Access keys is not ideal. Box 2: Shared access signatures (SAS) We need temp access for App2, so we need to use SAS.

## Question #7

## Topic 3

HOTSPOT -

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

| Name  | Type            | Resource group |
|-------|-----------------|----------------|
| VNET1 | Virtual network | RG1            |
| VNET2 | Virtual network | RG2            |
| VM1   | Virtual machine | RG2            |

The status of VM1 is Running.

You assign an Azure policy as shown in the exhibit. (Click the Exhibit tab.)

Home > Policy - Assignments > Assign Policy

## Assign Policy

**SCOPE**

\* Scope ([Learn more about setting the scope](#))  
Azure Pass/RG2 ...

Exclusions  
*Optionally select resources to exempt from the policy assignment* ...

**BASICS**

\* Policy definition  
Not allowed resource types ✓ ...

\* Assignment name i  
Not allowed resource types ✓

Description

Assigned by  
First User

**PARAMETERS**

\* Not allowed resource types i  
3 selected ✓

Assign Cancel

You assign the policy by using the following parameters:

Microsoft.ClassicNetwork/virtualNetworks

Microsoft.Network/virtualNetworks

Microsoft.Compute/virtualMachines

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

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

| Statements   | Yes                   | No   |
|--|-----------------------|--|
| An administrator can move VNET1 to RG2                 | <input type="radio"/> | <input checked="" type="radio"/>  |
| The state of VM1 changed to deallocated                | <input type="radio"/> | <input checked="" type="radio"/>  |
| An administrator can modify the address space of VNET2 | <input type="radio"/> | <input checked="" type="radio"/>  |

Tested in Lab:

- 1) An administrator can move VNET1 to RG2: "No"  
" ERROR: Resource 'VNET1' was disallowed by policy. ( Code: RequestDisallowedByPolicy)
- 2) The state of VM1 changed to deallocated: "No"  
It changes to Non-compliant
- 3) An administrator can modify the address space of VNET2: "No"  
ERROR: Failed to save address space changes to virtual network 'VNET2'. Error:  
Resource 'VNET2' was disallowed by policy.

**HOTSPOT -**

You have Azure subscription that includes following Azure file shares:

| Name   | In storage account | Location |
|--------|--------------------|----------|
| share1 | storage1           | West US  |
| share2 | storage1           | West US  |

You have the following on-premises servers:

| Name    | Folders                |
|---------|------------------------|
| Server1 | D:\Folder1, E:\Folder2 |
| Server2 | D:\Data                |

You create a Storage Sync Service named Sync1 and an Azure File Sync group named Group1. Group1 uses share1 as a cloud endpoint.

You register Server1 and Server2 in Sync1. You add D:\Folder1 on Server1 as a server endpoint of Group1.

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

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

| Statements   | Yes  | No  |
|--|--|---|
| share2 can be added as a cloud endpoint for Group1                 | <input type="radio"/>  | <input type="radio"/>              |
| E:\Folder2 on Server1 can be added as a server endpoint for Group1 | <input type="radio"/>  | <input checked="" type="radio"/>  |
| D:\Data on Server2 can be added as a server endpoint for Group1    | <input checked="" type="radio"/>  | <input type="radio"/>   |

Correct Answer:

Box 1: No

A sync group contains one cloud endpoint, or Azure file share, and at least one server endpoint.

Box 2: No

Azure File Sync does not support more than one server endpoint from the same server in the same Sync Group.

Box 3: Yes

Multiple server endpoints can exist on the same volume if their namespaces are not overlapping (for example, F:\sync1 and F:\sync2) and each endpoint is syncing to a unique sync group.

**HOTSPOT -**

You have an Azure File sync group that has the endpoints shown in the following table.

| Name      | Type            |
|-----------|-----------------|
| Endpoint1 | Cloud endpoint  |
| Endpoint2 | Server endpoint |
| Endpoint3 | Server endpoint |

Cloud tiering is enabled for Endpoint3.

You add a file named File1 to Endpoint1 and a file named File2 to Endpoint2.

On which endpoints will File1 and File2 be available within 24 hours of adding the files? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

File1:

Endpoint1 only

Endpoint3 only

Endpoint2 and Endpoint3 only

Endpoint1, Endpoint2, and Endpoint3

File2:

Endpoint2 only

Endpoint3 only

Endpoint2 and Endpoint3 only

Endpoint1, Endpoint2, and Endpoint3

Correct Answer:

File1: Endpoint1 only

It is a cloud endpoint, and it is scanned by the detection job every 24 hours.

File2: Endpoint1, Endpoint2 and Endpoint3

With the on-premises servers the file is scanned and synced automatically after it's being added.

**Note:** They changed the question in Exam from "within 24 hours" to "after 24 hours". So, the answer is:

File1: Endpoint1, Endpoint2 and Endpoint3

File2: Endpoint1, Endpoint2 and Endpoint3

## HOTSPOT -

You have several Azure virtual machines on a virtual network named VNet1.

You configure an Azure Storage account as shown in the following exhibit.

The screenshot shows the Azure Storage account settings for 'contoso'. The left sidebar lists various options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Events, Storage Explorer (preview), SETTINGS, Access keys, Configuration, Encryption, Shared access signature, Firewalls and virtual networks (which is selected), Properties, Locks, and Automation script. The main pane shows 'Firewalls and virtual networks' settings. It has a 'Save' and 'Discard' button at the top. Under 'Allow access from', 'Selected networks' is selected over 'All networks'. A note says 'Configure network security for your storage accounts.' Below this is a table for 'Virtual networks'. It shows one entry for 'VNet1' with subnet '1', address range '10.2.0.0/16', endpoint 'DemoRG', and subscription 'Production'. Another row below it shows 'Prod' with address range '10.2.0.0/24', status 'Enabled', endpoint 'DemoRG', and subscription 'Production'. Under 'Firewall', it says 'Add IP ranges to allow access from the Internet or your on-premises networks.' Below this is an 'ADDRESS RANGE' section with a text input field for 'IP address or CIDR'. The 'Exceptions' section contains three checkboxes: 'Allow trusted Microsoft services to access this storage account' (checked), 'Allow read access to storage logging from any network' (unchecked), and 'Allow read access to storage metrics from any network' (unchecked).

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

The virtual machines on the 10.2.9.0/24 subnet will have network connectivity to the file shares in the storage account [answer choice].

|                 |
|-----------------|
| always          |
| during a backup |
| never           |

Azure Backup will be able to back up the unmanaged hard disks of the virtual machines in the storage account [answer choice].

|                 |
|-----------------|
| always          |
| during a backup |
| never           |

Correct Answer:

VNet1's address space is 10.2.0.0/16. The VNet1 has only 1 Subnet associated: 10.2.0.0/24.

The address space of a VNet is irrelevant if there isn't a corresponding Subnet from, which VMs can be assigned IP addresses.

Box1: Never

VMs from 10.2.9.0/24 (10.2.9.0 - 10.2.9.255) are out of Subnet. Subnet IP range 10.2.0.0 - 10.2.0. 255.

Box2: Never

Since the checkbox to allow trusted Microsoft services is not checked. After you configure firewall and virtual network settings for your storage account, select Allow trusted Microsoft services to access this storage account as an exception to enable Azure Backup service to access the network restricted storage account.

Question #14

Topic 3

HOTSPOT -

You have a sync group named Sync1 that has a cloud endpoint. The cloud endpoint includes a file named File1.txt.

Your on-premises network contains servers that run Windows Server 2016. The servers are configured as shown in the following table.

| Name    | Share  | Share contents       |
|---------|--------|----------------------|
| Server1 | Share1 | File1.txt, File2.txt |
| Server2 | Share2 | File2.txt, File3.txt |

You add Share1 as an endpoint for Sync1. One hour later, you add Share2 as an endpoint for Sync1.

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

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

| Statements   | Yes  | No  |
|--|--|---|
| On the cloud endpoint, File1.txt is overwritten by File1.txt from Share1.  | <input type="radio"/>  | <input type="radio"/>  |
| On Server1, File1.txt is overwritten by File1.txt from the cloud endpoint. | <input type="radio"/>  | <input type="radio"/>  |
| File1.txt from Share1 replicates to Share2.                                | <input checked="" type="radio"/>  | <input type="radio"/>   |

1) On the cloud endpoint, File1.txt is overwritten by File1.txt from Share1: "No"

2) On Server1, File1.txt is overwritten by File1.txt from the cloud endpoint: "No"

3) File1.txt from Share1 replicates to Share2: "Yes"

Explanation: Files are never overwritten. At most when they have the same name the older one is renamed to "[FILE\_NAME]\_[SERVER\_NAME].[EXTENSION]".

**Question #16****Topic 3**

You have an Azure subscription that contains a storage account named account1.

You plan to upload the disk files of a virtual machine to account1 from your on-premises network. The on-premises network uses a public IP address space of 131.107.1.0/24.

You plan to use the disk files to provision an Azure virtual machine named VM1. VM1 will be attached to a virtual network named VNet1. VNet1 uses an IP address space of 192.168.0.0/24.

You need to configure account1 to meet the following requirements:

- Ensure that you can upload the disk files to account1.
- Ensure that you can attach the disks to VM1.
- Prevent all other access to account1.

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

NOTE: Each correct selection is worth one point.

- A. From the Networking blade of account1, select Selected networks. **Most Voted**
- B. From the Networking blade of account1, select Allow trusted Microsoft services to access this storage account.
- C. From the Networking blade of account1, add the 131.107.1.0/24 IP address range. **Most Voted**
- D. From the Networking blade of account1, add VNet1.
- E. From the Service endpoints blade of VNet1, add a service endpoint.

A. From the Networking blade of account1, select Selected networks.

C. From the Networking blade of account1, add the 131.107.1.0/24 IP address range.

Explanations: Azure Storage offers a multi-layered security model. Thanks to this model, you can protect your storage accounts for a specific group of supported networks. If network rules have been configured, only applications that request data from the specified group of networks can access a storage account.

**Question #20****Topic 3**

You have a Recovery Service vault that you use to test backups. The test backups contain two protected virtual machines.

You need to delete the Recovery Services vault.

What should you do first?

- A. From the Recovery Service vault, delete the backup data.
- B. Modify the disaster recovery properties of each virtual machine.
- C. Modify the locks of each virtual machine.
- D. From the Recovery Service vault, stop the backup of each backup item. **Most Voted**

[Hide Solution](#)[Discussion 50](#)

Correct Answer: D 

**HOTSPOT -**

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

| Name     | Type                    | Location   | Resource group        |
|----------|-------------------------|------------|-----------------------|
| RG1      | Resource group          | West US    | <i>Not applicable</i> |
| RG2      | Resource group          | West US    | <i>Not applicable</i> |
| Vault1   | Recovery Services vault | Central US | RG1                   |
| Vault2   | Recovery Services vault | West US    | RG2                   |
| VM1      | Virtual machine         | Central US | RG2                   |
| storage1 | Storage account         | West US    | RG1                   |
| SQL1     | Azure SQL database      | East US    | RG2                   |

In storage1, you create a blob container named blob1 and a file share named share1.

Which resources can be backed up to Vault1 and Vault2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Can use Vault1 for backups:

|                              |
|------------------------------|
| VM1 only                     |
| VM1 and share1 only          |
| VM1 and SQL1 only            |
| VM1, storage1, and SQL1 only |
| VM1, blob1, share1, and SQL1 |

Can use Vault2 for backups:

|                        |
|------------------------|
| storage1 only          |
| share1 only            |
| VM1 and share1 only    |
| blob1 and share1 only  |
| storage1 and SQL1 only |

Box 1: VM1 only

**VM1 is in the same region as Vault1.** File1 is not in the same region as Vault1. SQL is not in the same region as Vault1. **Blobs cannot be backup up to service vaults.** Note: To create a Vault to protect VMs, the Vault must be in the same Region as the VMs.

Box 2: Share1 only

Storage1 is in the same region as Vault2. Share1 is in Storage1.

Note:

**Only VM and File share is allowed to Backup.**

**Blob container cannot be backed up to service vault.**

**Question #22****Topic 3**

You have an Azure subscription named Subscription1.  
You have 5 TB of data that you need to transfer to Subscription1.  
You plan to use an Azure Import/Export job.  
What can you use as the destination of the imported data?

- A. a virtual machine
- B. an Azure Cosmos DB database
- C. Azure File Storage **Most Voted**
- D. the Azure File Sync Storage Sync Service

**Hide Solution****Discussion** 26**Correct Answer:** C 🎉**Question #25****Topic 3****HOTSPOT -**

You have an Azure Storage account named storage1 that uses Azure Blob storage and Azure File storage.  
You need to use AzCopy to copy data to the blob storage and file storage in storage1.  
Which authentication method should you use for each type of storage? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area****Blob storage:**

|  |
|--|
| Azure Active Directory (Azure AD) only   |
| Shared access signatures (SAS) only  |
| Access keys and shared access signatures (SAS) only                                |
| <b>Azure Active Directory (Azure AD) and shared access signatures (SAS) only</b>   |
| Azure Active Directory (Azure AD), access keys, and shared access signatures (SAS) |

**File storage:**

|  |
|--|
| Azure Active Directory (Azure AD) only   |
| <b>Shared access signatures (SAS) only</b>   |
| Access keys and shared access signatures (SAS) only                                |
| Azure Active Directory (Azure AD) and shared access signatures (SAS) only          |
| Azure Active Directory (Azure AD), access keys, and shared access signatures (SAS) |

**Correct Answer:**

In **azcopy** you can provide authorization credentials by using Azure Active Directory (AD), or  
by using a Shared Access Signature (SAS) token.

Box 1: Both Azure Active Directory (AD) and Shared Access Signature (SAS) token are  
supported for Blob storage.

Box 2: Only Shared Access Signature (SAS) token is supported for File storage.

Reference: <https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10>

**Question #26****Topic 3**

You have an Azure subscription that contains an Azure Storage account.

You plan to create an Azure container instance named container1 that will use a Docker image named Image1. Image1 contains a Microsoft SQL Server instance that requires persistent storage.

You need to configure a storage service for Container1.

What should you use?

A. Azure Files **Most Voted**

B. Azure Blob storage

C. Azure Queue storage

D. Azure Table storage

[Hide Solution](#)[Discussion \(138\)](#)

**Correct Answer:** A 

Reference:

Azure Files is the correct answer. The keyword here is: "persistent"

<https://azure.microsoft.com/en-us/blog/persistent-docker-volumes-with-azure-file-storage/>

**Question #29****Topic 3**

DRAG DROP -

You have an Azure subscription that contains an Azure file share.

You have an on-premises server named Server1 that runs Windows Server 2016.

You plan to set up Azure File Sync between Server1 and the Azure file share.

You need to prepare the subscription for the planned Azure File Sync.

Which two actions should you perform in the Azure subscription? To answer, drag the appropriate actions to the correct targets. Each action may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

**Actions**

Create a Storage Sync Service

Install the Azure File Sync agent

Create a sync group

Run Server Registration

**Answer Area**

First action:

Action

Second action:

Action

Yes, the question is very specific as to which actions to be performed in AZURE SUBSCRIPTION.

The answer should be CREATE STORAGE SYNC SERVICE and CREATE SYNC GROUP. The installation of the agent will be on-premise server. So, this action is not taking Place in Azure Subscription.

HOTSPOT -

You have an Azure subscription named Subscription1 that contains the resources shown in the following table:

| Name       | Type                    | Location    | Resource group        |
|------------|-------------------------|-------------|-----------------------|
| RG1        | Resource group          | East US     | <i>Not applicable</i> |
| RG2        | Resource group          | West US     | <i>Not applicable</i> |
| Vault1     | Recovery Services vault | West Europe | RG1                   |
| storage1   | Storage account         | East US     | RG2                   |
| storage2   | Storage account         | West US     | RG1                   |
| storage3   | Storage account         | West Europe | RG2                   |
| Analytics1 | Log Analytics workspace | East US     | RG1                   |
| Analytics2 | Log Analytics workspace | West US     | RG2                   |
| Analytics3 | Log Analytics workspace | West Europe | RG1                   |

You plan to configure Azure Backup reports for Vault1.

You are configuring the Diagnostics settings for the AzureBackupReports log.

Which storage accounts and which Log Analytics workspaces can you use for the Azure Backup reports of Vault1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Storage accounts:

storage1 only

storage2 only

storage3 only

storage1, storage2, and storage3

Log Analytics workspaces:

Analytics1 only

Analytics2 only

Analytics3 only

Analytics1, Analytics2, and Analytics3

Correct Answer:

Storage accounts: Storage 3 only

Storage Account must be in the same Region as the Recovery Services Vault. Log Analytics workspaces: Analytics1, Analytics2, and Analytics3

Set up one or more Log Analytics workspaces to store your Backup reporting data. The location and subscription where this Log Analytics workspace can be created is independent of the location and subscription where your Vaults exist.

**HOTSPOT -**

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

## Storage accounts

Default Directory

 Add  Manage view  Refresh  Export to CSV |  Assign tags  Delete |  Feedback

Filter by name...  Subscription == all  Resource group == all  Location == all  Add filter

Showing 1 to 4 of 4 records.

| <input type="checkbox"/> | Name ↑↓    | Type ↑↓         | Kind ↑↓     | Resource group ↑↓ | Location ↑↓ |
|--------------------------|------------|-----------------|-------------|-------------------|-------------|
| <input type="checkbox"/> | contoso101 | Storage account | StorageV2   | RG1               | East US     |
| <input type="checkbox"/> | contoso102 | Storage account | Storage     | RG1               | East US     |
| <input type="checkbox"/> | contoso103 | Storage account | BlobStorage | RG1               | East US     |
| <input type="checkbox"/> | contoso104 | Storage account | FileStorage | RG1               | East US     |

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

You can create a premium file share in

 contoso101 only  
contoso104 only  
contoso101 or contoso104 only  
contoso101, contoso102, or contoso104 only  
contoso101, contoso102, contoso103, or contoso104

You can use the Archive access tier in

 contoso101 only  
contoso101 or contoso103 only  
contoso101, contoso102, and contoso103 only  
contoso101, contoso102, and contoso104 only  
contoso101, contoso102, contoso103, and contoso104

Box 1: contoso104 only

Premium file shares are hosted in a special purpose storage account kind, called a FileStorage account.

Box 2: contoso101 and contos103 only

Object storage data tiering between hot, cool, and archive is supported in Blob Storage and General Purpose v2 (GPv2) accounts. General Purpose v1 (GPv1) accounts don't support tiering. The archive tier supports only LRS, GRS, and RA-GRS.

Question #36

Topic 3

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

| Name     | Type             | Performance |
|----------|------------------|-------------|
| storage1 | StorageV2        | Standard    |
| storage2 | BlobStorage      | Standard    |
| storage3 | BlockBlobStorage | Premium     |
| storage4 | FileStorage      | Premium     |

You plan to manage the data stored in the accounts by using lifecycle management rules.

To which storage accounts can you apply lifecycle management rules?

- A. storage1 only
- B. storage1 and storage2 only
- C. storage3 and storage4 only
- D. storage1, storage2, and storage3 only Most Voted
- E. storage1, storage2, storage3, and storage4

[Hide Solution](#)

[Discussion](#) 58

Correct Answer: D 

Question #39

Topic 3

HOTSPOT -

You have an Azure subscription that contains an Azure Storage account named storageaccount1.

You export storageaccount1 as an Azure Resource Manager template. The template contains the following sections.

```
{  
    "type": "Microsoft.Storage/storageAccount",  
    "apiVersion": "2019-06-01",  
    "name": "storageaccount1",  
    "location": "eastus",  
    "sku": {  
        "name": "Standard_LRS",  
        "tier": "Standard"  
    },  
    "kind": "StorageV2",  
    "properties": {  
        "networkAcls": {  
            "bypass": "AzureServices",  
            "virtualNetworkRules": [],  
            "ipRules": [],  
            "defaultAction": "Allow",  
        },  
        "supportsHttpsTrafficOnly": true,  
        "encryption": {  
            "services": {  
                "file": {  
                    "keyType": "Account",  
                    "enabled": true  
                }  
                "blob": {  
                    "keyType": "Account",  
                    "enabled": true  
                }  
            },  
            "keySource": "Microsoft.Storage"  
        },  
        "accessTier": "Hot"  
    }  
},
```

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

NOTE: Each correct selection is worth one point

Hot Area:

## Answer Area

| Statements  | Yes                              | No                               |
|---|----------------------------------|----------------------------------|
| A server that has a public IP address of 131.107.103.10 can access storageaccount1  | <input checked="" type="radio"/> | <input type="radio"/>            |
| Individual blobs in storageaccount1 can be set to use the archive tier  | <input checked="" type="radio"/> | <input type="radio"/>            |
| Global administrations in Azure Active Directory (Azure AD) can access a file share hosted in storageaccount1 by using their Azure AD credentials | <input type="radio"/>            | <input checked="" type="radio"/> |

### Question #40

Topic 3

You have an Azure subscription that contains a storage account named storage1.

You have the devices shown in the following table.

| Name    | Platform   |
|---------|------------|
| Device1 | Windows 10 |
| Device2 | Linux      |
| Device3 | macOS      |

From which devices can you use AzCopy to copy data to storage1?

- A. Device 1 only
- B. Device1, Device2 and Device3 Most Voted
- C. Device1 and Device2 only
- D. Device1 and Device3 only

[Hide Solution](#)

[Discussion 7](#)

Correct Answer: B 🎉

You have an Azure Storage account named storage1 that contains a blob container named container1.

You need to prevent new content added to container1 from being modified for one year.

What should you configure?

- A. the access tier
- B. an access policy** Most Voted
- C. the Access control (IAM) settings
- D. the access level

[Hide Solution](#)
[Discussion 16](#)

Correct Answer: B 🎉

HOTSPOT -

You have an Azure Storage account named storage1 that contains a blob container. The blob container has a default access tier of Hot. Storage1 contains a container named container1.

You create lifecycle management rules in storage1 as shown in the following table.

| Name  | Rule scope                      | Blob type   | Blob subtype | Rule block   | Prefix match          |
|-------|---------------------------------|-------------|--------------|--|-----------------------|
| Rule1 | Limit blobs by using filters.   | Block blobs | Base blobs   | If base blobs were not modified for two days, move to archive storage.<br>If base blobs were not modified for nine days, delete the blob.        | container1/Dep1       |
| Rule2 | Apply to all blobs in storage1. | Block blobs | Base blobs   | If base blobs were not modified for three days, move to cool storage.<br>If base blobs were not modified for nine days, move to archive storage. | <b>Not applicable</b> |

You perform the actions shown in the following table.

| Date      | Action  |
|-----------|---|
| October 1 | Upload three files named Dep1File1.docx, File2.docx, and File3.docx to container 1. |
| October 2 | Edit Dep1File1.docx and File3.docx.   |
| October 5 | Edit File2.docx.  |

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

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

| Statements                                  | Yes                              | No                    |
|---|----------------------------------|-----------------------|
| On October 10, you can read Dep1File1.docx. | <input checked="" type="radio"/> | <input type="radio"/> |
| On October 10, you can read File2.docx.     | <input checked="" type="radio"/> | <input type="radio"/> |
| On October 10, you can read File3.docx.     | <input checked="" type="radio"/> | <input type="radio"/> |

Rule1 does not apply to Dep1File1.docx since in order this to be applied the filename should have been container1/Dep1/File1.docx

So the reply is Yes\Yes\Yes

Question #43

Topic 3

You are configuring Azure Active Directory (Azure AD) authentication for an Azure Storage account named storage1.

You need to ensure that the members of a group named Group1 can upload files by using the Azure portal. The solution must use the principle of least privilege.

Which two roles should you configure for storage1? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Storage Account Contributor Most Voted

B. Storage Blob Data Contributor Most Voted Most Voted

C. Reader Most Voted

D. Contributor

E. Storage Blob Data Reader

[Hide Solution](#)

[Discussion](#) 30

**Correct Answer:** BC 

To access blob data in the Azure portal with Azure AD credentials, a user must have the following role assignments:

\* A data access role, such as Storage Blob Data Reader or Storage Blob Data Contributor

\* The Azure Resource Manager Reader role, at a minimum

The Reader role is an Azure Resource Manager role that permits users to view storage account resources, but not modify them. It does not provide read permissions to data in Azure Storage, but only to account management resources. The Reader role is necessary so that users can navigate to blob containers in the Azure portal.

Note: in order from least to greatest permissions:

The Reader and Data Access role -

The Storage Account Contributor role

The Azure Resource Manager Contributor role

The Azure Resource Manager Owner role

Reference:

<https://docs.microsoft.com/en-us/azure/storage/blobs/assign-azure-role-data-access>

*Community vote distribution*

BC (63%)

AB (23%)

7%

HOTSPOT -

You have an Azure Storage account named storage1 that stores images.

You need to create a new storage account and replicate the images in storage1 to the new account by using object replication.

How should you configure the new account? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Account type:

|  |
|--|
| StorageV2 only                         |
| StorageV2 or FileStorage only          |
| StorageV2 or BlobStorage only          |
| StorageV2, BlobStorage, or FileStorage |

Object type to create in the new account:

|            |
|------------|
| Container  |
| File share |
| Table      |
| Queue      |

You have an Azure subscription.

In the Azure portal, you plan to create a storage account named storage1 that will have the following settings:

- Performance: Standard
- Replication: Zone-redundant storage (ZRS)
- Access tier (default): Cool
- Hierarchical namespace: Disabled

You need to ensure that you can set Account kind for storage1 to BlockBlobStorage.

Which setting should you modify first?

A. Performance **Most Voted**

B. Replication

C. Access tier (default)

D. Hierarchical namespace

[Hide Solution](#)

[Discussion 15](#)

Correct Answer: A 🎉

You create an Azure Storage account.

You plan to add 10 blob containers to the storage account.

For one of the containers, you need to use a different key to encrypt data at rest.

What should you do before you create the container?

A. Generate a shared access signature (SAS).

B. Modify the minimum TLS version.

C. Rotate the access keys.

D. Create an encryption scope. **Most Voted**

[Hide Solution](#)

[Discussion](#) 8

Correct Answer: D 🎉

D) "Create an encryption scope."

Encryption scopes enable you to manage encryption with a key that is scoped to a container or an individual blob. You can use encryption scopes to create secure boundaries between data that resides in the same storage account but belongs to different customers.

You have an Azure subscription. The subscription contains a storage account named storage1 that has the lifecycle management rules shown in the following table.

| Name  | Blob prefix           | If base were last modified more than (days ago) | Then                    |
|-------|-----------------------|---|-------------------------|
| Rule1 | container1/           | 3 days  | Move to archive storage |
| Rule2 | <i>Not applicable</i> | 5 days  | Move to cool storage    |
| Rule3 | container2/           | 10 days   | Delete the blob         |
| Rule4 | container2/           | 15 days   | Move to archive storage |

On June 1, you store two blobs in storage1 as shown in the following table.

| Name  | Location   | Access tier |
|-------|------------|-------------|
| File1 | container1 | Hot         |
| File2 | container2 | Hot         |

### Answer Area

- | Statements   | Yes                   | No                               |
|--|-----------------------|----------------------------------|
| On June 6, File1 will be stored in the Cool access tier.     | <input type="radio"/> | <input checked="" type="radio"/> |
| On June 1, File2 will be stored in the Cool access tier.     | <input type="radio"/> | <input checked="" type="radio"/> |
| On June 16, File2 will be stored in the Archive access tier. | <input type="radio"/> | <input checked="" type="radio"/> |

You have an Azure subscription.

You plan to deploy a storage account named storage1 by using the following Azure Resource Manager (ARM) template.

```
{  
    "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",  
    "contentVersion": "1.0.0.0",  
    "resources": [  
        {  
            "name": "storage1",  
            "type": "Microsoft.Storage/storageAccounts",  
            "apiVersion": "2021-08-01",  
            "location": "East US",  
            "properties": {  
                "allowBlobPublicAccess": true,  
                "defaultToOAuthAuthentication": false,  
                "networkAcls": {  
                    "bypass": "AzureServices",  
                    "defaultAction": "Allow",  
                    "ipRules": []  
                }  
            },  
            "sku": {  
                "name": "Standard_LRS"  
            },  
            "kind": "StorageV2"  
        },  
        {  
            "name": "storage1/default",  
            "type": "Microsoft.Storage/storageAccounts/blobServices",  
            "apiVersion": "2021-08-01",  
            "properties": {  
                "restorePolicy": {  
                    "enabled": true,  
                    "days": 6  
                },  
                "deleteRetentionPolicy": {  
                    "enabled": true,  
                    "days": 7  
                },  
                "containerDeleteRetentionPolicy": {  
                    "enabled": true,  
                    "days": 7  
                },  
                "changeFeed": {  
                    "enabled": true  
                },  
                "isVersioningEnabled": true  
            },  
            "dependsOn": [  
                "[concat('Microsoft.Storage/storageAccounts/', 'storage1')]"  
            ]  
        }  
    ]  
}
```

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

| Statements  | Yes                              | No                               |
|---|----------------------------------|----------------------------------|
| Changes made to the data in storage1 can be rolled back after seven days. | <input type="radio"/>            | <input checked="" type="radio"/> |
| Only users located in the East US Azure region can connect to storage1.   | <input type="radio"/>            | <input checked="" type="radio"/> |
| Three copies of storage1 will be maintained in the East US Azure region.  | <input checked="" type="radio"/> | <input type="radio"/>            |

### Question #51

Topic 3

You have an on-premises server that contains a folder named D:\Folder1.

You need to copy the contents of D:\Folder1 to the public container in an Azure Storage account named contosodata.

Which command should you run?

- A. az storage blob copy start D:\Folder1 https://contosodata.blob.core.windows.net/public
- B. azcopy sync D:\folder1 https://contosodata.blob.core.windows.net/public --snapshot
- C. azcopy copy D:\folder1 https://contosodata.blob.core.windows.net/public --recursive
- D. az storage blob copy start-batch D:\Folder1 https://contosodata.blob.core.windows.net/public

[Hide Solution](#)

[Discussion](#) 3

**Correct Answer:** C 

*Community vote distribution*

C (100%)

You have an Azure subscription that contains a storage account named storage1. The storage1 account contains a container named container1.

You need to create a lifecycle management rule for storage1 that will automatically move the blobs in container1 to the lowest-cost tier after 90 days.

How should you complete the rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

```
{
  "rules": [
    {
      "enabled": true,
      "name": "rule1",
      "type": "Lifecycle",
      "definition": {
        "actions": {
          "baseBlob": {
            "enableAutoTierToHotFromCool": {
              "tierToArchive": {},
              "tierToCool": {}
            }
          },
          "daysAfterModificationGreaterThan": 90
        }
      }
    }
  ],
  "filters": {
    "blobIndexMatch": [],
    "blobTypes": [],
    "prefixMatch": []
  }
}
***
```

You have an Azure subscription that contains a virtual machine named VM1.

You need to back up VM1. The solution must ensure that backups are stored across three availability zones in the primary region.

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

**Answer Area**

Create a Recovery Services vault.

Set Replication to Zone-redundant storage (ZRS).

For VM1, create a backup policy and configure the backup.

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

| Name       | Type            |
|------------|-----------------|
| storage1   | Storage account |
| container1 | Blob container  |
| table1     | Storage table   |

You need to perform the tasks shown in the following table.

| Name  | Type                                 |
|-------|--------------------------------------|
| Task1 | Create a new storage account.        |
| Task2 | Upload an append blob to container1. |
| Task3 | Create a file share in storage1.     |
| Task4 | Add data to table1.                  |

Which tasks can you perform by using Azure Storage Explorer?

- A. Task1 and Task3 only
- B. Task1, Task2, and Task3 only
- C. Task1, Task3, and Task4 only
- D. Task2, Task3, and Task4 only
- E. Task1, Task2, Task3, and Task4

Hide SolutionDiscussion

4

Correct Answer: D 

Azure Storage Explorer does not have the ability to create a new storage account directly. Instead, you can use Azure Storage Explorer to connect to and manage existing storage accounts in Azure.

You have an Azure AD user named User1 and a read-access geo-redundant storage (RA-GRS) account named contoso2023.

You need to meet the following requirements:

- User1 must be able to write blob data to contoso2023.
- The contoso2023 account must fail over to its secondary endpoint.

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

The screenshot shows the Azure Storage Account settings for 'contoso2023'. The left sidebar lists several categories: 'Search (Ctrl + /)', 'Diagnose and solve problems', 'Access Control (IAM)', 'Data migration', 'Events', and 'Storage browser'. Below these are sections for 'Data storage' (Containers, File shares, Queues, Tables) and 'Security + networking' (Networking, Azure CDN, Access keys, Shared access signature, Encryption, Microsoft Defender for Cloud). At the bottom is a 'Data management' section containing 'Geo-replication', 'Data protection', 'Object replication', 'Blob inventory', 'Static website', and 'Lifecycle management'. The 'Access Control (IAM)' and 'Geo-replication' items are highlighted with red boxes.

You have an Azure subscription that contains a storage account named storage1.

You plan to create a blob container named container1.

You need to use customer-managed key encryption for container1.

Which key should you use?

- A. an EC key that uses the P-384 curve only
  - B. an EC key that uses the P-521 curve only
  - C. an EC key that uses the P-384 curve or P-521 curve only
  - D. an RSA key with a key size of 4096 only
- E. an RSA key type with a key size of 2048, 3072, or 4096 only Most Voted

[Hide Solution](#)[Discussion 4](#)

**Correct Answer:** E 

*Community vote distribution*

E (89%)

11%

## Topic 4 - Question Set 4

### Question #1

Topic 4

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

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

You deploy an Azure Kubernetes Service (AKS) cluster named AKS1.

You need to deploy a YAML file to AKS1.

Solution: From Azure CLI, you run az aks.

Does this meet the goal?

A. Yes

B. No **Most Voted**

[Hide Solution](#)

[Discussion 11](#)

Correct Answer: **B** 🏆

Correct Answer B - No

To deploy the YAML file you need to runs kubectl apply -f file\_name.yaml

You plan to automate the deployment of a virtual machine scale set that uses the Windows Server 2016 Datacenter image.

You need to ensure that when the scale set virtual machines are provisioned, they have web server components installed.

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

NOTE: Each correct selection is worth one point.

- A. Upload a configuration script **Most Voted**
- B. Create an automation account
- C. Create an Azure policy
- D. Modify the extensionProfile section of the Azure Resource Manager template **Most Voted**
- E. Create a new virtual machine scale set in the Azure portal

[Hide Solution](#)

[Discussion 84](#)

**Correct Answer:** DE 

Virtual Machine Scale Sets can be used with the Azure Desired State Configuration (DSC) extension handler. Virtual machine scale sets provide a way to deploy and manage large numbers of virtual machines, and can elastically scale in and out in response to load. DSC is used to configure the VMs as they come online so they are running the production software.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-dsc>

*Community vote distribution*

AD (82%)

DE (18%)

Correct Answer: A and D

The Custom Script Extension downloads and executes scripts on Azure VMs. This extension is useful for post deployment configuration, software installation, or any other configuration / management task. Scripts can be downloaded from Azure storage or GitHub, or provided to the Azure portal at extension run-time.

The Custom Script extension integrates with Azure Resource Manager templates, and can also be used with the Azure CLI, Azure PowerShell, Azure portal, or the REST API. The following Custom Script Extension definition downloads a sample script from GitHub, installs the required packages, then writes the VM instance hostname to a basic HTML page.

DRAG DROP -

You onboard 10 Azure virtual machines to Azure Automation State Configuration.

You need to use Azure Automation State Configuration to manage the ongoing consistency of the virtual machine configurations.

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

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

Select and Place:

## Actions

## Answer Area

Assign tags to the virtual machines

Check the compliance status of the node

Compile a configuration into a node configuration

Upload a configuration to Azure Automation State Configuration

Create a management group



1. Upload a configuration to Azure Automation State Configuration
2. Compile a configuration into a node configuration
3. Check the compliance status of the node.

### Question #12

### Topic 4

You have an Azure Resource Manager template named Template1 that is used to deploy an Azure virtual machine.

Template1 contains the following text:

```
"location": {  
    "type": "String",  
    "defaultValue": "eastus",  
    "allowedValues": [  
        "canadacentral",  
        "eastus",  
        "westeurope",  
        "westus" ]  
}
```

The variables section in Template1 contains the following text:

```
"location": "westeurope"
```

The resources section in Template1 contains the following text:

```
"type": "Microsoft.Compute/virtualMachines",  
"apiVersion": "2018-10-01",  
"name": "[variables('vmName')]",  
"location": "westeurope",
```

You need to deploy the virtual machine to the West US location by using Template1.

What should you do?

A. Modify the location in the resources section to westus Most Voted

B. Select West US during the deployment

C. Modify the location in the variables section to westus

[Hide Solution](#)

[Discussion 48](#)

**Correct Answer:** A 🎉

*Community vote distribution*

A (100%)

## Question #19

Topic 4

You have an Azure subscription that contains a web app named webapp1.

You need to add a custom domain named www.contoso.com to webapp1.

What should you do first?

A. Create a DNS record Most Voted

B. Add a connection string

C. Upload a certificate.

D. Stop webapp1.

[Hide Solution](#)

[Discussion 24](#)

**Correct Answer:** A 🎉

You can use either a CNAME record or an A record to map a custom DNS name to App Service.

Reference:

<https://docs.microsoft.com/en-us/Azure/app-service/app-service-web-tutorial-custom-domain>

*Community vote distribution*

A (100%)

### Question #30

Topic 4

You have an Azure subscription named Subscription1 that has the following providers registered:

- Authorization
- Automation
- Resources
- Compute
- KeyVault
- Network
- Storage
- Billing
- Web

Subscription1 contains an Azure virtual machine named VM1 that has the following configurations:

- Private IP address: 10.0.0.4 (dynamic)
- Network security group (NSG): NSG1
- Public IP address: None
- Availability set: AVSet
- Subnet: 10.0.0.0/24
- Managed disks: No
- Location: East US

You need to record all the successful and failed connection attempts to VM1.

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

NOTE: Each correct selection is worth one point.

A. Enable Azure Network Watcher in the East US Azure region.

B. Add an Azure Network Watcher connection monitor.

C. Register the MicrosoftLogAnalytics provider.

D. Create an Azure Storage account. **Most Voted**

E. Register the Microsoft.Insights resource provider. **Most Voted**

F. Enable Azure Network Watcher flow logs. **Most Voted**

[Hide Solution](#)

[Discussion 41](#)

**Correct Answer:** AEF 

### Question #31

Topic 4

You need to deploy an Azure virtual machine scale set that contains five instances as quickly as possible.

What should you do?

A. Deploy five virtual machines. Modify the Availability Zones settings for each virtual machine.

B. Deploy five virtual machines. Modify the Size setting for each virtual machine.

C. Deploy one virtual machine scale set that is set to VM (virtual machines) orchestration mode.

D. Deploy one virtual machine scale set that is set to ScaleSetVM orchestration mode. **Most Voted**

[Hide Solution](#)

[Discussion 34](#)

**Correct Answer:** D 

**HOTSPOT -**

You have a pay-as-you-go Azure subscription that contains the virtual machines shown in the following table.

| Name | Resource group | Daily cost |
|------|----------------|------------|
| VM1  | RG1            | 20 euros   |
| VM2  | RG2            | 30 euros   |

You create the budget shown in the following exhibit.

**Budget1**

Resource group

 [Edit budget](#)  [Delete budget](#)**BUDGET SUMMARY**

|               |                      |
|---------------|----------------------|
| Name          | Budget1              |
| Scope         | RG1 (Resource group) |
| Filters       | -                    |
| Amount        | 1,000.00 EUR         |
| Budget period | Resets billing month |
| Start date    | 6/20/2019            |
| End date      | 6/19/2021            |

**BUDGET ALERTS**

| Alert conditions         | % OF BUDGET       | AMOUNT | ACTION GROUP | ACTION GROUP |
|--------------------------|-------------------|--------|--------------|--------------|
|                          | 50%               | €500   | AG1          | 1 Email      |
|                          | 70%               | €700   | AG2          | 1 SMS        |
|                          | 100%              | €1,000 | AG3          | 1 Azure app  |
| Alert recipients (email) | User1@Contoso.com |        |              |              |

The AG1 action group contains a user named admin@contoso.com only.

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

Hot Area:

### Answer Area

When the maximum amount in Budget1 is reached, [answer choice].

|   |
|---|
| VM1 and VM2 are turned off                  |
| VM1 and VM2 continue to run                 |
| VM1 is turned off, and VM2 continues to run |

Based on the current usage costs of the virtual machines, [answer choice].

|   |
|---|
| no email notifications will be sent each month    |
| one email notification will be sent each month    |
| two email notifications will be sent each month   |
| three email notifications will be sent each month |

Box 1: VM1 and VM2 continue to run

The Budget's scope is RG1, so only VM1 will be handled. When the budget thresholds you've created are exceeded, only notifications are triggered. When alert hits 100%, the action group is a Azure app, which I assume a Azure logic App. It is not clear what this app does. accordingly, we can assume no action to stop the VM as a spending limit. To stop resources, you need to setup additional things, none of which are mentioned in the question.

Box 2: one email notification will be sent each month.

Budget alerts have scope in Resource Group RG1, which includes VM1, but not VM2. VM1 consumes 20 Euro/day, so 20 euros \* 30 days = 600 euros. The 50%, 500 Euro limit, will be reached in 25 days ( $25 \times 20 = 500$ ), so an email will be sent. The 70% and 100% alert conditions will not be reached within a month, and they don't trigger email actions anyway, because AG1 action group contains a user.

Credit alerts: Credit alerts are generated automatically at 90% and at 100% of your Azure credit balance. Whenever an alert is generated, it's reflected in cost alerts and in the email sent to the account owners. 90% and 100% will not be reached though.

If you don't specify a particular action group, an email is sent to the alert recipients. so, as we have AG1 group already in place. Only single email will be sent.

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

| Name  | Role                       |
|-------|----------------------------|
| User1 | None                       |
| User2 | Global administrator       |
| User3 | Cloud device administrator |
| User4 | Intune administrator       |

Adatum.com has the following configurations:

- Users may join devices to Azure AD is set to User1.
- Additional local administrators on Azure AD joined devices is set to None.

You deploy Windows 10 to a computer named Computer1. User1 joins Computer1 to adatum.com.

You need to identify the local Administrator group membership on Computer1.

Which users are members of the local Administrators group?

- A. User1 only
- B. User2 only
- C. User1 and User2 only** Most Voted
- D. User1, User2, and User3 only
- E. User1, User2, User3, and User4

[Hide Solution](#)[Discussion 62](#)

Correct Answer: C 🎉

HOTSPOT -

You have Azure subscriptions named Subscription1 and Subscription2.

Subscription1 has following resource groups:

| Name | Region      | Lock type |
|------|-------------|-----------|
| RG1  | West Europe | None      |
| RG2  | West Europe | Read Only |

RG1 includes a web app named App1 in the West Europe location.

Subscription2 contains the following resource groups:

| Name | Region      | Lock type |
|------|-------------|-----------|
| RG3  | East Europe | Delete    |
| RG4  | Central US  | none      |

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

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

### Statements

### Yes

### No

App1 can be moved to RG2

App1 can be moved to RG3

App1 can be moved to RG4

Box 1: No -

RG2 is read only. ReadOnly means authorized users can read a resource, but they cannot delete or update the resource.

Box 2: Yes -

Box 3: Yes -

Note:

App Service resources are region-specific and cannot be moved directly across regions. You can move the App Service resource by creating a copy of your existing App Service resource in the target region, then move your content over to the new app. You can then delete the source app and App Service plan. To make copying your app easier, you can clone an individual App Service app into an App Service plan in another region.

Reference:

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

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/move-limitations/app-service-move-limitations>

HOTSPOT -

You have an Azure subscription named Subscription1 that contains the following resource group:

- Name: RG1
- Region: West US
- Tag: `tag1`: `value1`

You assign an Azure policy named Policy1 to Subscription1 by using the following configurations:

- Exclusions: None
- Policy definition: Append a tag and its value to resources
- Assignment name: Policy1
- Parameters:
- Tag name: tag2

Tag value: value2 -

After Policy1 is assigned, you create a storage account that has the following configuration:

- Name: storage1
- Location: West US
- Resource group: RG1
- Tags: `tag3`: `value3`

You need to identify which tags are assigned to each resource.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Tags assigned to RG1:

|                                       |
|---------------------------------------|
| "tag1": "value1" only                 |
| "tag2": "value2" only                 |
| "tag1": "value1" and "tag2": "value2" |

Tags assigned to storage1:

|  |
|--|
| "tag3": "value3" only                                    |
| "tag1": "value1" and "tag3": "value3" only               |
| "tag2": "value2" and "tag3": "value3" only               |
| "tag1": "value1", "tag2": "value2", and "tag3": "value3" |

You have an Azure Kubernetes Service (AKS) cluster named AKS1.

You need to configure cluster autoscaler for AKS1.

Which two tools should you use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. the kubectl command Most Voted

B. the az aks command Most Voted Most Voted

C. the Set-AzVm cmdlet

D. the Azure portal Most Voted

E. the Set-AzAks cmdlet

There are 2 things to understand:

a) Are we talking about pods?

b) Are we talking about nodes?

The question is regarding how to autoscale the AKS, so it means that we are talking about the nodes. As we are talking how to scale the nodes: a) az aks is necessary b) Then you scale the nodes in the portal.

**The correct answers are B & D.**

If we want to scale the pods, the options would be kubelet, but it is not the case. We are not talking about the containers, we are talking about the infrastructure behind this.

FYI also - the PowerShell command that can do this same task is "Set-AzAksCluster" (not Set-AzAks).  
B and D it is!

<https://docs.microsoft.com/en-us/azure/aks/cluster-autoscaler>

You create the following resources in an Azure subscription:

- An Azure Container Registry instance named Registry1
- An Azure Kubernetes Service (AKS) cluster named Cluster1

You create a container image named App1 on your administrative workstation.

You need to deploy App1 to Cluster1.

What should you do first?

A. Run the docker push command. Most Voted

B. Create an App Service plan.

C. Run the az acr build command.

D. Run the az aks create command.

Break down the question first:

1. You already have a container and an AKS cluster for your app - so no need to "create" these.
2. You have a container image named App1 already on your location machine, ready to be pushed" to your Azure container.
3. What do you need to do first?

Therefore the next thing to do is Push the container instant to your Azure Container registry using the Docker command (**answer A**)

<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-get-started-docker-cli?tabs=azure-cli#push-the-image-to-your-registry>

No need to create a App Service Plan (B) - Not required

No need to use az acr build (C) - Already created Azure Container Registry

No need to user az aks create (D) - Already created Azure AKS cluster

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

| Name       | Type                      | Resource group        | Location   |
|------------|---------------------------|-----------------------|------------|
| RG1        | Resource group            | <i>Not applicable</i> | Central US |
| RG2        | Resource group            | <i>Not applicable</i> | West US    |
| VMSS1      | Virtual machine scale set | RG2                   | West US    |
| Proximity1 | Proximity placement group | RG1                   | Central US |
| Proximity2 | Proximity placement group | RG2                   | West US    |
| Proximity3 | Proximity placement group | RG1                   | Central US |

You need to configure a proximity placement group for VMSS1.

Which proximity placement groups should you use?

- A. Proximity2 only Most Voted
- B. Proximity1, Proximity2, and Proximity3
- C. Proximity1 only
- D. Proximity1 and Proximity3 only

[Hide Solution](#)

[Discussion](#) 67

Correct Answer: A 🎉

Resource Group location of VMSS1 is the RG2 location, which is West US.

Only Proximity2, which also in RG2, is location in West US

Reference:

<https://azure.microsoft.com/en-us/blog/introducing-proximity-placement-groups/>

**Question #47***Topic 4*

You have an Azure subscription named Subscription1.  
You deploy a Linux virtual machine named VM1 to Subscription1.  
You need to monitor the metrics and the logs of VM1.  
What should you use?

- A. Azure HDInsight
- B. Linux Diagnostic Extension (LAD) 3.0** Most Voted
- C. the AzurePerformanceDiagnostics extension
- D. Azure Analysis Services

**Hide Solution****Discussion** 103**Correct Answer:** B 🎉

The Linux Diagnostic Extension should be used which downloads the Diagnostic Extension (LAD) agent on Linux server.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/diagnostics-linux>

*Community vote distribution***Question #49***Topic 4*

You plan to deploy three Azure virtual machines named VM1, VM2, and VM3. The virtual machines will host a web app named App1.  
You need to ensure that at least two virtual machines are available if a single Azure datacenter becomes unavailable.  
What should you deploy?

- A. all three virtual machines in a single Availability Zone
- B. all virtual machines in a single Availability Set
- C. each virtual machine in a separate Availability Zone** Most Voted
- D. each virtual machine in a separate Availability Set

**Hide Solution****Discussion** 109**Correct Answer:** C 🎉

Use availability zones to protect from datacenter level failures.

C is the correct answer - If you want Datacenter level high availability - VMs should be deployed in different zones.

Availability Set - Within Datacenter- configure update domains and fault domains Availability zone - Within region (usually three Datacenter per region).

You have an Azure virtual machine named VM1 that runs Windows Server 2019.  
You save VM1 as a template named Template1 to the Azure Resource Manager library.  
You plan to deploy a virtual machine named VM2 from Template1.  
What can you configure during the deployment of VM2?

- A. operating system
- B. administrator username
- C. virtual machine size
- D. resource group **Most Voted**

### Confirming RG.

Manual steps: log in, deploy VM1. Accept all defaults. Go to resource > template > save to library. View library > deploy template, It pre-populates the subscription but you have to set an RG. VM Name can be customized, admin user/pass are pulled from template.

You have an Azure subscription that contains an Azure virtual machine named VM1. VM1 runs a financial reporting app named App1 that does not support multiple active instances.

At the end of each month, CPU usage for VM1 peaks when App1 runs.

You need to create a scheduled runbook to increase the processor performance of VM1 at the end of each month.

What task should you include in the runbook?

- A. Add the Azure Performance Diagnostics agent to VM1.
- B. Modify the VM size property of VM1. **Most Voted**
- C. Add VM1 to a scale set.
- D. Increase the vCPU quota for the subscription.
- E. Add a Desired State Configuration (DSC) extension to VM1.

[Hide Solution](#)[Discussion](#)

139

**Correct Answer:** E 📦

Reference:

<https://docs.microsoft.com/en-us/azure/automation/automation-quickstart-dsc-configuration>

Community vote distribution

B (95%)

5%

**Correct Answer:** B

Here we need to modify the size of the VM to increase the number of vCPU's assigned to the VM. This can be included as a task in the runbook. The VM size property can be modified by a runbook that is triggered by metrics, but you can schedule it monthly.

Refer to <https://www.youtube.com/watch?v=pQ9dQ13B2vM>

You plan to deploy several Azure virtual machines that will run Windows Server 2019 in a virtual machine scale set by using an Azure Resource Manager template. You need to ensure that NGINX is available on all the virtual machines after they are deployed.

What should you use?

- A. Deployment Center in Azure App Service
- B. A Desired State Configuration (DSC) extension Most Voted
- C. the New-AzConfigurationAssignment cmdlet
- D. a Microsoft Intune device configuration profile

[Hide Solution](#)[Discussion 33](#)

Correct Answer: **B** 

**HOTSPOT -**

You deploy an Azure Kubernetes Service (AKS) cluster that has the network profile shown in the following exhibit.

**Network profile**

|                    |                |
|--------------------|----------------|
| Type (plugin)      | Basic (Kubnet) |
| Pod CIDR           | 10.244.0.0/16  |
| Service CIDR       | 10.0.0.0/16    |
| DNS service IP     | 10.0.0.10      |
| Docker bridge CIDR | 172.17.0.1/16  |

**Network options**

HTTP application routing

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

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Containers will be assigned an IP address in the [answer choice] subnet.

|               |
|---------------|
| ▼             |
| 10.244.0.0/16 |
| 10.0.0.0/16   |
| 172.17.0.1/16 |

Services in the AKS cluster will be assigned an IP address in the [answer choice] subnet.

|               |
|---------------|
| ▼             |
| 10.244.0.0/16 |
| 10.0.0.0/16   |
| 172.17.0.1/16 |

Correct Answer:

Box 1: 10.244.0.0/16 The Pod CIDR, because containers live inside Pods.

Note: You can't change this address range once the cluster is deployed, if you need more addresses for additional nodes.

Box 2: 10.0.0.0/16

The Service CIDR is used to assign internal services in the AKS cluster an IP address.

Reference: <https://docs.microsoft.com/en-us/azure/aks/configure-kubenet>

<https://docs.microsoft.com/en-us/azure/aks/configure-azure-cni#plan-ip-addressing-for-your-cluster>

Question #54

Topic 4

HOTSPOT -

You have the App Service plan shown in the following exhibit.

The screenshot shows the 'Default' scale condition configuration in the Azure portal. It includes:

- Delete warning:** A note stating "The very last or default recurrence rule cannot be deleted. Instead, you can disable autoscale to turn off autoscale".
- Scale mode:** Set to "Scale based on a metric" (radio button selected).
- Rules:**
  - Scale out:** When "homepage" and "(Maximum) CpuPercentage > 85", Increase count by 1.
  - Scale in:** When "homepage" and "(Average) CpuPercentage < 30", Decrease count by 1.
- + Add a rule:** Link to add more rules.
- Instance limits:** Minimum set to 1, Maximum set to 5, Default set to 1.
- Schedule:** A note: "This scale condition is executed when none of the other scale condition(s) match".

The scale-in settings for the App Service plan are configured as shown in the following exhibit.

|                                  |   |
|----------------------------------|---|
| <b>Operator *</b>                | <b>Metric threshold to trigger scale action *</b> ⓘ |
| Less than                        | 30 %  |
| <b>Duration (in minutes) *</b> ⓘ |   |
| 5 ✓                              |   |
| <b>Time grain (in mins) *</b> ⓘ  | <b>Time grain statistic *</b> ⓘ                     |
| 1                                | Average ✓   |
| <b>Action</b>                    |   |
| <b>Operation *</b>               |   |
| Decrease count by                |   |
| <b>Instance count *</b>          | <b>Cool down (minutes) *</b> ⓘ                      |
| 1 ✓                              | 5   |

The scale out rule is configured with the same duration and cool down tile as the scale in rule.

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

NOTE: Each correct selection is worth one point.

Hot Area:

If after deployment CPU usage is 70 percent for one hour and then reaches 90 percent for five minutes, at that time the total number of instances will be [answer choice].

|   |
|---|
| 1 |
| 2 |
| 3 |
| 4 |
| 5 |

If after deployment the CPU maintains constant usage of 90 percent for one hour, and then the average CPU usage is below 25 percent for nine minutes, at that point the number of instances will be [answer choice].

|   |
|---|
| 1 |
| 2 |
| 3 |
| 4 |
| 5 |

## Box 1: 2

70% for 1h, and then 90% for 5 minutes. So, from the default of 1 it will scale out 1 more. So, 2 in total.

## Box 2: 4

90% for 1h and then 25% for 9minutes. So, from the default of 1 it will scale out to the max 5 ( $60/5 = 12$ , which means 6 times scale out, because we have 5 minutes period of cool down). Then when it drops to 25% for 9 minutes and it will scale in once after 5 mins (since the average of the last 5 minutes is under 30%), so it will decrease by 1, so 4 in total. Then it will have a cooldown of 5 minutes before scaling in again, but since only 4 minutes left from 9 minutes ( $9-5 = 4$ ), it won't scale in again. So, 4 in total.

### Question #55

### Topic 4

You have an Azure virtual machine named VM1 that runs Windows Server 2019. The VM was deployed using default drive settings.

You sign in to VM1 as a user named User1 and perform the following actions:

- Create files on drive C.
- Create files on drive D.
- Modify the screen saver timeout.
- Change the desktop background.

You plan to redeploy VM1.

Which changes will be lost after you redeploy VM1?

- A. the modified screen saver timeout
- B. the new desktop background
- C. the new files on drive D Most Voted**
- D. the new files on drive C

[Hide Solution](#)

[Discussion 31](#)

**Correct Answer:** C 🎉

*Community vote distribution*

C (100%)

Correct Answer: C

For Windows Server, the temporary disk is mounted as "D:\\".

For Linux based VM's the temporary disk is mounted as "/dev/sdb1".

<https://www.cloudelicious.net/azure-vms-and-their-temporary-storage>

**HOTSPOT -**

You have an Azure subscription that contains a virtual machine scale set. The scale set contains four instances that have the following configurations:

- Operating system: Windows Server 2016
- Size: Standard\_D1\_v2

You run the get-azvmss cmdlet as shown in the following exhibit:

```
PS Azure:> (Get-AzVmss -Name WebProd -ResourceGroupName RG1).VirtualMachineProfile.OsProfile.WindowsConfiguration  
  
ProvisionVMAgent      : True  
EnableAutomaticUpdates : False  
TimeZone               :  
AdditionalUnattendContent :  
WinRM                 :  
  
Azure:/  
PS Azure:> Get-AzVmss -Name WebProd -ResourceGroupName RG1 | Select -ExpandProperty UpgradePolicy  
  
Mode RollingUpgradePolicy  AutomaticOSUpgradePolicy  
-----  
Automatic              Microsoft.Azure.Management.Compute.Models.AutomaticOSUpgradePolicy  
  
Azure:/  
PS Azure:> []
```

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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

When an administrator changes the virtual machine size, the size will be changed on up to [answer choice] virtual machines simultaneously.

|   |
|---|
| 0 |
| 1 |
| 2 |
| 4 |

When a new build of the Windows Server 2016 image is released, the new build will be deployed to up to [answer choice] virtual machines simultaneously.

|   |
|---|
| 0 |
| 1 |
| 2 |
| 4 |

Correct Answer:

Box 1: 4

If you resize the Scale Set all the VMs get resized at once, thus 4 is the correct answer. The first command has nothing to do with VM Resizing.

Box 2: 1

What's set to 'false' is Patch updates. This is recommended to be set to 'False' when Automatic OS upgrades are set to 'True'. What this means is that the automatic rolling OS Upgrades will happen at 20%.

Question #60

Topic 4

HOTSPOT -

You have an Azure subscription named Subscription1. Subscription1 contains two Azure virtual machines VM1 and VM2. VM1 and VM2 run Windows Server 2016.

VM1 is backed up daily by Azure Backup without using the Azure Backup agent.

VM1 is affected by ransomware that encrypts data.

You need to restore the latest backup of VM1.

To which location can you restore the backup? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

You can perform a file recovery of VM1 to:

|   |
|---|
| VM1 only  |
| VM1 or a new Azure virtual machine only             |
| VM1 and VM2 only                                    |
| A new Azure virtual machine only                    |
| Any Windows computer that has Internet connectivity |

You can restore VM1 to:

|   |
|---|
| VM1 only  |
| VM1 or a new Azure virtual machine only             |
| VM1 and VM2 only                                    |
| Any Windows computer that has Internet connectivity |

Correct Answer:

Box 1: VM1 and VM2 only as an answer.

For files recovery, you download and run a windows executable to map a network drive. It can only run when the OS meets the requirements. Any computer running Windows Server 2016 or Windows 10 is suitable. File recovery can be done from any machine on the Internet. Note: There might be compatibility issues with any Windows computer, so consider VM1 and VM2 only as an answer.

## Box 2: VM1 or a new Azure virtual machine only

For restoring a VM, you can choose 'Create new' or 'Replace existing'.

Question #63

Topic 4

HOTSPOT -

You have an Azure subscription.

You plan to use Azure Resource Manager templates to deploy 50 Azure virtual machines that will be part of the same availability set. You need to ensure that as many virtual machines as possible are available if the fabric fails or during servicing. How should you configure the template? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

```
{  
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",  
  "contentVersion": "1.0.0.0",  
  "parameters": {},  
  "resources": [  
    {  
      "type": "Microsoft.Compute/availabilitySets",  
      "name": "ha",  
      "apiVersion": "2017-12-01",  
      "location": "eastus",  
      "properties": {  
        "platformFaultDomainCount":   
        ,  
        "platformUpdateDomainCount":   
      }  
    }  
  ]  
}
```

### Box 1: 3

2 or 3 is max, depending on which region you are in. platformFaultDomainCount should be 3 (since its in East US)

### Box 2: 20

Use 20 for platformUpdateDomainCount. UpdateDomains are max up to 20 Domains only,

**HOTSPOT -**

You have an Azure subscription.

You deploy a virtual machine scale set that is configured as shown in the following exhibit.

## Create a virtual machine scale set

Basics Disks Networking Scaling Management Health Advanced

An Azure virtual machine scale set can automatically increase or decrease the number of VM instances that run your application. This automated and elastic behavior reduces the management overhead to monitor and optimize the performance of your application. [Learn more about VMSS scaling](#)

### Instance

Initial instance count \*

### Scaling

Scaling policy  Manual  Custom

Minimum number of VMs \*

Maximum number of VMs \*

### Scale out

CPU threshold (%) \*

Duration in minutes \*

Number of VMs to increase by \*

### Scale in

CPU threshold (%) \*

Number of VMs to decrease by \*

### Diagnostic logs

Collect diagnostic logs from Autoscale   Disabled  Enabled

### Scale-In policy

Configure the order in which virtual machines are selected for deletion during a scale-in operation.  
[Learn more about scale-in policies](#).

### Scale-in policy

Default - balance across availability zones and fault domains, then delete V...

Use the drop-down menus to select the answer choice that answers each question based on the information presented in the graphic

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

At 9:00 AM, the scale set starts and CPU utilization is 90 percent for 15 minutes. How many virtual machine instances will be running at 9:15 AM?

|   |   |
|---|---|
|   | ▼ |
| 2 |   |
| 3 |   |
| 4 |   |
| 5 |   |

At 10:00 AM, the scale set has five virtual machine instances running and CPU utilization falls to less than 15 percent for 60 minutes. How many virtual machine instances will be running at 11:00 AM?

|   |   |
|---|---|
|   | ▼ |
| 1 |   |
| 2 |   |
| 3 |   |
| 4 |   |

You have web apps in the West US, Central US and East US Azure regions.

You have the App Service plans shown in the following table.

| Name | Operating system | Location   | SKU and size    |
|------|------------------|------------|-----------------|
| ASP1 | Windows          | West US    | Standard S1     |
| ASP2 | Linux            | Central US | Premium V2 P1v2 |
| ASP3 | Linux            | East US    | Premium V2 P1v2 |
| ASP4 | Linux            | East US    | Premium V2 P1v2 |

You plan to create an additional App Service plan named ASP5 that will use the Linux operating system.

You need to identify in which of the currently used locations you can deploy ASP5.

What should you recommend?

- A. West US, Central US, or East US Most Voted
- B. Central US only
- C. East US only
- D. West US only

[Hide Solution](#)

[Discussion 32](#)

**Correct Answer:** A 

An App service plan could be any of the regions mentioned, if it was just the deploying the App based on the required OS then it could be streamlined to the OS+region.so A makes sense

You plan to deploy several Azure virtual machines that will run Windows Server 2019 in a virtual machine scale set by using an Azure Resource Manager template. You need to ensure that NGINX is available on all the virtual machines after they are deployed. What should you use?

- A. the New-AzConfigurationAssignment cmdlet
- B. a Desired State Configuration (DSC) extension**
- C. Azure Active Directory (Azure AD) Application Proxy
- D. Azure Application Insights

**Hide Solution****Discussion 7****Correct Answer:** B 🎉

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-overview>*Community vote distribution***B (100%)****HOTSPOT -**

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

| Name                                 | Type             |
|--------------------------------------|------------------|
| ManagementGroup1                     | Management group |
| RG1                                  | Resource group   |
| 9c8bc1cd-7655-4c66-b3ea-a8ee101d8f75 | Subscription ID  |
| Tag1                                 | Tag              |

In Azure Cloud Shell, you need to create a virtual machine by using an Azure Resource Manager (ARM) template. How should you complete the command? To answer, select the appropriate options in the answer area.

Hot Area:

```
$adminPassword = Read-Host -Prompt "Enter the administrator password" -AsSecureString
```

|                               |  |
|-------------------------------|--|
| New-AzVm                      | -Tag Tag1 '  |
| New-AzResource                | -ResourceGroupName RG1 '                           |
| New-AzTemplateSpec            | -GroupName ManagementGroup1 '                      |
| New-AzResourceGroupDeployment | -Subscription 9c8bc1cd-7655-4c66-b3ea-a8ee101d8f75 |

- TemplateUri "https://raw.githubusercontent.com/Azure/azure-quickstart-templates/master/101-vm-simple-windows/azuredploy.json" '  
- adminUsername LocalAdministrator -adminPassword \$adminPassword -dnsLabelPrefix ContosoVM1

Box 1: New-AzResourceGroupDeployment. This cmdlet allows you to use a custom ARM template file to deploy resources to a resource group.

Box 2: -ResourceGroupName RG1. It's one of parameters of New-AzResourceGroupDeployment to specify to which resource group you want to deploy resources.

#### Question #69

#### Topic 4

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 questions sets might have more than one correct solution, while others might not have a correct solution.

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

You deploy an Azure Kubernetes Service (AKS) cluster named AKS1.

You need to deploy a YAML file to AKS1.

Solution: From Azure Cloud Shell, you run az aks.

Does this meet the goal?

A. Yes

B. No

[Hide Solution](#)

[Discussion](#) 6

**Correct Answer:** B 🏆

To deploy a YAML file, the command is:

kubectl apply -f <file\_name>.yaml

Reference:

<https://docs.microsoft.com/en-us/azure/aks/kubernetes-walkthrough>

*Community vote distribution*

B (100%)

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

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

You have an Azure virtual machine named VM1 that runs Windows Server 2016.

You need to create an alert in Azure when more than two error events are logged to the System event log on VM1 within an hour.

Solution: You create an Azure Log Analytics workspace and configure the data settings. You add the Microsoft Monitoring Agent VM extension to VM1. You create an alert in Azure Monitor and specify the Log Analytics workspace as the source.

Does this meet the goal?

A. Yes

B. No **Most Voted**

[Hide Solution](#)

[Discussion](#) 80

**Correct Answer:** B 🎉

You must install the Microsoft Monitoring Agent on VM1, and not the Microsoft Monitoring Agent VM extension.

Reference:

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

*Community vote distribution*

B (83%)

A (17%)

You Install the Microsoft Monitoring Agent VM agent to VM1 > This is Correct

1. Log analytics agent - Install in VM.
2. Log analytics workspace - collect the log files from Log Analytics Agent.
3. Azure Monitor - Create alert based on logs read from Log Analytics Workspace.

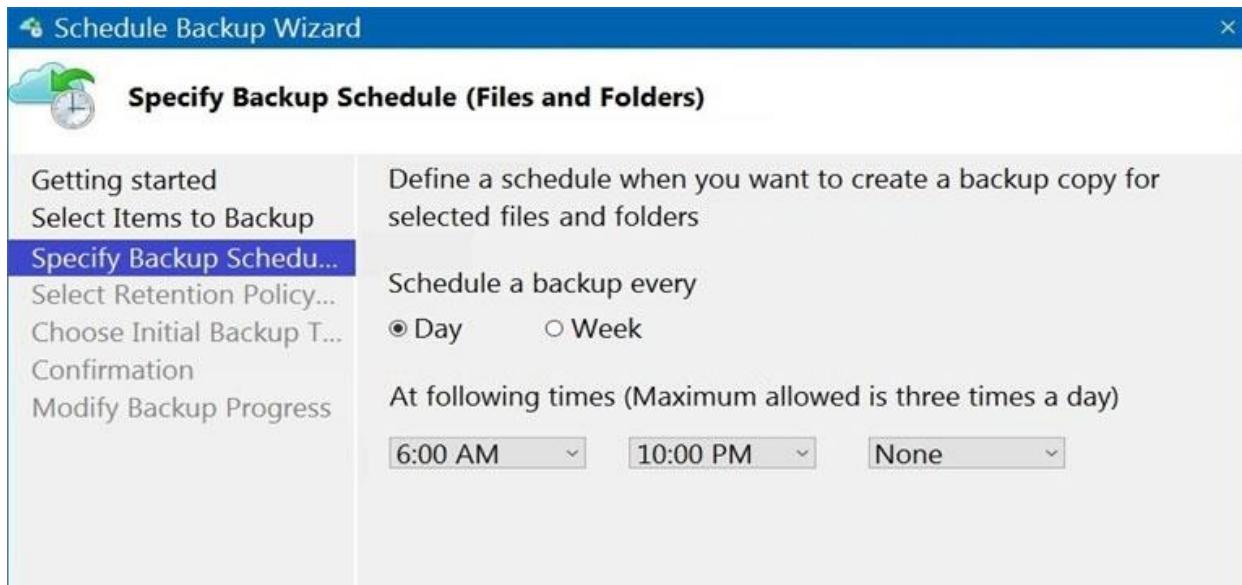
The Azure Monitor Agent is implemented as an Azure VM extension. The question is about MMA (microsoft monitoring agent) which is the legacy agent which needs to be installed on the VM.

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

| Name   | Type                    | Resource group | Location |
|--------|-------------------------|----------------|----------|
| Vault1 | Recovery services vault | RG1            | East US  |
| VM1    | Virtual machine         | RG1            | East US  |
| VM2    | Virtual machine         | RG1            | West US  |

All virtual machines run Windows Server 2016.

On VM1, you back up a folder named Folder1 as shown in the following exhibit.



You plan to restore the backup to a different virtual machine.

You need to restore the backup to VM2.

What should you do first?

- A. From VM1, install the Windows Server Backup feature.
- B. From VM2, install the Microsoft Azure Recovery Services Agent. Most Voted
- C. From VM1, install the Microsoft Azure Recovery Services Agent.
- D. From VM2, install the Windows Server Backup feature.

[Hide Solution](#)

[Discussion 11](#)

Correct Answer: B

**HOTSPOT -**

You have an Azure subscription.

You need to use an Azure Resource Manager (ARM) template to create a virtual machine that will have multiple data disks.

How should you complete the template? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

```
{  
  "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",  
  "parameters": {  
    "numberOfDataDisks": {  
      "type": "int",  
      "metadata": {  
        "description": "The number of dataDisks to create."  
      }  
    },  
    ...  
  },  
  "resources": [  
    {  
      "type": "Microsoft.Compute/virtualMachines",  
      "apiVersion": "2017-03-30",  
      ...  
      "properties": {  
        "storageProfile": {  
          ...  


|                |   |
|----------------|---|
| "copy": [      | ▼ |
| "copyIndex": [ |   |
| "dependsOn": [ |   |

  
          { "name": "dataDisks",  
            "count": "[parameters('numberOfDataDisks')]",  
            "input": {  
              "diskSizeGB": 1023,  
              "lun": 

|             |   |
|-------------|---|
| "[copy      | ▼ |
| "[copyIndex |   |
| "[dependsOn |   |

  
              "createOption": "Empty"  
            }  
          }  
        }  
      }  
    }  
  ]  
}
```

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

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

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

| Name  | Type            | Location     | Resource group        |
|-------|-----------------|--------------|-----------------------|
| RG1   | Resource group  | East US      | <i>Not applicable</i> |
| RG2   | Resource group  | West Europe  | <i>Not applicable</i> |
| RG3   | Resource group  | North Europe | <i>Not applicable</i> |
| VNET1 | Virtual network | Central US   | RG1                   |
| VM1   | Virtual machine | West US      | RG2                   |

Subscription1 also includes a virtual network named VNET2. VM1 connects to a virtual network named VNET2 by using a network interface named NIC1.

You need to create a new network interface named NIC2 for VM1.

Solution: You create NIC2 in RG1 and West US.

Does this meet the goal?

A. Yes

B. No

[Hide Solution](#)

[Discussion 10](#)

**Correct Answer:** A 

The virtual machine you attach a network interface to and the virtual network you connect it to must exist in the same location, here West US, also referred to as a region.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface>

*Community vote distribution*

A (100%)

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

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

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

| Name  | Type            | Location     | Resource group        |
|-------|-----------------|--------------|-----------------------|
| RG1   | Resource group  | East US      | <i>Not applicable</i> |
| RG2   | Resource group  | West Europe  | <i>Not applicable</i> |
| RG3   | Resource group  | North Europe | <i>Not applicable</i> |
| VNET1 | Virtual network | Central US   | RG1                   |
| VM1   | Virtual machine | West US      | RG2                   |

Subscription1 also includes a virtual network named VNET2. VM1 connects to a virtual network named VNET2 by using a network interface named NIC1.

You need to create a new network interface named NIC2 for VM1.

Solution: You create NIC2 in RG2 and Central US.

Does this meet the goal?

A. Yes

B. No

[Hide Solution](#)

[Discussion 3](#)

Correct Answer: **B** 

The virtual machine you attach a network interface to and the virtual network you connect it to must exist in the same location, here West US, also referred to as a region.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface>

Community vote distribution

**B (100%)**

You develop the following Azure Resource Manager (ARM) template to create a resource group and deploy an Azure Storage account to the resource group.

```
{  
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",  
    "contentVersion": "1.0.0.0",  
    "resources": [  
        {  
            "type": "Microsoft.Resources/resourceGroups",  
            "apiVersion": "2018-05-01",  
            "location": "eastus",  
            "name": "RG1"  
        },  
        {  
            "type": "Microsoft.Resources/deployments",  
            "apiVersion": "2017-05-10",  
            "name": "storageDeployment",  
            "resourceGroup": "RG1",  
            "dependsOn": [  
                "[resourceId('Microsoft.Resources/resourceGroups/', 'RG1')]"  
            ],  
            "properties": {  
                "mode": "Incremental",  
                "template": {  
                    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",  
                    "contentVersion": "1.0.0.0",  
                    "resources": [  
                        {  
                            "type": "Microsoft.Storage/storageAccounts",  
                            "apiVersion": "2017-10-01",  
                            "name": "storage1",  
                            "location": "eastus",  
                            "kind": "StorageV2",  
                            "sku": {  
                                "name": "Standard_LRS"  
                            }  
                        }  
                    ]  
                }  
            }  
        }  
    ]  
}
```

Which cmdlet should you run to deploy the template?

- A. New-AzResource
- B. New-AzResourceGroupDeployment Most Voted
- C. New-AzTenantDeployment
- D. New-AzDeployment Most Voted

D is correct here.

We are creating RG and storage acc. in this RG.

By using New-AzResourceGroupDeployment command -> "Adds an Azure deployment to a resource group."

#### Question #78

#### Topic 4

HOTSPOT -

You have an Azure App Service app named WebApp1 that contains two folders named Folder1 and Folder2. You need to configure a daily backup of WebApp1. The solution must ensure that Folder2 is excluded from the backup.

What should you create first, and what should you use to exclude Folder2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

#### Answer Area

First create:

- An Azure Storage account
- A Backup vault
- A Recovery Services vault
- A resource group

To exclude Folder2, use:

- A \_backup.filter file
- A backup policy
- A lock
- A WebJob

You plan to deploy several Azure virtual machines that will run Windows Server 2019 in a virtual machine scale set by using an Azure Resource Manager template. You need to ensure that NGINX is available on all the virtual machines after they are deployed. What should you use?

- A. the Publish-AzVMDscConfiguration cmdlet
- B. Azure Application Insights
- C. Azure Custom Script Extension **Most Voted**
- D. a Microsoft Endpoint Manager device configuration profile

[Hide Solution](#)[Discussion 9](#)**Correct Answer:** C 📦

Use Azure Resource Manager templates to install applications into virtual machine scale sets with the Custom Script Extension.

Note: The Custom Script Extension downloads and executes scripts on Azure VMs. This extension is useful for post deployment configuration, software installation, or any other configuration / management task.

To see the Custom Script Extension in action, create a scale set that installs the NGINX web server and outputs the hostname of the scale set VM instance.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/tutorial-install-apps-template>

*Community vote distribution*

C (91%)

9%

You have an Azure subscription. The subscription contains a virtual machine that runs Windows 10. You need to join the virtual machine to an Active Directory domain.

How should you complete the Azure Resource Manager (ARM) template? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

{

```
"apiVersion": "2017-03-30",
"type": "Microsoft.Compute/VirtualMachines",
"Properties": [
    "Extensions",
    "Microsoft.Compute/virtualMachines",
    "Microsoft.Compute/virtualMachines/extensions",
    "name": "[concat(parameters('VName'), '/joindomain')]",
    "location": "[parameter('location')]",
    "properties": {
        "publisher": "Microsoft.Compute",
        "type": "JsonADDomainExtension",
        "typeHandlerVersion": "1.3",
        "autoUpgradeMinorVersion": true,
        "settings": {
            "Name": "[parameters('domainName')]",
            "User": "[parameters('domainusername')]",
            "Restart": "true",
            "Options": "3"
        }
    },
    "ProtectedSettings": {
        "Settings": {},
        "Statuses": {}
    }
]
"Password": "[parameters('domainPassword')]"
}
```

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

| Name       | Type                      | Resource group        | Location   |
|------------|---------------------------|-----------------------|------------|
| RG1        | Resource group            | <i>Not applicable</i> | Central US |
| RG2        | Resource group            | <i>Not applicable</i> | West US    |
| VMSS1      | Virtual machine scale set | RG2                   | West US    |
| Proximity1 | Proximity placement group | RG1                   | West US    |
| Proximity2 | Proximity placement group | RG2                   | Central US |
| Proximity3 | Proximity placement group | RG1                   | Central US |

You need to configure a proximity placement group for VMSS1.

Which proximity placement groups should you use?

- A. Proximity2 only
- B. Proximity1, Proximity2, and Proximity3
- C. Proximity1 only **Most Voted**
- D. Proximity1 and Proximity3 only

[Hide Solution](#)[Discussion 8](#)

**Correct Answer:** C 🎉

Resource Group location of VMSS1 is the RG2 location, which is West US.

Only Proximity1, which also in RG2, is located in West US

Note: When you assign your virtual machines to a proximity placement group, the virtual machines are placed in the same data center, resulting in lower and deterministic latency for your applications.

Reference:

<https://azure.microsoft.com/en-us/blog/introducing-proximity-placement-groups/>

*Community vote distribution*

C (100%)

You are creating an Azure Kubernetes Services (AKS) cluster as shown in the following exhibit.

## Create Kubernetes cluster

Validation passed

### Basics

|                         |                                 |
|-------------------------|---------------------------------|
| Subscription            | Visual Studio Premium with MSDN |
| Resource group          | RG1                             |
| Region                  | West Europe                     |
| Kubernetes cluster name | AKS1                            |
| Kubernetes version      | 1.20.9                          |

### Node pools

|                                   |          |
|-----------------------------------|----------|
| Node pools                        | 1        |
| Enable virtual nodes              | Disabled |
| Enable virtual machine scale sets | Enabled  |

### Authentication

|                                    |  |
|------------------------------------|--|
| Authentication method              | Service principal  |
| Role-based access control (RBAC)   | Enabled  |
| AKS-managed Azure Active Directory | Disabled   |
| Encryption type                    | (Default) Encryption at-rest with a platform-managed key |

### Networking

|                          |          |
|--------------------------|----------|
| Network configuration    | Kubenet  |
| DNS name prefix          | AKS1-dns |
| Load balancer            | Standard |
| Private cluster          | Disabled |
| Authorized IP ranges     | Disabled |
| Network policy           | None     |
| HTTP application routing | No       |

[Create](#)

[< Previous](#)

[Next >](#)

[Download a template for automation](#)

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

### Answer Area

To ensure that you can create Windows containers in AKS1, you must [answer choice].

|  |
|--|
| enable virtual nodes                     |
| increase the number of node pools        |
| modify the Kubernetes version setting    |
| modify the Network configuration setting |

To ensure that you can integrate AKS1 with an Azure container registry, you must modify the [answer choice] setting.

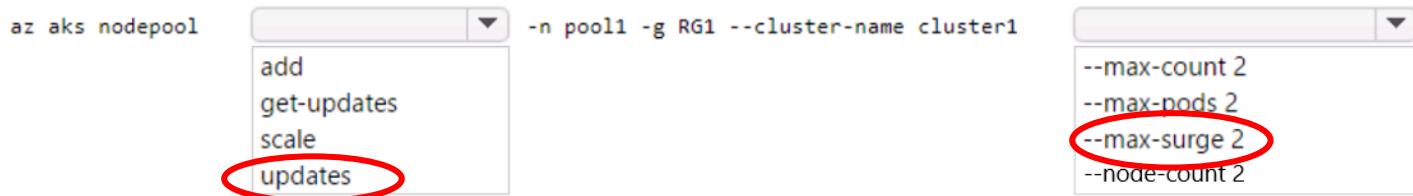
|                                    |
|------------------------------------|
| AKS-managed Azure Active Directory |
| Authentication method              |
| Authorized IP ranges               |
| Kubernetes version                 |
| Network configuration              |

You have an Azure subscription that contains an Azure Kubernetes Service (AKS) cluster named Cluster1. Cluster1 hosts a node pool named Pool1 that has four nodes.

You need to perform a coordinated upgrade of Cluster1. The solution must meet the following requirements:

- Deploy two new nodes to perform the upgrade.
- Minimize costs.

How should you complete the command? To answer, select the appropriate options in the answer area.



I assume there is a typo, where it says "updates" it should be "update".

az aks nodepool \*\*update\*\* -n pool1 -g RG1 --cluster-name cluster1 \*\*max-surge 2\*\*

<https://learn.microsoft.com/en-us/cli/azure/aks/nodepool?view=azure-cli-latest>

We want to edit an existing node pool, so we cannot use "add":

We want to update the properties of the node pool, so we need to use: az aks nodepool update

We want to set it up to use more nodes during an update, so this one is right: --max-surge

You have an Azure subscription.

You create the following file named Deploy.json.

```
{  
  "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",  
  "contentVersion": "1.0.0.0",  
  "parameters": {  
    "location": {  
      "type": "string",  
      "defaultValue": "westus"  
    }  
  },  
  "resources": [  
    {  
      "apiVersion": "2019-04-01",  
      "type": "Microsoft.Storage/storageAccounts",  
      "name": "[concat(copyIndex(),'storage', uniqueString(resourceGroup().id))]",  
      "location": "[resourceGroup().location]",  
      "sku": {  
        "name": "Premium_LRS"  
      },  
      "kind": "StorageV2",  
      "properties": {},  
      "copy": {  
        "name": "storagecopy",  
        "count": 3  
      }  
    }  
  ]  
}
```

You connect to the subscription and run the following commands.

```
New-AzResourceGroup -Name RG1 -Location "centralus"  
New-AzResourceGroupDeployment -ResourceGroupName RG1 -TemplateFile "deploy.json"
```

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

### Answer Area

| Statements   | Yes                              | No                               |
|--|----------------------------------|----------------------------------|
| The commands will create four new resources.                           | <input checked="" type="radio"/> | <input type="radio"/>            |
| The commands will create storage accounts in the West US Azure region. | <input type="radio"/>            | <input checked="" type="radio"/> |
| The first storage account that is created will have a prefix of 0.     | <input checked="" type="radio"/> | <input type="radio"/>            |

Answers: Yes / No / Yes

Y: The 4 resources created are the RG1 resource group + the 3 storage accounts

N: the location of the storage accounts is defined by the parameter "location" in the "resources" item that has the value of the Resource Group (stated by the "resourceGroup().location" function that returns the location of the resource group RG1 which is in Central US)

Y: the names of the storage accounts have the prefix given by the copyIndex() function in "name": "[concat(copyIndex(),'storage',uniqueString(resourceGroup().id))]", which starts at the position 0

You plan to deploy several Azure virtual machines that will run Windows Server 2019 in a virtual machine scale set by using an Azure Resource Manager template.

You need to ensure that NGINX is available on all the virtual machines after they are deployed.

What should you use?

- A. Azure Custom Script Extension
- B. Deployment Center in Azure App Service
- C. the Publish-AzVMDscConfiguration cmdlet
- D. the New-AzConfigurationAssignment cmdlet

[Hide Solution](#)



[Discussion](#)

5

**Correct Answer:** A 

*Community vote distribution*

A (100%)

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

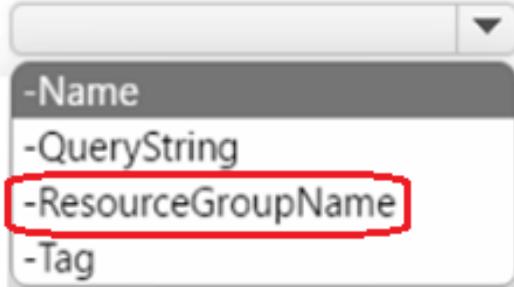
You plan to use an Azure Resource Manager (ARM) template named template1 to deploy resources. The solution must meet the following requirements:

- Deploy new resources to RG1.
- Remove all the existing resources from RG1 before deploying the new resources.

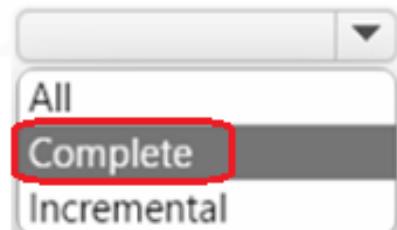
How should you complete the command? To answer, select the appropriate options in the answer area.

```
New-AzResourceGroupDeployment -TemplateUri  
"https://contoso.com/template1" -TemplateParameterfile
```

params.json



RG1 -Mode



Answer is correct.

"In complete mode, Resource Manager deletes resources that exist in the resource group but are not specified in the template."

<https://learn.microsoft.com/en-us/powershell/module/az.resources/new-azresourcegroupdeployment?view=azps-9.2.0#-mode>

You have an Azure App Service web app named app1.

You configure autoscaling as shown in following exhibit.

The screenshot shows the 'Default' scale condition for an Azure App Service. It includes sections for 'Delete warning', 'Scale mode' (set to 'Scale based on a metric'), 'Rules' (with a note about having at least one rule), 'Scale out' (when Average CpuPercentage > 70, increase count by 1), 'Instance limits' (minimum 1, maximum 5, default 1), and a 'Schedule' section stating 'This scale condition is executed when none of the other scale condition(s) match'.

**Default\*** Auto created scale condition

Delete warning The very last or default recurrence rule cannot be deleted. Instead, you can disable autoscale to turn off autoscale.

Scale mode

Rules It is recommended to have at least one scale in rule. To create new rules, click [Add a rule](#).

Scale out

When [\(Average\) CpuPercentage > 70](#) Increase count by 1

+ Add a rule

Instance limits

|         |         |         |
|---------|---------|---------|
| Minimum | Maximum | Default |
| 1       | 5       | 1       |

Schedule **This scale condition is executed when none of the other scale condition(s) match**

You configure the autoscale rule criteria as shown in the following exhibit.

### Criteria

Time aggregation \*

Maximum

Metric namespace \*

App Service plans standard metrics

Metric name

CPU Percentage

1 minute time grain

Dimension Name

Operator

Dimension Values

Add

Instance

=

All values



If you select multiple values for a dimension, autoscale will aggregate the metric across the selected values, not evaluate the metric for each values individually.



CpuPercentage (Maximum)

1.67 %

Enable metric divide by instance count

Operator \*

Metric threshold to trigger scale action \*

Greater than

70

%

Duration (minutes) \*

10

Time grain (minutes)

Time grain statistic \*

1

Average

### Action

Operation \*

Cool down (minutes) \*

Increase count by

5

Instance count \*

1

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

After CPU usage has reached 80 percent for 15 minutes, [answer choice] will be running.

▼

|             |
|-------------|
| 1 instance  |
| 2 instances |
| 3 instances |
| 4 instances |
| 5 instances |

Once the first scale-out instance is created, the minimum time before an additional instance is created will be [answer choice].

▼

|            |
|------------|
| 1 minute   |
| 5 minutes  |
| 10 minutes |
| 15 minutes |

2, 15

Initial instance is 1 as specified in first figure. 80% for 15 minutes reaches 10 minutes duration, but haven't reached second turn of scale out, so only one new instance is created.

Since cool down time is 5 minutes, which means after one scale happens, it will count 5 minutes before counting a new 10 minutes, so 15 minutes total.

## Topic 5 - Question Set 5

### Question #1

Topic 5

HOTSPOT -

You have an Azure subscription named Sub1.

You plan to deploy a multi-tiered application that will contain the tiers shown in the following table.

| Tier                          | Accessible from the Internet | Number of virtual machines |
|-------------------------------|------------------------------|----------------------------|
| Front-end web server          | Yes                          | 10                         |
| Business logic                | No                           | 100                        |
| Microsoft SQL Server database | No                           | 5                          |

You need to recommend a networking solution to meet the following requirements:

- Ensure that communication between the web servers and the business logic tier spreads equally across the virtual machines.
- Protect the web servers from SQL injection attacks.

Which Azure resource should you recommend for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Ensure that communication between the web servers and the business logic tier spreads equally across the virtual machines:

|  |
|--|
| an application gateway that uses the Standard tier |
| an application gateway that uses the WAF tier      |
| an internal load balancer                          |
| a network security group (NSG)                     |
| a public load balancer                             |

Protect the web servers from SQL injection attacks:

|  |
|--|
| an application gateway that uses the Standard tier |
| an application gateway that uses the WAF tier      |
| an internal load balancer                          |
| a network security group (NSG)                     |
| a public load balancer                             |

Your company has three offices. The offices are located in Miami, Los Angeles, and New York. Each office contains datacenter.

You have an Azure subscription that contains resources in the East US and West US Azure regions. Each region contains a virtual network. The virtual networks are peered.

You need to connect the datacenters to the subscription. The solution must minimize network latency between the datacenters.

What should you create?

- A. three Azure Application Gateways and one On-premises data gateway
- B. three virtual hubs and one virtual WAN **Most Voted**
- C. three virtual WANs and one virtual hub
- D. three On-premises data gateways and one Azure Application Gateway

B is correct.

**Hub:** A virtual hub is a Microsoft-managed virtual network. The hub contains various service endpoints to enable connectivity. From your on-premises network (vpnsite), you can connect to a VPN Gateway inside the virtual hub, connect ExpressRoute circuits to a virtual hub, or even connect mobile users to a Point-to-site gateway in the virtual hub. The hub is the core of your network in a region. Multiple virtual hubs can be created in the same region.

You plan to deploy five virtual machines to a virtual network subnet.

Each virtual machine will have a public IP address and a private IP address.

Each virtual machine requires the same inbound and outbound security rules.

What is the minimum number of network interfaces and network security groups that you require? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

Minimum number of network interfaces:

|    |
|----|
| 5  |
| 10 |
| 15 |
| 20 |

Minimum number of network security groups:

|    |
|----|
| 1  |
| 2  |
| 5  |
| 10 |

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

| Name | Type            |
|------|-----------------|
| LB1  | Load balancer   |
| VM1  | Virtual machine |
| VM2  | Virtual machine |

LB1 is configured as shown in the following table.

| Name                 | Type                      | Value   |
|----------------------|---------------------------|---|
| bepool1              | Backend pool              | VM1, VM2  |
| LoadBalancerFrontEnd | Frontend IP configuration | Public IP address   |
| hprobe1              | Health probe              | Protocol: TCP<br>Port: 80<br>Interval: 5 seconds<br>Unhealthy threshold: 2  |
| rule1                | Load balancing rule       | IP version: IPv4<br>Frontend IP address: LoadBalancerFrontEnd<br>Port: 80<br>Backend Port: 80<br>Backend pool: bepool1<br>Health probe: hprobe1 |

You plan to create new inbound NAT rules that meet the following requirements:

☞ Provide Remote Desktop access to VM1 from the internet by using port 3389.

☞ Provide Remote Desktop access to VM2 from the internet by using port 3389.

What should you create on LB1 before you can create the new inbound NAT rules?

A. a frontend IP address Most Voted

B. a load balancing rule Most Voted

C. a health probe

D. a backend pool

[Hide Solution](#)

[Discussion](#) 95

**Correct Answer:** A 

*Community vote distribution*

A (52%)

B (48%)

You plan to create new inbound NAT rules that meet the following requirements:

- \* Provide Remote Desktop access to VM1 from the internet by using port 3389.
- \* Provide Remote Desktop access to VM2 from the internet by using port 3389.

What should you create on LB1 before you can create the new inbound NAT rules?

A. a frontend IP address -

This lets you RDP to a specific VM1 or VM2 using Port 3389.

Other solutions using one IP require floating IP where you can't choose VM1 or VM2, or they require different ports which is contrary to the 3389 requirements.

B. a load balancing rule - does not provide RDP access to a specific VM1 or VM2 over port 3389.

C. a health probe - does not provide RDP access to a specific VM1 or VM2 over port 3389.

D. a backend pool - does not provide RDP access to a specific VM1 or VM2 over port 3389.

HOTSPOT -

You have Azure virtual machines that run Windows Server 2019 and are configured as shown in the following table.

| Name | Private IP address | Public IP address | Virtual network name | DNS suffix configured in Windows Server |
|------|--------------------|-------------------|----------------------|---|
| VM1  | 10.1.0.4           | 52.186.85.63      | VNET1                | Adatum.com                              |
| VM2  | 10.1.0.5           | 13.92.168.13      | VNET1                | Contoso.com                             |

You create a private Azure DNS zone named adatum.com. You configure the adatum.com zone to allow auto registration from VNET1.

Which A records will be added to the adatum.com zone for each virtual machine? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

A records for VM1:

|  |
|--|
| None                                     |
| Private IP address only                  |
| Public IP address only                   |
| Private IP address and public IP address |

A records for VM2:

|  |
|--|
| None                                     |
| Private IP address only                  |
| Public IP address only                   |
| Private IP address and public IP address |

You have an Azure virtual network named VNet1 that connects to your on-premises network by using a site-to-site VPN. VNet1 contains one subnet named Subnet1.

Subnet1 is associated to a network security group (NSG) named NSG1. Subnet1 contains a basic internal load balancer named ILB1. ILB1 has three Azure virtual machines in the backend pool.

You need to collect data about the IP addresses that connects to ILB1. You must be able to run interactive queries from the Azure portal against the collected data.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

Resource to create:

|                                  |
|----------------------------------|
| An Azure Event Grid              |
| An Azure Log Analytics workspace |
| An Azure Storage account         |

Resource on which to enable diagnostics:

|                            |
|----------------------------|
| ILB1                       |
| NSG1                       |
| The Azure virtual machines |

Correct Answer:

Box 1: An Azure Log Analytics workspace

In the Azure portal you can set up a Log Analytics workspace, which is a unique Log Analytics environment with its own data repository, data sources, and solutions.

Box 2: NSG1

NSG flow logs allow viewing information about ingress and egress IP traffic through a Network security group. Through this, the IP addresses that connect to the ILB can be monitored when the diagnostics are enabled on a Network Security Group.

We cannot enable diagnostics on an internal load balancer to check for the IP addresses.

As for Internal LB, it is basic one. Basic can only connect to storage account. Also, Basic LB has only activity logs, which doesn't include the connectivity workflow. So, we need to use NSG to meet the mentioned requirements.

You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains four subnets named Gateway, Perimeter, NVA, and Production. The NVA subnet contains two network virtual appliances (NVAs) that will perform network traffic inspection between the Perimeter subnet and the Production subnet. You need to implement an Azure load balancer for the NVAs. The solution must meet the following requirements:

- The NVAs must run in an active-active configuration that uses automatic failover.
- The load balancer must load balance traffic to two services on the Production subnet. The services have different IP addresses.

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

NOTE: Each correct selection is worth one point.

A. Deploy a basic load balancer

B. Deploy a standard load balancer **Most Voted**

C. Add two load balancing rules that have HA Ports and Floating IP enabled

D. Add two load balancing rules that have HA Ports enabled and Floating IP disabled **Most Voted**

E. Add a frontend IP configuration, a backend pool, and a health probe **Most Voted**

F. Add a frontend IP configuration, two backend pools, and a health probe

[Hide Solution](#)

[Discussion 72](#)

Correct Answer: **BCF** 

B- Standard Load Balancer support High Availability

C- We need 2 High availability ports Rules ( backend pools ) and Float IP enabled. The HA ports load-balancing rules help you with scenarios, such as high availability and scale for network virtual appliances (NVAs) inside virtual networks.

F- For the 2 High availability ports Rules need to set 1 Front IP of LB and 2 backend pool (2 services) and health probe

Additional Explanation:

1st High availability ports Rule: Front End IP (LB) , backend1(service1),health probe, HA port selected and Float IP selected

2nd High availability ports Rule: Front End IP (LB) , backend2(service2),health probe, HA port selected and Float IP selected

You have an Azure subscription named Subscription1 that contains two Azure virtual networks named VNet1 and VNet2. VNet1 contains a VPN gateway named VPNGW1 that uses static routing. There is a site-to-site VPN connection between your on-premises network and VNet1.

On a computer named Client1 that runs Windows 10, you configure a point-to-site VPN connection to VNet1.

You configure virtual network peering between VNet1 and VNet2. You verify that you can connect to VNet2 from the on-premises network. Client1 is unable to connect to VNet2.

You need to ensure that you can connect Client1 to VNet2.

What should you do?

- A. Download and re-install the VPN client configuration package on Client1. **Most Voted**
- B. Select Allow gateway transit on VNet1.
- C. Select Allow gateway transit on VNet2.
- D. Enable BGP on VPNGW1

[Hide Solution](#)[Discussion 48](#)

Correct Answer: A 🎉

"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"

I would go with `A` is the correct option as the S2S config has been changed AFTER the P2S client installation was performed. Installation of the client software package needs installing again post S2S config changes.

You have an Azure subscription. The subscription contains virtual machines that run Windows Server 2016 and are configured as shown in the following table.

| Name | Virtual network | DNS suffix configured in Windows Server |
|------|-----------------|---|
| VM1  | VNET2           | Contoso.com                             |
| VM2  | VNET2           | None                                    |
| VM3  | VNET2           | Adatum.com                              |

You create a public Azure DNS zone named adatum.com and a private Azure DNS zone named contoso.com. You create a virtual network link for contoso.com as shown in the following exhibit.

The screenshot shows the Azure portal interface for managing a virtual network link. At the top, there's a header with a back button, a search bar, and navigation links for 'Compute', 'Storage', 'Networking', 'Databases', 'Machine Learning', and 'API Management'. Below the header, the main content area has a title 'link1' and a subtitle 'contoso.com'. There are tabs for 'Overview', 'Settings', 'Logs', and 'Metrics'. A toolbar below the tabs includes 'Save', 'Discard', 'Delete', 'Access Control (IAM)', and 'Tags'. The main body of the page contains the following fields:

- Link name:** link1
- Link state:** Completed
- Provisioning state:** Succeeded
- Virtual network details:** Virtual network id: /subscriptions/8372f433-2dcd-4361-b5ef-5b188fed87d0/resourceGroups/RG2/provi... (with a copy icon)
- Virtual network:** VNET2
- Configuration:** A checkbox labeled 'Enable auto registration' is checked.

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

## Answer Area

| Statements  | Yes                              | No                               |
|---|----------------------------------|----------------------------------|
| When VM1 starts, a record for VM1 is added to the contoso.com DNS zone. | <input checked="" type="radio"/> | <input type="radio"/>            |
| When VM2 starts, a record for VM2 is added to the contoso.com DNS zone. | <input checked="" type="radio"/> | <input type="radio"/>            |
| When VM3 starts, a record for VM3 is added to the adatum.com DNS zone.  | <input type="radio"/>            | <input checked="" type="radio"/> |

### Question #11

Topic 5

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

| Name  | Type                         | Azure region | Resource group |
|-------|------------------------------|--------------|----------------|
| VNet1 | Virtual network              | West US      | RG2            |
| VNet2 | Virtual network              | West US      | RG1            |
| VNet3 | Virtual network              | East US      | RG1            |
| NSG1  | Network security group (NSG) | East US      | RG2            |

To which subnets can you apply NSG1?

- A. the subnets on VNet1 only
- B. the subnets on VNet2 and VNet3 only
- C. the subnets on VNet2 only
- D. the subnets on VNet3 only **Most Voted**
- E. the subnets on VNet1, VNet2, and VNet3

[Hide Solution](#)

[Discussion 29](#)

Correct Answer: D 

All Azure resources are created in an Azure region and subscription. A resource can only be created in a virtual network that exists in the same region and subscription as the resource.

**Question #12****Topic 5**

DRAG DROP -

You have an Azure subscription that contains two virtual networks named VNet1 and VNet2. Virtual machines connect to the virtual networks.

The virtual networks have the address spaces and the subnets configured as shown in the following table.

| Virtual network | Address space | Subnet                     | Peering |
|-----------------|---------------|----------------------------|---------|
| VNet1           | 10.1.0.0/16   | 10.1.0.0/24<br>10.1.1.0/26 | VNet2   |
| VNet2           | 10.2.0.0/16   | 10.2.0.0/24                | VNet1   |

You need to add the address space of 10.33.0.0/16 to VNet1. The solution must ensure that the hosts on VNet1 and VNet2 can communicate.

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

Select and Place:

**Actions**

Remove VNet1.

Add the 10.33.0.0/16 address space to VNet1.

Create a new virtual network named VNet1.

On the peering connection in VNet2, allow gateway transit.

Recreate peering between VNet1 and VNet2.

On the peering connection in VNet1, allow gateway transit.

Remove peering between VNet1 and VNet2.

**Answer Area**

Remove peering between VNet1 and VNet2.

Add the 10.33.0.0/16 address space to VNet1.

Recreate peering between VNet1 and VNet2.

**Question #13****Topic 5**

You have an Azure subscription that contains the resource groups shown in the following table.

| Name | Location |
|------|----------|
| RG1  | West US  |
| RG2  | East US  |

RG1 contains the resources shown in the following table.

| Name     | Type              | Location |
|----------|-------------------|----------|
| storage1 | Storage account   | West US  |
| VNet1    | Virtual network   | West US  |
| NIC1     | Network interface | West US  |
| Disk1    | Disk              | West US  |
| VM1      | Virtual machine   | West US  |

VM1 is running and connects to NIC1 and Disk1. NIC1 connects to VNET1.

RG2 contains a public IP address named IP2 that is in the East US location. IP2 is not assigned to a virtual machine.

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

NOTE: Each correct selection is worth one point.

## Answer Area

| Statements   | <b>Yes</b>                       | <b>No</b>                        |
|--|----------------------------------|----------------------------------|
| You can move storage1 to RG2.                            | <input checked="" type="radio"/> | <input type="radio"/>            |
| You can move NIC1 to RG2.                                | <input checked="" type="radio"/> | <input type="radio"/>            |
| If you move IP2 to RG1, the location of IP2 will change. | <input type="radio"/>            | <input checked="" type="radio"/> |

1. YES. I was able to move the storage from RG1 to RG2, however it stayed in the West US region.
2. YES.

I was able to move NIC1 from RG1 to RG2 which was associated with VM1 and VNET1 subnet1, however it stayed in the West US region.

3. NO.

You have an Azure web app named webapp1.

You have a virtual network named VNET1 and an Azure virtual machine named VM1 that hosts a MySQL database. VM1 connects to VNET1.

You need to ensure that webapp1 can access the data hosted on VM1.

What should you do?

- A. Deploy an internal load balancer
- B. Peer VNET1 to another virtual network
- C. Connect webapp1 to VNET1 Most Voted
- D. Deploy an Azure Application Gateway

[Hide Solution](#)[Discussion 121](#)

**Correct Answer:** D 🏆

*Community vote distribution*

C (100%)

You create an Azure VM named VM1 that runs Windows Server 2019.  
VM1 is configured as shown in the exhibit. (Click the Exhibit tab.)

The screenshot shows the Azure portal interface for a virtual machine named VM1. The top navigation bar includes 'Connect', 'Start', 'Restart', 'Stop', 'Capture', 'Delete', and 'Refresh' buttons. On the left, a sidebar lists various management options: Security, Extensions, Continuous delivery (Preview), Availability set, Configuration, Identity, Properties, Locks, Export template, Auto-shutdown, Backup, Disaster recovery, Update management, Inventory, Change tracking, Configuration management ..., Policies, Run command, Monitoring, Insights (preview), Alerts, Metrics, and Diagnostics settings. The main content area displays detailed configuration information for VM1, including its resource group (RG1), status (Stopped (deallocated)), location (West Europe), subscription (Azure Pass – Sponsorship), and subscription ID (80f9d59c-629e-4346-b577-8b7e1ef1316a). It also shows computer name, operating system (Windows), size (Standard DS2 v2 (2 vcpus, 7 GiB memory)), ephemeral OS disk (N/A), public and private IP addresses (VM1-ip, 10.0.0.4), virtual network/subnet (VNET1/default), and DNS name (Configure). A 'Tags (change)' section allows adding tags. Below this, a chart titled 'CPU (average)' shows usage over the last hour, with values ranging from 0% to 100% at 10:15 PM, 10:30 PM, 10:45 PM, and 11 PM. The chart title is 'Percentage-CPU (Avg) vm1'. Another chart titled 'Network (total)' shows a value of 608.

You need to enable Desired State Configuration for VM1.  
What should you do first?

- A. Connect to VM1.
- B. Start VM1.
- C. Capture a snapshot of VM1.
- D. Configure a DNS name for VM1.

[Hide Solution](#)

[Discussion 25](#)

**Correct Answer:** B 

Status is Stopped (Deallocated).

The DSC extension for Windows requires that the target virtual machine is able to communicate with Azure.

The VM needs to be started.

Reference:

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

*Community vote distribution*

B (100%)

## Question #16

Topic 5

You have five Azure virtual machines that run Windows Server 2016. The virtual machines are configured as web servers.

You have an Azure load balancer named LB1 that provides load balancing services for the virtual machines.

You need to ensure that visitors are serviced by the same web server for each request.

What should you configure?

- A. Floating IP (direct server return) to Disabled
- B. Session persistence to None
- C. Floating IP (direct server return) to Enabled
- D. Session persistence to Client IP

[Hide Solution](#)

[Discussion 11](#)

**Correct Answer:** D 

With Sticky Sessions when a client starts a session on one of your web servers, session stays on that specific server. To configure An Azure Load-Balancer For Sticky Sessions set Session persistence to Client IP or to Client IP and protocol.

On the following image you can see sticky session configuration:

Note:

- Client IP and protocol specifies that successive requests from the same client IP address and protocol combination will be handled by the same virtual machine.
- Client IP specifies that successive requests from the same client IP address will be handled by the same virtual machine.

Reference:

<https://cloudopszone.com/configure-azure-load-balancer-for-sticky-sessions/>

*Community vote distribution*

D (100%)

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

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

You have an Azure subscription that contains the following resources:

- A virtual network that has a subnet named Subnet1
- Two network security groups (NSGs) named NSG-VM1 and NSG-Subnet1
- A virtual machine named VM1 that has the required Windows Server configurations to allow Remote Desktop connections

NSG-Subnet1 has the default inbound security rules only.

NSG-VM1 has the default inbound security rules and the following custom inbound security rule:

- Priority: 100
- Source: Any
- Source port range: \*
- Destination: \*
- Destination port range: 3389
- Protocol: UDP
- Action: Allow

VM1 has a public IP address and is connected to Subnet1. NSG-VM1 is associated to the network interface of VM1. NSG-Subnet1 is associated to Subnet1.

You need to be able to establish Remote Desktop connections from the internet to VM1.

Solution: You add an inbound security rule to NSG-Subnet1 that allows connections from the Any source to the \*destination for port range 3389 and uses the TCP protocol. You remove NSG-VM1 from the network interface of VM1.

Does this meet the goal?

A. Yes Most Voted

B. No Most Voted

[Hide Solution](#)

[Discussion 134](#)

**Correct Answer: B** 

The default port for RDP is TCP port 3389. A rule to permit RDP traffic must be created automatically when you create your VM.

Note on NSG-Subnet1: Azure routes network traffic between all subnets in a virtual network, by default.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-rdp-connection>

*Community vote distribution*

A (71%)

B (29%)

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

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

You have an Azure subscription that contains the following resources:

- A virtual network that has a subnet named Subnet1
- Two network security groups (NSGs) named NSG-VM1 and NSG-Subnet1
- A virtual machine named VM1 that has the required Windows Server configurations to allow Remote Desktop connections

NSG-Subnet1 has the default inbound security rules only.

NSG-VM1 has the default inbound security rules and the following custom inbound security rule:

- Priority: 100
- Source: Any
- Source port range: \*
- Destination: \*
- Destination port range: 3389

Protocol: UDP –

- Action: Allow

VM1 has a public IP address and is connected to Subnet1. NSG-VM1 is associated to the network interface of VM1. NSG-Subnet1 is associated to Subnet1.

You need to be able to establish Remote Desktop connections from the internet to VM1.

Solution: You add an inbound security rule to NSG-Subnet1 that allows connections from the internet source to the VirtualNetwork destination for port range 3389 and uses the UDP protocol.  
Does this meet the goal?

A. Yes

B. No **Most Voted**

[Hide Solution](#)

[Discussion 29](#)

**Correct Answer: B** 

The default port for RDP is TCP port 3389. A rule to permit RDP traffic must be created automatically when you create your VM.

Note on NSG-Subnet1: Azure routes network traffic between all subnets in a virtual network, by default.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-rdp-connection>

*Community vote distribution*

**B (75%)**

**A (25%)**

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription that contains the following resources:

- A virtual network that has a subnet named Subnet1
- Two network security groups (NSGs) named NSG-VM1 and NSG-Subnet1
- A virtual machine named VM1 that has the required Windows Server configurations to allow Remote Desktop connections

NSG-Subnet1 has the default inbound security rules only.

NSG-VM1 has the default inbound security rules and the following custom inbound security rule:

- Priority: 100
- Source: Any
- Source port range: \*
- Destination: \*
- Destination port range: 3389
- Protocol: UDP
- Action: Allow

VM1 has a public IP address and is connected to Subnet1. NSG-VM1 is associated to the network interface of VM1. NSG-Subnet1 is associated to Subnet1.

You need to be able to establish Remote Desktop connections from the internet to VM1.

Solution: You add an inbound security rule to NSG-Subnet1 and NSG-VM1 that allows connections from the internet source to the VirtualNetwork destination for port range 3389 and uses the TCP protocol.

Does this meet the goal?

A. Yes **Most Voted**

B. No

[Hide Solution](#)

[Discussion](#) 57

**Correct Answer: A** 

The default port for RDP is TCP port 3389. A rule to permit RDP traffic must be created automatically when you create your VM.

Note on NSG-Subnet1: Azure routes network traffic between all subnets in a virtual network, by default.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-rdp-connection>

*Community vote distribution*

A (75%)

B (25%)

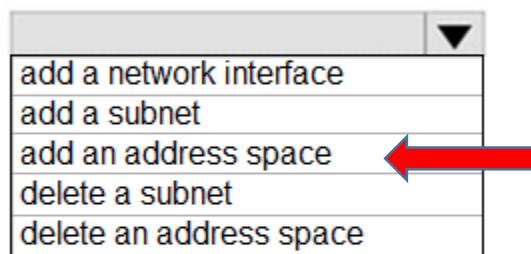
You have a virtual network named VNet1 that has the configuration shown in the following exhibit.

```
Name          : VNet1
ResourceGroupName  : Production
Location        : westus
Id             : /subscriptions/14d26092-8e42-4ea7-b770-
9dcef70fb1ea/resourceGroups/Production/providers/Microsoft.Network/virtualNetworks/VNet1
Etag           : W/"76f7edd6-d022-455b-aeae-376059318e5d"
ResourceGuid    : 562696cc-b2ba-4cc5-9619-0a735d6c34c7
ProvisioningState : Succeeded
Tags           :
AddressSpace   : {
    "AddressPrefixes": [
        "10.2.0.0/16"
    ]
}
DhcpOptions    : {}
Subnets        : [
    {
        "Name": "default",
        "Etag": "W/\"76f7edd6-d022-455b-aeae-376059318e5d\"",
        "Id": "/subscriptions/14d26092-8e42-4ea7-b770-
9dcef70fb1ea/resourceGroups/Production/providers/Microsoft.Network/
virtualNetworks/VNet1/subnets/default",
        "AddressPrefix": "10.2.0.0/24",
        "IpConfigurations": [],
        "ResourceNavigationLinks": [],
        "ServiceEndpoints": [],
        "ProvisioningState": "Succeeded"
    }
]
VirtualNetworkPeerings : []
EnableDDoSProtection : false
EnableVmProtection   : false
```

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

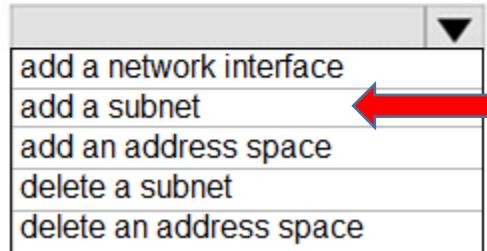
## Answer Area

Before a virtual machine on VNet1 can receive an IP address from 192.168.1.0/24, you must first



- add a network interface
- add a subnet
- add an address space ←
- delete a subnet
- delete an address space

Before a virtual machine on VNet1 can receive an IP address from 10.2.1.0/24, you must first



- add a network interface
- add a subnet ←
- add an address space
- delete a subnet
- delete an address space

You have an Azure subscription that contains a virtual network named VNET1. VNET1 contains the subnets shown in the following table.

| Name    | Connected virtual machines |
|---------|----------------------------|
| Subnet1 | VM1, VM2                   |
| Subnet2 | VM3, VM4                   |
| Subnet3 | VM5, VM6                   |

Each virtual machine uses a static IP address.

You need to create network security groups (NSGs) to meet following requirements:

- Allow web requests from the internet to VM3, VM4, VM5, and VM6.
- Allow all connections between VM1 and VM2.
- Allow Remote Desktop connections to VM1.
- Prevent all other network traffic to VNET1.

What is the minimum number of NSGs you should create?

A. 1 Most Voted

B. 3

C. 4

D. 12

Correct Answer: A

NSGs can be associated to subnets, individual VMs (classic), or individual network interfaces (NIC) attached to VMs (Resource Manager). You can associate zero, or one, NSG(s) to each VNet subnet and NIC in a virtual machine. The same NSG can be associated to as many subnets and NICs as you choose. So, you can create 1 NSG and associate it with all 3 Subnets.

- Allow web requests from internet to VM3, VM4, VM5 and VM 6: You need to add an inbound rule to allow Internet TCP 80 to VM3, VM4, VM5 and VM6 static IP addresses.
- Allow all connections between VM1 & VM2: You do not need an NSG as communication in the same VNet is allowed by default, without even configuring NSG.
- Allow remote desktop to VM1: You need to add an inbound rule to allow RDP 3389 in VM1's static IP address .
- Prevent all other network traffic to VNET1: You do not need to configure any NSG as the there is explicit deny rule (DenyAllInbound) in every NSG.

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

| Name  | Type            | Resource group |
|-------|-----------------|----------------|
| VNET1 | Virtual network | RG1            |
| VM1   | Virtual machine | RG1            |

The Not allowed resource types Azure policy that has policy enforcement enabled is assigned to RG1 and uses the following parameters:

Microsoft.Network/virtualNetworks

Microsoft.Compute/virtualMachines

In RG1, you need to create a new virtual machine named VM2, and then connect VM2 to VNET1.

What should you do first?

- A. Remove Microsoft.Compute/virtualMachines from the policy.
- B. Create an Azure Resource Manager template
- C. Add a subnet to VNET1.
- D. Remove Microsoft.Network/virtualNetworks from the policy.

[Hide Solution](#)

[Discussion](#) 15

**Correct Answer:** A 

The Not allowed resource types Azure policy prohibits the deployment of specified resource types. You specify an array of the resource types to block.

Virtual Networks and Virtual Machines are prohibited.

Reference:

<https://docs.microsoft.com/en-us/azure/governance/policy/samples/not-allowed-resource-types>

*Community vote distribution*

A (100%)

Your company has an Azure subscription named Subscription1.

The company also has two on-premises servers named Server1 and Server2 that run Windows Server 2016. Server1 is configured as a DNS server that has a primary DNS zone named adatum.com. Adatum.com contains 1,000 DNS records.

You manage Server1 and Subscription1 from Server2. Server2 has the following tools installed:

- The DNS Manager console
- Azure PowerShell
- Azure CLI 2.0

You need to move the adatum.com zone to an Azure DNS zone in Subscription1. The solution must minimize administrative effort.

What should you use?

A. Azure CLI Most Voted

B. Azure PowerShell

C. the Azure portal

D. the DNS Manager console

[Hide Solution](#)

[Discussion 64](#)

**Correct Answer:** B 

Step 1: Installing the DNS migration script

Open an elevated PowerShell window (Administrative mode) and run following command `install-script PrivateDnsMigrationScript`

Step 2: Running the script -

Execute following command to run the script

`PrivateDnsMigrationScript.ps1 -`

Reference:

<https://docs.microsoft.com/en-us/azure/dns/private-dns-migration-guide>

*Community vote distribution*

A (91%)

9%

- Azure DNS supports importing and exporting zone files by using the Azure command-line interface (CLI). Zone file import is not currently supported via Azure PowerShell or the Azure portal.

`PrivateDNSMigrationScript` is for migrating legacy Azure DNS private zones to the new Azure DNS private zone resource.

You have a public load balancer that balances ports 80 and 443 across three virtual machines named VM1, VM2, and VM3.

You need to direct all the Remote Desktop Protocol (RDP) connections to VM3 only.

What should you configure?

A. an inbound NAT rule **Most Voted**

B. a new public load balancer for VM3

C. a frontend IP configuration

D. a load balancing rule

[Hide Solution](#)

[Discussion \(12\)](#)

**Correct Answer:** A 

Reference:

<https://docs.microsoft.com/en-us/azure/load-balancer/tutorial-load-balancer-port-forwarding-portal> <https://pixelrobots.co.uk/2017/08/azure-load-balancer-for-rds/>

*Community vote distribution*

A (100%)

HOTSPOT -

You have an Azure subscription named Subscription1 that contains the virtual networks in the following table.

| Name  | Subnets            |
|-------|--------------------|
| VNet1 | Subnet11, Subnet12 |
| VNet2 | Subnet13           |

Subscription1 contains the virtual machines in the following table.

| Name | Subnet   | Availability set      |
|------|----------|-----------------------|
| VM1  | Subnet11 | AS1                   |
| VM2  | Subnet11 | AS1                   |
| VM3  | Subnet11 | <i>Not applicable</i> |
| VM4  | Subnet11 | <i>Not applicable</i> |
| VM5  | Subnet12 | <i>Not applicable</i> |
| VM6  | Subnet12 | <i>Not applicable</i> |

In Subscription1, you create a load balancer that has the following configurations:

- Name: LB1
- SKU: Basic
- Type: Internal
- Subnet: Subnet12
- Virtual network: VNET1

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

NOTE: Each correct selection is worth one point.

## Answer Area

| Statements                                       | Yes                              | No                               |
|--|----------------------------------|----------------------------------|
| LB1 can balance the traffic between VM1 and VM2. | <input checked="" type="radio"/> | <input type="radio"/>            |
| LB1 can balance the traffic between VM3 and VM4. | <input type="radio"/>            | <input checked="" type="radio"/> |
| LB1 can balance the traffic between VM5 and VM6. | <input type="radio"/>            | <input checked="" type="radio"/> |

Basic Load Balancer: Backend pool endpoints for Virtual machines in a single availability set or virtual machine scale set.

Subnet12 association will be used to assign an IP for the internal load balancer, not to load balance the VMs in the Subnet.

**Box 1: Yes**

VM1 and VM are in the Availability Set.

**Box 2: No**

Both VMs are not part of any Availability Set or Scale Set.

**Box 3: No**

Both VMs are not part of any Availability Set or Scale Set.

Reference: <https://docs.microsoft.com/en-us/azure/load-balancer/skus>

**HOTSPOT -**

You have an Azure virtual machine that runs Windows Server 2019 and has the following configurations:

- Name: VM1
- Location: West US
- Connected to: VNET1
- Private IP address: 10.1.0.4
- Public IP addresses: 52.186.85.63
- DNS suffix in Windows Server: Adatum.com

You create the Azure DNS zones shown in the following table.

| Name        | Type    | Location     |
|-------------|---------|--------------|
| Adatum.pri  | Private | West Europe  |
| Contoso.pri | Private | Central US   |
| Adatum.com  | Public  | West Europe  |
| Contoso.com | Public  | North Europe |

You need to identify which DNS zones you can link to VNET1 and the DNS zones to which VM1 can automatically register.

Which zones should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

DNS zones that you can link to VNET1:

|                                |
|--------------------------------|
| Adatum.com only                |
| Adatum.pri and adatum.com only |
| The private zones only         |
| The public zones only          |

DNS zones to which VM1 can automatically register:

|                                |
|--------------------------------|
| Adatum.com only                |
| Adatum.pri and adatum.com only |
| The private zones only         |
| The public zones only          |

DRAG DROP -

You have an on-premises network that you plan to connect to Azure by using a site-to-site VPN.

In Azure, you have an Azure virtual network named VNet1 that uses an address space of 10.0.0.0/16. VNet1 contains a subnet named Subnet1 that uses an address space of 10.0.0.0/24.

You need to create a site-to-site VPN to Azure.

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

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

Select and Place:

**Actions****Answer Area**

Create a local gateway.

Create a gateway subnet.

Create a VPN gateway.

Create a VPN gateway.

Create a gateway subnet.

Create a local gateway.



Create a custom DNS server.

Create a VPN connection.



Create a VPN connection.

Create an Azure Content Delivery Network (CDN) profile.

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

| Name    | Type            | Details               |
|---------|-----------------|-----------------------|
| VNet1   | Virtual network | <i>Not applicable</i> |
| Subnet1 | Subnet          | Hosted on VNet1       |
| VM1     | Virtual machine | On Subnet1            |
| VM2     | Virtual machine | On Subnet1            |

VM1 and VM2 are deployed from the same template and host line-of-business applications.

You configure the network security group (NSG) shown in the exhibit. (Click the Exhibit tab.)

→ Move    Delete    Refresh

Resource group (change) : RG1lod9053488      Custom security rules : 1 inbound, 1 outbound  
 Location : East US      Associated with : 0 subnets, 0 network interfaces  
 Subscription (change) : Microsoft AZ  
 Subscription ID : ac344a74-f85a-4b2e-8057-642088faaf20

Tags (change) : Click here to add tags

Inbound security rules

| PRIORITY | NAME                           | PORT | PROTOCOL | SOURCE            | DESTINATION    | ACTION |
|----------|--------------------------------|------|----------|-------------------|----------------|--------|
| 100      | Port_80                        | 80   | TCP      | Internet          | Any            | Deny   |
| 65000    | AllowVnetInBound               | Any  | Any      | VirtualNetwork    | VirtualNetwork | Allow  |
| 65001    | Allow AzureLoadBalancerInBound | Any  | Any      | AzureLoadBalancer | Any            | Allow  |
| 65500    | DenyAllInBound                 | Any  | Any      | Any               | Any            | Deny   |

Outbound security rules

| PRIORITY | NAME                  | PORT | PROTOCOL | SOURCE         | DESTINATION    | ACTION |
|----------|-----------------------|------|----------|----------------|----------------|--------|
| 100      | DenyWebSites          | 80   | TCP      | Any            | Internet       | Deny   |
| 65000    | AllowVnetOutBound     | Any  | Any      | VirtualNetwork | VirtualNetwork | Allow  |
| 65001    | AllowInternetOutBound | Any  | Any      | Any            | Internet       | Allow  |
| 65500    | DenyAllOutBound       | Any  | Any      | Any            | Any            | Deny   |

You need to prevent users of VM1 and VM2 from accessing websites on the Internet over TCP port 80.

What should you do?

- A. Disassociate the NSG from a network interface
- B. Change the Port\_80 inbound security rule.
- C. Associate the NSG to Subnet1. **Most Voted**
- D. Change the DenyWebsITES outbound security rule.

[Hide Solution](#)

[Discussion 19](#)

**Correct Answer:** C 

You can associate or dissociate a network security group from a network interface or subnet.

The NSG has the appropriate rule to block users from accessing the Internet. We just need to associate it with Subnet1.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/manage-network-security-group>

*Community vote distribution*

C (100%)

## Question #29

Topic 5

You have two subscriptions named Subscription1 and Subscription2. Each subscription is associated to a different Azure AD tenant.

Subscription1 contains a virtual network named VNet1. VNet1 contains an Azure virtual machine named VM1 and has an IP address space of 10.0.0.0/16.

Subscription2 contains a virtual network named VNet2. VNet2 contains an Azure virtual machine named VM2 and has an IP address space of 10.10.0.0/24.

You need to connect VNet1 to VNet2.

What should you do first?

- A. Move VM1 to Subscription2.
- B. Move VNet1 to Subscription2.
- C. Modify the IP address space of VNet2.
- D. Provision virtual network gateways. **Most Voted**

[Hide Solution](#)

[Discussion 41](#)

**Correct Answer:** D 

Correct Answer: D

There is no overlap between the VNets: VNet1: 10.0.0.0/16 - CIDR IP Range 10.0.0.0 - 10.0.255.255 VNet2: 10.10.0.0/24 - CIDR IP Range 10.10.0.0 - 10.0.0.255

Note: If a virtual network has address ranges that overlap with another virtual network or on-premises network, the two networks can't be connected.

You can connect virtual networks (VNets) by using the VNet-to-VNet connection type. Virtual networks can be in different regions and from different subscriptions. When you connect VNets from different subscriptions, the subscriptions don't need to be associated with the same Active Directory tenant.

They just need to have a Virtual network gateway to communicate using Public IP where it is secured using SSTP or IKEv2.

You plan to create an Azure virtual machine named VM1 that will be configured as shown in the following exhibit.

### Create a virtual machine

 Changing Basic options may reset selections you have made. Review all options prior to creating the virtual machine.

**Basics**   Disks   Networking   Management   Advanced   Tags   Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image.

Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization.

Looking for classic VMs? [Create VM from Azure Marketplace](#)

#### PROJECT DETAILS

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

|  |   |
|--|---|
| * Subscription        | MyDev-Test Subscription            |
| └── * Resource group  | RG1 <br><a href="#">Create new</a> |

#### INSTANCE DETAILS

|  |  |
|--|--|
| * Virtual machine name  | VM1  |
| * Region                | (US) West US 2    |
| Availability options    | No infrastructure redundancy required   |
| * Image                 | Windows Server 2016 Datacenter <br><a href="#">Browse all public and private images</a> |
| Azure Spot instance     | <input type="radio"/> Yes <input checked="" type="radio"/> No  |

\* Size 

**Standard DS1 v2**

1 vcpu, 3.5 GiB memory (ZAR 632.47/month)

[Change size](#)

The planned disk configurations for VM1 are shown in the following exhibit.

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

#### Disk options

\* OS disk type [?](#)

Standard HDD



The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.

Enable Ultra Disk compatibility (Preview) [?](#)  Yes  No

Ultra Disks are only available when using Managed Disks.

#### Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

Adding unmanaged data disks is currently not supported at the time of VM creation. You can add them after the VM is created.

#### Advanced

Use managed disks [?](#)

No  Yes

\* Storage account [?](#)

(new) rg1 disks799



[Create new](#)

You need to ensure that VM1 can be created in an Availability Zone.

Which two settings should you modify? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Use managed disks [Most Voted](#)

B. OS disk type

C. Availability options [Most Voted](#)

D. Size

E. Image

[Hide Solution](#)

Discussion 38

Correct Answer: AC

A: Your VMs should use managed disks if you want to move them to an Availability Zone by using Site Recovery.

C: When you create a VM for an Availability Zone, Under Settings > High availability, select one of the numbered zones from the Availability zone dropdown.

**HOTSPOT -**

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

| Name  | Type                      | Resource group        | Location   |
|-------|---------------------------|-----------------------|------------|
| RG1   | Resource group            | <i>Not applicable</i> | Central US |
| RG2   | Resource group            | <i>Not applicable</i> | West US    |
| RG3   | Resource group            | <i>Not applicable</i> | East US    |
| VMSS1 | Virtual machine scale set | RG1                   | West US    |

VMSS1 is set to VM (virtual machines) orchestration mode.

You need to deploy a new Azure virtual machine named VM1, and then add VM1 to VMSS1.

Which resource group and location should you use to deploy VM1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

Resource group:

RG1 only

RG2 only

RG1 or RG2 only

RG1, RG2, or RG3

Location:

West US only

Central US only

Central US or West US only

East US, Central US, or West US

Box 1: RG1, RG2, or RG3

The resource group stores metadata about the resources. When you specify a location for the resource group, you're specifying where that metadata is stored. The location of the RG doesn't influence the choice of the location of VM. Best practice would be to create the VM1 in the RG1 because the scale set is in RG1. And Microsoft recommends that resources contained in a Resource Group share the same resource lifecycle.

Box 2: West US only

You can add the virtual machine to a scale set in the same region, zone, and resource group.

You have an Azure subscription that contains three virtual networks named VNET1, VNET2, and VNET3. Peering for VNET1 is configured as shown in the following exhibit.

**VNET1 | Peerings**  
Virtual network

Search (Ctrl+/  
Overview  
Activity log  
Access control (IAM)  
Tags  
Diagnose and solve problems

Add Refresh X

Search peerings

| NAME     | PEERING STATUS | PEER  | GATEWAY TRANSIT |
|----------|----------------|-------|-----------------|
| Peering1 | Connected      | VNET2 | Disabled        |
| Peering1 | Connected      | VNET3 | Disabled        |

Peering for VNET2 is configured as shown in the following exhibit.

**VNET2 | Peerings**  
Virtual network

Search (Ctrl+/  
Overview  
Activity log  
Access control (IAM)  
Tags  
Diagnose and solve problems

Add Refresh X

Search peerings

| NAME     | PEERING STATUS | PEER  | GATEWAY TRANSIT |
|----------|----------------|-------|-----------------|
| Peering1 | Connected      | VNET1 | Disabled        |

Peering for VNET3 is configured as shown in the following exhibit.

**VNET3 | Peerings**  
Virtual network

Search (Ctrl+/  
Overview  
Activity log  
Access control (IAM)  
Tags  
Diagnose and solve problems

Add Refresh X

Search peerings

| NAME     | PEERING STATUS | PEER  | GATEWAY TRANSIT |
|----------|----------------|-------|-----------------|
| Peering1 | Connected      | VNET1 | Disabled        |

How can packets be routed between the virtual networks? To answer, select the appropriate options in the answer area.

## Answer Area

Packets from VNET1 can be routed to:

|                 |
|-----------------|
| VNET2 only      |
| VNET3 only      |
| VNET2 and VNET3 |

Packets from VNET2 can be routed to:

|                 |
|-----------------|
| VNET1 only      |
| VNET3 only      |
| VNET1 and VNET3 |

Question #33

Topic 5

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

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

You have a computer named Computer1 that has a point-to-site VPN connection to an Azure virtual network named VNet1. The point-to-site connection uses a self-signed certificate.

From Azure, you download and install the VPN client configuration package on a computer named Computer2.

You need to ensure that you can establish a point-to-site VPN connection to VNet1 from Computer2.

Solution: You modify the Azure Active Directory (Azure AD) authentication policies.

Does this meet the goal?

A. Yes

B. No

[Hide Solution](#)

[Discussion 16](#)

Correct Answer: **B** 

Instead export the client certificate from Computer1 and install the certificate on Computer2.

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

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

You have an Azure subscription that contains 10 virtual networks. The virtual networks are hosted in separate resource groups.

Another administrator plans to create several network security groups (NSGs) in the subscription.

You need to ensure that when an NSG is created, it automatically blocks TCP port 8080 between the virtual networks.

Solution: You create a resource lock, and then you assign the lock to the subscription.

Does this meet the goal?

A. Yes

B. No

[Hide Solution](#)

[Discussion 19](#)

Correct Answer: **B** 

You have an Azure subscription named Subscription1. Subscription1 contains a virtual machine named VM1. You have a computer named Computer1 that runs Windows 10. Computer1 is connected to the Internet. You add a network interface named vm1173 to VM1 as shown in the exhibit. (Click the Exhibit tab.)

**Network Interface: vm1173**

Virtual network/subnet: RG1-vnet/default  
networking: **Disabled**

**Effective security rules**

Public IP: VM1-ip  
Private IP: **10.0.0.5** Accelerated

**Topology**

**Inbound port rules**    **Outbound port rules**    **Application security groups**    **Load balancing**

**Add inbound port rule**

| PRIORITY | NAME               | PORT | PROTOCOL | SOURCE      | DESTINA...  | ACTION                                       |
|----------|--------------------|------|----------|-------------|-------------|--|
| 300      | ⚠️ RDP             | 3389 | TCP      | Any         | Any         | <span style="color: green;">Allow</span> ... |
| 65000    | AllowVnetInBound   | Any  | Any      | VirtualN... | VirtualN... | <span style="color: green;">Allow</span> ... |
| 65001    | AllowAzureLoadB... | Any  | Any      | AzureLo...  | Any         | <span style="color: green;">Allow</span> ... |
| 65500    | DenyAllInBound     | Any  | Any      | Any         | Any         | <span style="color: red;">Deny</span> ...    |

From Computer1, you attempt to connect to VM1 by using Remote Desktop, but the connection fails. You need to establish a Remote Desktop connection to VM1. What should you do first?

- A. Change the priority of the RDP rule
- B. Attach a network interface
- C. Delete the DenyAllInBound rule
- D. Start VM1

[Hide Solution](#)

[Discussion](#) 47

**Correct Answer:** D 

Incorrect Answers:

A: Rules are processed in priority order, with lower numbers processed before higher numbers, because lower numbers have higher priority. Once traffic matches a rule, processing stops. RDP already has the lowest number and thus the highest priority.

B: The network interface has already been added to VM.

C: The Outbound rules are fine.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/security-overview>

*Community vote distribution*

D (100%)

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

| Name | IP address | Connected to  |
|------|------------|---------------|
| VM1  | 10.1.0.4   | VNET1/Subnet1 |
| VM2  | 10.1.10.4  | VNET1/Subnet2 |
| VM3  | 172.16.0.4 | VNET2/SubnetA |
| VM4  | 10.2.0.8   | VNET3/SubnetB |

A DNS service is installed on VM1.

You configure the DNS servers settings for each virtual network as shown in the following exhibit.

Save Discard

DNS servers ⓘ

Default (Azure-provided)

Custom

|                |     |
|----------------|-----|
| 10.1.0.4       | ... |
| Add DNS server | ... |

You need to ensure that all the virtual machines can resolve DNS names by using the DNS service on VM1.

What should you do?

- A. Configure a conditional forwarder on VM1
- B. Add service endpoints on VNET1
- C. Add service endpoints on VNET2 and VNET3
- D. Configure peering between VNET1, VNET2, and VNET3 Most Voted

[Hide Solution](#)

[Discussion](#) 34

Correct Answer: D 🎉

You have an Azure subscription that contains the Azure virtual machines shown in the following table.

| Name | Connected to subnet |
|------|---------------------|
| VM1  | 172.16.1.0/24       |
| VM2  | 172.16.2.0/24       |

You add inbound security rules to a network security group (NSG) named NSG1 as shown in the following table.

| Priority | Source        | Destination   | Protocol | Port | Action |
|----------|---------------|---------------|----------|------|--------|
| 100      | 172.16.1.0/24 | 172.16.2.0/24 | TCP      | Any  | Allow  |
| 101      | Any           | 172.16.2.0/24 | TCP      | Any  | Deny   |

You run Azure Network Watcher as shown in the following exhibit.

Resource group \*

RG1 ✓

Source type \*

Virtual machine ▾

\* Virtual machine

VM1 ▾

Destination

Select a virtual machine  Specify manually

Resource group \*

RG1 ✓

Virtual machine \* ⓘ

VM2 ▾

Probe Settings

Protocol ⓘ

TCP  ICMP

Destination port \* ⓘ

8080 ▾

---

Advanced settings

**Check**

Status

⚠️ Unreachable

Agent extension version  
1.4

Source virtual machine  
VM1

You run Network Watcher again as shown in the following exhibit.

Source type \*

Virtual machine

\* Virtual machine

VM1

Destination

Select a virtual machine  Specify manually

Resource group \*

RG1

Virtual machine \* ⓘ

VM2

Probe Settings

Protocol ⓘ

TCP  ICMP

**Check**

Status

Reachable

Agent extension version  
1.4

Source virtual machine  
[VM1](#)

[Grid view](#) [Topology view](#)

Hops

| NAME | IP ADDRESS | STATUS                               | NEXT HOP IP ADDRESS | RTT FROM SOURCE (... |
|------|------------|--------------------------------------|---------------------|----------------------|
| VM1  | 172.16.1.4 | <span style="color: green;">✓</span> | 172.16.2.4          | 0                    |
| VM2  | 172.16.2.4 | <span style="color: green;">✓</span> | -                   | -                    |

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

### Answer Area

| Statements                                      | Yes                              | No                               |
|---|----------------------------------|----------------------------------|
| NSG1 limits VM1 traffic                         | <input type="radio"/>            | <input checked="" type="radio"/> |
| NSG1 applies to VM2                             | <input checked="" type="radio"/> | <input type="radio"/>            |
| VM1 and VM2 connect to the same virtual network | <input checked="" type="radio"/> | <input type="radio"/>            |

Box 1: No

NSG1 limits the traffic that is flowing into 172.16.2.0/24 (Subnet2), which host VM2.

Box 2: Yes

Since Network Watcher is showing that traffic from VM1 to VM2 is not reaching on the TCP port, that means that NSG1 is applied to VM2. We can understand for sure, that it is not applied to VM1.

Box 3: Yes

In Network Watcher, you can see that the next hop is the destination VM2. This means that they are part of the same virtual network.

#### Question #39

Topic 5

You have the Azure virtual network named VNet1 that contains a subnet named Subnet1. Subnet1 contains three Azure virtual machines. Each virtual machine has a public IP address.

The virtual machines host several applications that are accessible over port 443 to users on the Internet.

Your on-premises network has a site-to-site VPN connection to VNet1.

You discover that the virtual machines can be accessed by using the Remote Desktop Protocol (RDP) from the Internet and from the on-premises network.

You need to prevent RDP access to the virtual machines from the Internet, unless the RDP connection is established from the on-premises network. The solution must ensure that all the applications can still be accessed by the Internet users.

What should you do?

- A. Modify the address space of the local network gateway
- B. Create a deny rule in a network security group (NSG) that is linked to Subnet1 Most Voted
- C. Remove the public IP addresses from the virtual machines
- D. Modify the address space of Subnet1

[Hide Solution](#)

[Discussion 32](#)

Correct Answer: B 

You have an Azure subscription named Subscription1 that contains an Azure virtual network named VNet1. VNet1 connects to your on-premises network by using Azure ExpressRoute.

You plan to prepare the environment for automatic failover in case of ExpressRoute failure.

You need to connect VNet1 to the on-premises network by using a site-to-site VPN. The solution must minimize cost.

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

NOTE: Each correct selection is worth one point.

A. Create a connection Most Voted

B. Create a local site VPN gateway Most Voted

C. Create a VPN gateway that uses the VpnGw1 SKU Most Voted

D. Create a gateway subnet

E. Create a VPN gateway that uses the Basic SKU

VNet1 is already connected by ExpressRoute, which we presume that the subnet gateway was already created. SKU need to be VpnGw1 because Basic does not coexist with ExpressRoute.

So, answers should be A, B and C.

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

| Name | Type                      |
|------|---------------------------|
| VM1  | Virtual machine           |
| VM2  | Virtual machine           |
| LB1  | Load balancer (Basic SKU) |

You install the Web Server role (IIS) on VM1 and VM2, and then add VM1 and VM2 to LB1. LB1 is configured as shown in the LB1 exhibit. (Click the LB1 tab.)

#### Essentials ^

|   |   |
|---|---|
| Resource group ( <a href="#">change</a> )<br><b>VMRG</b>          | Backend pool<br>Backend1 (2 virtual machines)<br>Health probe<br>Probe1(HTTP:80/Probe1.htm) |
| Location<br><b>West Europe</b>                                    | Load balancing rule<br>Rule1 (TCP/80)<br>NAT rules<br>-                                     |
| Subscription name ( <a href="#">change</a> )<br><b>Azure Pass</b> | Public IP address<br><b>104.40.178.194 (LB1)</b>  |
| Subscription ID<br><b>e65d2b22-fde8</b>                           |   |
| SKU<br><b>Basic</b>   |   |

Rule1 is configured as shown in the Rule1 exhibit. (Click the Rule1 tab.)

\* Name

\* IP Version  
 IPv4  IPv6

\* Frontend IP address ⓘ

Protocol  
 TCP  UDP

\* Port

\* Backend port ⓘ

Backend pool ⓘ

Health probe ⓘ

Session persistence ⓘ

Idle timeout (minutes) ⓘ  
 4

Floating IP (direct server return) ⓘ  
Disabled

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

NOTE: Each correct selection is worth one point.

## Answer Area

| Statements  | Yes                              | No                               |
|---|----------------------------------|----------------------------------|
| VM1 is in the same availability set as VM2.   | <input checked="" type="radio"/> | <input type="radio"/>            |
| If Probe1.htm is present on VM1 and VM2, LB1 will balance TCP port 80 between VM1 and VM2.    | <input checked="" type="radio"/> | <input type="radio"/>            |
| If you delete Rule1, LB1 will balance all the requests between VM1 and VM2 for all the ports. | <input type="radio"/>            | <input checked="" type="radio"/> |

Box 1: Yes

A Basic Load Balancer supports virtual machines in a single availability set or virtual machine scale set.

Box 2: Yes

When using load-balancing rules with Azure Load Balancer, you need to specify health probes to allow Load Balancer to detect the backend endpoint status. The configuration of the health probe and probe responses determine which backend pool instances will receive new flows. You can use health probes to detect the failure of an application on a backend endpoint. You can also generate a custom response to a health probe and use the health probe for flow control to manage load or planned downtime. When a health probe fails, Load Balancer will stop sending new flows to the respective unhealthy instance. Outbound connectivity is not impacted, only inbound connectivity is impacted.

Box 3: No

There will be no load balancing between the VMs.

Basic Load Balancer: Virtual machines in a single availability set or virtual machine scale set.

Standard Load Balancer: Any virtual machines or virtual machine scale sets in a single virtual network.

You have an Azure virtual machine named VM1 that connects to a virtual network named VNet1. VM1 has the following configurations:

- Subnet: 10.0.0.0/24
- Availability set: AVSet
- Network security group (NSG): None
- Private IP address: 10.0.0.4 (dynamic)
- Public IP address: 40.90.219.6 (dynamic)

You deploy a standard, Internet-facing load balancer named slb1.

You need to configure slb1 to allow connectivity to VM1.

Which changes should you apply to VM1 as you configure slb1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

Before you create a backend pool on slb1, you must:

- Create and assign an NSG to VM1
- Remove the public IP address from VM1
- Change the private IP address of VM1 to static

Before you can connect to VM1 from slb1, you must:

- Create and configure an NSG
- Remove the public IP address from VM1
- Change the private IP address of VM1 to static

Box 1: Remove the public IP address from VM1

Note: A public load balancer can provide outbound connections for virtual machines (VMs) inside your virtual network. These connections are accomplished by translating their private IP addresses to public IP addresses. Public Load Balancers are used to load balance internet traffic to your VMs. Load balancer and the public IP address SKU must match when you use them with public IP addresses. Only Basic SKU IPs work with the Basic SKU load balancer and only Standard SKU IPs work with Standard SKU load balancers.

Box 2: Create and configure an NSG

NSGs are used to explicitly permit allowed traffic. If you do not have an NSG on a subnet or NIC of your virtual machine resource, traffic is not allowed to reach this resource.

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

| Name  | Type              | Location     |
|-------|-------------------|--------------|
| VNET1 | Virtual network   | East US      |
| IP1   | Public IP address | West Europe  |
| RT1   | Route table       | North Europe |

You need to create a network interface named NIC1.

In which location can you create NIC1?

- A. East US and North Europe only
- B. East US only **Most Voted**
- C. East US, West Europe, and North Europe
- D. East US and West Europe only

[Hide Solution](#)

[Discussion](#) 16

**Correct Answer:** B 🎉

Before creating a network interface, you must have an existing virtual network in the same location and subscription you create a network interface in.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface>

*Community vote distribution*

B (100%)

You have Azure virtual machines that run Windows Server 2019 and are configured as shown in the following table.

| Name | Virtual network name | DNS suffix configured in Windows Server |
|------|----------------------|---|
| VM1  | VNET1                | Contoso.com                             |
| VM2  | VNET2                | Contoso.com                             |

You create a public Azure DNS zone named adatum.com and a private Azure DNS zone named contoso.com. For contoso.com, you create a virtual network link named link1 as shown in the exhibit. (Click the Exhibit tab.)

**link1**  
contoso.com

Save

Link name  
link1

Link state  
Completed

Provisioning state  
Succeeded

Virtual network details

Virtual network id  
</subscriptions/8372f433-2dcd-4361-b5ef-5b188fed87d0/resourceGroups/RG2/provi...>

Virtual network  
VNET1

Configuration  
 Enable auto registration

You discover that VM1 can resolve names in contoso.com but cannot resolve names in adatum.com. VM1 can resolve other hosts on the Internet.

You need to ensure that VM1 can resolve host names in adatum.com.

What should you do?

- A. Update the DNS suffix on VM1 to be adatum.com
- B. Configure the name servers for adatum.com at the domain registrar **Most Voted**
- C. Create an SRV record in the contoso.com zone
- D. Modify the Access control (IAM) settings for link1

[Hide Solution](#)

[Discussion](#) 31

**Correct Answer:** A 

If you use Azure Provided DNS then appropriate DNS suffix will be automatically applied to your virtual machines. For all other options you must either use Fully Qualified Domain Names (FQDN) or manually apply appropriate DNS suffix to your virtual machines.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-name-resolution-for-vms-and-role-instances>

*Community vote distribution*

**B (100%)**

You plan to use Azure Network Watcher to perform the following tasks:

☞ Task1: Identify a security rule that prevents a network packet from reaching an Azure virtual machine.

☞ Task2: Validate outbound connectivity from an Azure virtual machine to an external host.

Which feature should you use for each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

Task1:

|                     |
|---------------------|
| IP flow verify      |
| Next hop            |
| Packet capture      |
| Security group view |
| Traffic Analytics   |

Task2:

|                         |
|-------------------------|
| Connection troubleshoot |
| IP flow verify          |
| Next hop                |
| NSG flow logs           |
| Traffic Analytics       |

Box 1: IP flow verify

At some point, a VM may become unable to communicate with other resources, because of a security rule. The IP flow verify capability enables you to specify a source and destination IPv4 address, port, protocol (TCP or UDP), and traffic direction (inbound or outbound). IP flow verify then tests the communication and informs you if the connection succeeds or fails. If the connection fails, IP flow verify tells you which.

Box 2: Connection troubleshoot

Diagnose outbound connections from a VM: The connection troubleshoot capability enables you to test a connection between a VM and another VM, an FQDN, a URI, or an IPv4 address. The test returns similar information returned when using the connection monitor capability, but tests the connection at a point in time, rather than monitoring it over time, as connection monitor does. Learn more about how to troubleshoot connections using connection-troubleshoot.

You have an Azure subscription that contains the Azure virtual machines shown in the following table.

| Name | Operating system             | Subnet  | Virtual network |
|------|------------------------------|---------|-----------------|
| VM1  | Windows Server 2019          | Subnet1 | VNET1           |
| VM2  | Windows Server 2019          | Subnet2 | VNET1           |
| VM3  | Red Hat Enterprise Linux 7.7 | Subnet3 | VNET1           |

You configure the network interfaces of the virtual machines to use the settings shown in the following table.

| Name | DNS server    |
|------|---------------|
| VM1  | None          |
| VM2  | 192.168.10.15 |
| VM3  | 192.168.10.15 |

From the settings of VNET1 you configure the DNS servers shown in the following exhibit.

DNS servers ⓘ

Default (Azure-provided)

Custom

193.77.134.10 ...

Add DNS ser ...

The virtual machines can successfully connect to the DNS server that has an IP address of 192.168.10.15 and the DNS server that has an IP address of 193.77.134.10.

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

## Answer Area

| Statements                                     | Yes                              | No                               |
|--|----------------------------------|----------------------------------|
| VM1 connects to 193.77.134.10 for DNS queries. | <input checked="" type="radio"/> | <input type="radio"/>            |
| VM2 connects to 193.77.134.10 for DNS queries. | <input type="radio"/>            | <input checked="" type="radio"/> |
| VM3 connects to 192.168.10.15 for DNS queries. | <input checked="" type="radio"/> | <input type="radio"/>            |

NIC configured DNS servers takes precedence over VNET configured DNS servers.

Box 1: Yes

VM1 uses the VNET configured DNS 193.77.134.10. You can specify DNS server IP addresses in the VNet settings. The setting is applied as the default DNS server(s) for all VMs in the VNet. The DNS is set on the VNET level.

Box 2: No

VM2 uses the NIC configured DNS 192.168.10.15. You can set DNS servers per VM or cloud service to override the default network settings. This VM has 192.168.10.5 set as DNS server, so it overrides the default DNS set on VNET1.

Box 3: Yes

VM3 uses the NIC configured DNS 192.168.10.15. You can set DNS servers per VM or cloud service to override the default network settings. This VM has 192.168.10.5 set as DNS server, so it overrides the default DNS set on VNET1.

You have an Azure subscription that contains the resource groups shown in the following table.

| Name | Lock name | Lock type |
|------|-----------|-----------|
| RG1  | None      | None      |
| RG2  | Lock      | Delete    |

RG1 contains the resources shown in the following table.

| Name     | Type              | Lock name | Lock type |
|----------|-------------------|-----------|-----------|
| storage2 | Storage account   | Lock1     | Delete    |
| VNET2    | Virtual network   | Lock2     | Read-only |
| IP2      | Public IP address | None      | None      |

You need to identify which resources you can move from RG1 to RG2, and which resources you can move from RG2 to RG1.

Which resources should you identify? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

## Answer Area

Resources that you can move from RG1 to RG2:

None  
IP1 only  
IP1 and storage1 only  
IP1 and VNET1 only  
IP1, VNET2, and storage1



Resources that you can move from RG2 to RG1:

None  
IP2 only  
IP2 and storage2 only  
IP2 and VNET2 only  
IP2, VNET2, and storage2



Box 1: IP1, VNET2, and storage1

Box 2: IP2, VNET2, and storage2

Locks are designed for any update or removal. In this case we want to move only, we are not deleting, and we are not changing anything in the resource.

RO or Delete locks does not have any impact for Move operation and it doesn't matter if it comes from RG level or are directly attached to the resource.

VNETS can be moved as well. Only limitation is VNET Peering needs to be disabled first. But this is not a case for this question.

#### Question #50

#### Topic 5

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

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

You have an Azure subscription that contains the virtual machines shown in the following table.

| Name | Public IP SKU | Connected to  | Status                |
|------|---------------|---------------|-----------------------|
| VM1  | None          | VNET1/Subnet1 | Stopped (deallocated) |
| VM2  | Basic         | VNET1/Subnet2 | Running               |

You deploy a load balancer that has the following configurations:

- Name: LB1
- Type: Internal
- SKU: Standard
- Virtual network: VNET1

You need to ensure that you can add VM1 and VM2 to the backend pool of LB1.

Solution: You create a Basic SKU public IP address, associate the address to the network interface of VM1, and then start VM1.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B** 

A Backend Pool configured by IP address has the following limitations:

- Standard load balancer only

Reference:

<https://docs.microsoft.com/en-us/azure/load-balancer/backend-pool-management>

*Community vote distribution*

**B (100%)**

Correct Answer: B – No

You can only attach virtual machines that are in the same location and on the same virtual network as the LB. Virtual machines must have a standard SKU public IP or no public IP.

The LB needs to be a standard SKU to accept individual VMs outside an availability set or vmss. VMs do not need to have public IPs but if they do have them they have to be standard SKU. VMs can only be from a single network. When they don't have a public IP they are assigned an ephemeral IP.

Also, when adding them to a backend pool, it doesn't matter in which status are the VMs.

Note: Load balancer and the public IP address SKU must match when you use them with public IP addresses.

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

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

You have an Azure subscription that contains the virtual machines shown in the following table.

| Name | Public IP SKU | Connected to  | Status                |
|------|---------------|---------------|-----------------------|
| VM1  | None          | VNET1/Subnet1 | Stopped (deallocated) |
| VM2  | Basic         | VNET1/Subnet2 | Running               |

You deploy a load balancer that has the following configurations:

- Name: LB1
- Type: Internal
- SKU: Standard
- Virtual network: VNET1

You need to ensure that you can add VM1 and VM2 to the backend pool of LB1.

Solution: You create two Standard SKU public IP addresses and associate a Standard SKU public IP address to the network interface of each virtual machine.

Does this meet the goal?

A. Yes **Most Voted**

B. No

[Hide Solution](#)

[Discussion 27](#)

**Correct Answer: A** 🎉

A Backend Pool configured by IP address has the following limitations:

- Standard load balancer only

Reference:

<https://docs.microsoft.com/en-us/azure/load-balancer/backend-pool-management>

*Community vote distribution*

A (88%)

13%

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

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

You have a computer named Computer1 that has a point-to-site VPN connection to an Azure virtual network named VNet1. The point-to-site connection uses a self-signed certificate.

From Azure, you download and install the VPN client configuration package on a computer named Computer2.

You need to ensure that you can establish a point-to-site VPN connection to VNet1 from Computer2.

Solution: You export the client certificate from Computer1 and install the certificate on Computer2.

Does this meet the goal?

A. Yes

B. No

[Hide Solution](#)

[Discussion 20](#)

**Correct Answer:** A 

Each client computer that connects to a VNet using Point-to-Site must have a client certificate installed. You generate a client certificate from the self-signed root certificate, and then export and install the client certificate. If the client certificate is not installed, authentication fails.

Reference:

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

*Community vote distribution*

 A (100%)

You have an Azure virtual machine named VM1.

The network interface for VM1 is configured as shown in the exhibit. (Click the Exhibit tab.)

**Network Interface: vm1175**    [Effective security rules](#)    [Topology](#)    [Virtual network/subnet: RG5-vnet/default](#)    [Public IP: 40.127.109.108](#)    [Private IP: 172.16.1.4](#)    [Accelerated networking: Disabled](#)

#### APPLICATION SECURITY GROUPS [Edit](#)

[Configure the application security groups](#)

#### INBOUND PORT RULES [Edit](#)

**Network security group VM1-nsg (attached to network interface: vm1175)**  
Impacts 0 subnets, 1 network interfaces

[Add inbound port rule](#)

| PRIORITY | NAME                          | PORT           | PROTOCOL | SOURCE          | DESTINATION    | ACTION | ... |
|----------|-------------------------------|----------------|----------|-----------------|----------------|--------|-----|
| 300      | ⚠️ RDP                        | 3389           | TCP      | Any             | Any            | Allow  | ... |
| 400      | ⚠️ Rule1                      | 80             | TCP      | Any             | Any            | Deny   | ... |
| 500      | Rule2                         | 80,443         | TCP      | Any             | Any            | Deny   | ... |
| 1000     | Rule4                         | 50-100,400-500 | UDP      | Any             | Any            | Allow  | ... |
| 2000     | Rule5                         | 50-5000        | Any      | Any             | VirtualNetwork | Deny   | ... |
| 3000     | Rule6                         | 150-300        | Any      | Any             | Any            | Allow  | ... |
| 4000     | Rule3                         | 60-500         | Any      | Any             | VirtualNetwork | Allow  | ... |
| 65000    | AllowVnetInBound              | Any            | Any      | VirtualNetwork  | VirtualNetwork | Allow  | ... |
| 65001    | AllowAzureLoadBalancerInBo... | Any            | Any      | AzureLoadBal... | Any            | Allow  | ... |
| 65500    | DenyAllInBound                | Any            | Any      | Any             | Any            | Deny   | ... |

You deploy a web server on VM1, and then create a secure website that is accessible by using the HTTPS protocol. VM1 is used as a web server only.

You need to ensure that users can connect to the website from the Internet.

What should you do?

- A. Modify the protocol of Rule4
- B. Delete Rule1
- C. For Rule5, change the Action to Allow and change the priority to 401 Most Voted
- D. Create a new inbound rule that allows TCP protocol 443 and configure the rule to have a priority of 501.

[Hide Solution](#)

[Discussion](#) 39

Correct Answer: C 

HTTPS uses port 443.

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

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

You have an Azure subscription that contains 10 virtual networks. The virtual networks are hosted in separate resource groups.

Another administrator plans to create several network security groups (NSGs) in the subscription.

You need to ensure that when an NSG is created, it automatically blocks TCP port 8080 between the virtual networks.

Solution: From the Resource providers blade, you unregister the Microsoft.ClassicNetwork provider.

Does this meet the goal?

A. Yes

B. No

[Hide Solution](#)

[Discussion 15](#)

**Correct Answer:** **B** 

You should use a policy definition.

Resource policy definition used by Azure Policy enables you to establish conventions for resources in your organization by describing when the policy is enforced and what effect to take. By defining conventions, you can control costs and more easily manage your resources.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-policy/policy-definition>

*Community vote distribution*

t-us

B (100%)

Correct Answer: B – No

You need to use a custom policy definition, because there is not a built-in policy.

Resource policy definition used by Azure Policy enables you to establish conventions for resources in your organization by describing when the policy is enforced and what effect to take. By defining conventions, you can control costs and more easily manage your resources.

You manage two Azure subscriptions named Subscription1 and Subscription2.

Subscription1 has following virtual networks:

| Name  | Address space | Location    |
|-------|---------------|-------------|
| VNET1 | 10.10.10.0/24 | West Europe |
| VNET2 | 172.16.0.0/16 | West US     |

The virtual networks contain the following subnets:

| Name     | Address space   | In virtual network |
|----------|-----------------|--------------------|
| Subnet11 | 10.10.10.0/24   | VNET1              |
| Subnet21 | 172.16.0.0/18   | VNET2              |
| Subnet22 | 172.16.128.0/18 | VNET2              |

Subscription2 contains the following virtual network:

- ⇒ Name: VNETA
- ⇒ Address space: 10.10.128.0/17
- ⇒ Location: Canada Central

VNETA contains the following subnets:

| Name     | Address space  |
|----------|----------------|
| SubnetA1 | 10.10.130.0/24 |
| SubnetA2 | 10.10.131.0/24 |

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

### Answer Area

| Statements  | Yes                              | No                               |
|---|----------------------------------|----------------------------------|
| A Site-to-Site connection can be established between VNET1 and VNET2. | <input type="radio"/>            | <input checked="" type="radio"/> |
| VNET1 and VNET2 can be peered.  | <input checked="" type="radio"/> | <input type="radio"/>            |
| VNET1 and VNETA can be peered.  | <input checked="" type="radio"/> | <input type="radio"/>            |

Correct Answer:

VNET1: 10.10.10.0 - 10.10.10.255

VNET2: 172.16.0.0 - 172.16.255.255

VNETA: 10.10.128.0 - 10.10.255.255

Box 1: No

To create a VNet to VNet VPN you need to have a special Gateway Subnet. Here, the VNet has no sufficient address space to create a Gateway Subnet and thus to establish a VNet to VNet VPN connection.

Here the VNet has only /24 CIDR blocks of address space and this space is already taken by its Subnet11.

Box 2: Yes

For VNet peering the only consideration is that the VNets do not overlap. VNET1 and VNET2 do not overlap.

Box 3: Yes

For VNet peering the only consideration is that the VNets do not overlap. VNET1 and VNETA do not overlap.

#### Question #5

#### Topic 5

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

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

You have an app named App1 that is installed on two Azure virtual machines named VM1 and VM2. Connections to App1 are managed by using an Azure Load Balancer.

The effective network security configurations for VM2 are shown in the following exhibit.

The screenshot shows the Azure portal interface for managing network settings. On the left, there's a sidebar with options like Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. Under Settings, Networking is selected. The main pane shows the 'VM2 - Networking' page for a virtual machine. At the top, there are buttons for Attach network interface and Detach network interface. Below that, a section for 'Network Interface: VM2-NIC1' shows details: Virtual network/subnet: Vnet1/Subnet11, NIC Public IP: -, NIC Private IP: 10.240.11.5, Accelerated networking: Disabled. There are tabs for Effective security rules and Topology. Under Inbound port rules, it says 'Impacts 1 subnets, 0 network interfaces'. A table lists the rules:

| Priority | Name                          | Port | Protocol | Source            | Destination    | Action             | ... |
|----------|-------------------------------|------|----------|-------------------|----------------|--------------------|-----|
| 100      | Allow_131.107.100.50          | 443  | TCP      | 131.107.100.50    | VirtualNetwork | <span>Allow</span> | ... |
| 200      | BlockAllOther443              | 443  | Any      | Any               | Any            | <span>Deny</span>  | ... |
| 65000    | AllowVnetInBound              | Any  | Any      | VirtualNetwork    | VirtualNetwork | <span>Allow</span> | ... |
| 65001    | AllowAzureLoadBalancerInBound | Any  | Any      | AzureLoadBalancer | Any            | <span>Allow</span> | ... |
| 65500    | DenyAllInBound                | Any  | Any      | Any               | Any            | <span>Deny</span>  | ... |

You discover that connections to App1 from 131.107.100.50 over TCP port 443 fail.

You verify that the Load Balancer rules are configured correctly.

You need to ensure that connections to App1 can be established successfully from 131.107.100.50 over TCP port 443.

Solution: You create an inbound security rule that denies all traffic from the 131.107.100.50 source and has a cost of 64999.

Does this meet the goal?

A. Yes

B. No

[Hide Solution](#)

[Discussion 24](#)

**Correct Answer:** *B* 

Reference:

<https://fastreroute.com/azure-network-security-groups-explained/>

*Community vote distribution*

 B (100%)

Correct Answer: B – No

You want to establish a successful connection from 131.107.100.50 over TCP port 43, and the solution suggests to create a deny inbound rule with low priority. It doesn't make any sense.

Virtual machines in load-balanced pools: The source port and address range applied are from the originating computer, not the load balancer. The destination port and address range are for the destination computer, not the load balancer.

AllowAzureLoadBalancerInBound: The AzureLoadBalancer service tag translates to the virtual IP address of the host, 168.63.129.16 where the Azure health probe originates. Actual traffic does not travel through here, and if you don't use Azure Load Balancing, this rule can be overridden.

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an app named App1 that is installed on two Azure virtual machines named VM1 and VM2. Connections to App1 are managed by using an Azure Load Balancer.

The effective network security configurations for VM2 are shown in the following exhibit.

Home > VM2 - Networking

## VM2 - Networking

Virtual machine

Search (Ctrl+I) Attach network interface Detach network interface

**Network Interface: VM2-NIC1 Effective security rules Topology**

Virtual network/subnet: Vnet1/Subnet11 NIC Public IP: - NIC Private IP: 10.240.11.5 Accelerated networking: Disabled

Inbound port rules Outbound port rules Application security groups Load balancing

Network security group NSG2 (attached to network interface: Subnet11)  
Impacts 1 subnets, 0 network interfaces Add inbound port rule

| Priority | Name                          | Port | Protocol | Source            | Destination    | Action             | ... |
|----------|-------------------------------|------|----------|-------------------|----------------|--------------------|-----|
| 100      | Allow_131.107.100.50          | 443  | TCP      | 131.107.100.50    | VirtualNetwork | <span>Allow</span> | ... |
| 200      | BlockAllOther443              | 443  | Any      | Any               | Any            | <span>Deny</span>  | ... |
| 65000    | AllowVnetInBound              | Any  | Any      | VirtualNetwork    | VirtualNetwork | <span>Allow</span> | ... |
| 65001    | AllowAzureLoadBalancerInBound | Any  | Any      | AzureLoadBalancer | Any            | <span>Allow</span> | ... |
| 65500    | DenyAllInBound                | Any  | Any      | Any               | Any            | <span>Deny</span>  | ... |

You discover that connections to App1 from 131.107.100.50 over TCP port 443 fail.

You verify that the Load Balancer rules are configured correctly.

You need to ensure that connections to App1 can be established successfully from 131.107.100.50 over TCP port 443.

Solution: You delete the BlockAllOther443 inbound security rule.

Does this meet the goal?

A. Yes Most Voted

B. No Most Voted

[Hide Solution](#)

[Discussion \(57\)](#)

**Correct Answer: B** 🎉

Reference:

<https://fastreroute.com/azure-network-security-groups-explained/>

Community vote distribution

B (61%)

A (39%)

Correct Answer: B - No

Allow\_131.107.100.50 rule has a higher priority (100) than BlockAllOther441 (200) and it allows inbound traffic over TCP 443 from source 131.107.100.50. App1 (VM1 and VM2) is in a VNet, so this rule applies. Unfortunately, we still cannot access App1, so the issue is somewhere else, maybe the VMs are off, or the firewall is blocking it.

#### Question #59

#### Topic 5

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

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

You have an app named App1 that is installed on two Azure virtual machines named VM1 and VM2. Connections to App1 are managed by using an Azure Load Balancer.

The effective network security configurations for VM2 are shown in the following exhibit.

Home > VM2 - Networking

**VM2 - Networking** Virtual machine

Search (Ctrl+ /)

Attach network interface Detach network interface

**Network Interface: VM2-NIC1 Effective security rules Topology**

Virtual network/subnet: Vnet1/Subnet1 NIC Public IP: - NIC Private IP: 10.240.11.5 Accelerated networking: Disabled

Inbound port rules Outbound port rules Application security groups Load balancing

Network security group NSG2 (attached to network interface: Subnet11)  
Impacts 1 subnets, 0 network interfaces

Add inbound port rule

| Priority | Name                          | Port | Protocol | Source            | Destination    | Action | ... |
|----------|-------------------------------|------|----------|-------------------|----------------|--------|-----|
| 100      | Allow_131.107.100.50          | 443  | TCP      | 131.107.100.50    | VirtualNetwork | Allow  | ... |
| 200      | BlockAllOther443              | 443  | Any      | Any               | Any            | Deny   | ... |
| 65000    | AllowVnetInBound              | Any  | Any      | VirtualNetwork    | VirtualNetwork | Allow  | ... |
| 65001    | AllowAzureLoadBalancerInBound | Any  | Any      | AzureLoadBalancer | Any            | Allow  | ... |
| 65500    | DenyAllInBound                | Any  | Any      | Any               | Any            | Deny   | ... |

You discover that connections to App1 from 131.107.100.50 over TCP port 443 fail.

You verify that the Load Balancer rules are configured correctly.

You need to ensure that connections to App1 can be established successfully from 131.107.100.50 over TCP port 443.

Solution: You modify the priority of the Allow\_131.107.100.50 inbound security rule.

Does this meet the goal?

A. Yes

B. No

[Hide Solution](#)

[Discussion \(18\)](#)

**Correct Answer:** B 🎉

The rule currently has the highest priority.

Reference:

<https://fastreroute.com/azure-network-security-groups-explained/>

Community vote distribution

B (75%)

A (25%)

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

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

You have an Azure subscription that contains 10 virtual networks. The virtual networks are hosted in separate resource groups.

Another administrator plans to create several network security groups (NSGs) in the subscription.

You need to ensure that when an NSG is created, it automatically blocks TCP port 8080 between the virtual networks.

Solution: You assign a built-in policy definition to the subscription.

Does this meet the goal?

A. Yes

B. No

[Hide Solution](#)

[Discussion 25](#)

**Correct Answer:** B 

Resource policy definition used by Azure Policy enables you to establish conventions for resources in your organization by describing when the policy is enforced and what effect to take. By defining conventions, you can control costs and more easily manage your resources.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-policy/policy-definition>

*Community vote distribution*

 B (100%)

There is no such built-in policy (yet), that is why we need a custom one.

You have an Azure subscription.

You plan to deploy an Azure Kubernetes Service (AKS) cluster to support an app named App1. On-premises clients connect to App1 by using the IP address of the pod.

For the AKS cluster, you need to choose a network type that will support App1.

What should you choose?

A. kubenet

B. Azure Container Networking Interface (CNI) Most Voted

C. Hybrid Connection endpoints

D. Azure Private Link

[Hide Solution](#)

[Discussion 18](#)

**Correct Answer:** B 

Answer is correct "B".

To have previously reserved IP address for a certain Pod, you should use Azure Container Networking Interface (CNI).

Nodes = Kubenet

Pods = CNI

You have an Azure subscription that contains the virtual machines shown in the following table.

| Name | Public IP SKU | Connected to  | Status                |
|------|---------------|---------------|-----------------------|
| VM1  | None          | VNET1/Subnet1 | Stopped (deallocated) |
| VM2  | Basic         | VNET1/Subnet2 | Running               |

You deploy a load balancer that has the following configurations:

- Name: LB1
- Type: Internal
- SKU: Standard
- Virtual network: VNET1

You need to ensure that you can add VM1 and VM2 to the backend pool of LB1.

Solution: You disassociate the public IP address from the network interface of VM2.

Does this meet the goal?

A. Yes Most Voted

B. No

[Hide Solution](#)

[Discussion 40](#)

**Correct Answer: B** 🎉

*Community vote distribution*

A (100%)

You have an Azure subscription that contains 10 virtual networks. The virtual networks are hosted in separate resource groups.

Another administrator plans to create several network security groups (NSGs) in the subscription. You need to ensure that when an NSG is created, it automatically blocks TCP port 8080 between the virtual networks.

Solution: You configure a custom policy definition, and then you assign the policy to the subscription.

Does this meet the goal?

A. Yes

B. No

[Hide Solution](#)

[Discussion 12](#)

**Correct Answer:** A 

Resource policy definition used by Azure Policy enables you to establish conventions for resources in your organization by describing when the policy is enforced and what effect to take. By defining conventions, you can control costs and more easily manage your resources.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-policy/policy-definition>

*Community vote distribution*

A (100%)

You have two Azure virtual networks named VNet1 and VNet2. VNet1 contains an Azure virtual machine named VM1. VNet2 contains an Azure virtual machine named VM2.

VM1 hosts a frontend application that connects to VM2 to retrieve data.

Users report that the frontend application is slower than usual.

You need to view the average round-trip time (RTT) of the packets from VM1 to VM2.

Which Azure Network Watcher feature should you use?

A. IP flow verify

B. Connection troubleshoot

C. Connection monitor **Most Voted**

D. NSG flow logs

[Hide Solution](#)

[Discussion 30](#)

**Correct Answer:** C 

You have an Azure subscription that contains the public load balancers shown in the following table.

| Name | SKU      |
|------|----------|
| LB1  | Basic    |
| LB2  | Standard |

You plan to create six virtual machines and to load balance requests to the virtual machines. Each load balancer will load balance three virtual machines.

You need to create the virtual machines for the planned solution.

How should you create the virtual machines? To answer, select the appropriate options in the answer area.

### Answer Area

The virtual machines that will be load balanced by using LB1 must:

- be connected to the same virtual network
- be created in the same resource group
- be created in the same availability set or virtual machine scale set
- run the same operating system

The virtual machines that will be load balanced by using LB2 must:

- be connected to the same virtual network
- be created in the same resource group
- be created in the same availability set or virtual machine scale set
- run the same operating system

Correct:

Standard SKU: any virtual machines or virtual machine scale sets in a single virtual network.

Basic SKU: Virtual machines in a single availability set or virtual machine scale set.

[<https://docs.microsoft.com/en-us/azure/load-balancer/skus>](https://docs.microsoft.com/en-us/azure/load-balancer/skus)

You have an on-premises data center and an Azure subscription. The data center contains two VPN devices. The subscription contains an Azure virtual network named VNet1. VNet1 contains a gateway subnet.

You need to create a site-to-site VPN. The solution must ensure that if a single instance of an Azure VPN gateway fails, or a single on-premises VPN device fails, the failure will not cause an interruption that is longer than two minutes.

What is the minimum number of public IP addresses, virtual network gateways, and local network gateways required in Azure? To answer, select the appropriate options in the answer area.

## Answer Area

Public IP addresses:

|   |
|---|
| 1 |
| 2 |
| 3 |
| 4 |



Virtual network gateways:

|   |
|---|
| 1 |
| 2 |
| 3 |
| 4 |



Local network gateways:

|   |
|---|
| 1 |
| 2 |
| 3 |
| 4 |



Every Azure VPN gateway consists of two instances in an active-standby configuration. For any planned maintenance or unplanned disruption that happens to the active instance, the standby instance would take over (failover) automatically, and resume the S2S VPN or VNet-to-VNet connections. The switch over will cause a brief interruption. For planned maintenance, the connectivity should be restored within 10 to 15 seconds. For unplanned issues, the connection recovery will be longer, about 1 to 3 minutes in the worst case. For P2S VPN client connections to the gateway, the P2S connections will be disconnected and the users will need to reconnect from the client machines.

<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-highlyavailable>

## 2-1-2:

2 Public IP addresses (each Azure VPN gateway spawns 2 VPN endpoints, each with its own IP  
1 Single Azure VPN gateway is redundant by default

2 on-premise VPN devices are mentioned, and single local network gateway can only be set up with a SINGLE ip for on-premise VPN device, two local network gateway are needed for redundancy.

### Question #67

### Topic 5

You have an Azure subscription that contains two virtual machines as shown in the following table.

| Name | Operating system    | Location    | IP address | DNS server               |
|------|---------------------|-------------|------------|--------------------------|
| VM1  | Windows Server 2019 | West Europe | 10.0.0.4   | Default (Azure-provided) |
| VM2  | Windows Server 2019 | West Europe | 10.0.0.5   | Default (Azure-provided) |

You perform a reverse DNS lookup for 10.0.0.4 from VM2.

Which FQDN will be returned?

A. vm1.core.windows.net

B. vm1.azure.com

C. vm1.westeurope.cloudapp.azure.com

D. vm1.internal.cloudapp.net **Most Voted**

[Hide Solution](#)

[Discussion 56](#)

**Correct Answer: B** 🎉

*Community vote distribution*

D (100%)

You have an app named App1 that is installed on two Azure virtual machines named VM1 and VM2. Connections to App1 are managed by using an Azure Load Balancer.

The effective network security configurations for VM2 are shown in the following exhibit.

**Network Interface: VM2-NIC1 Effective security rules Topology**

Virtual network/subnet: Vnet1/Subnet11 NIC Public IP: - NIC Private IP: 10.240.11.5 Accelerated networking: Disabled

Inbound port rules Outbound port rules Application security groups Load balancing

Network security group NSG2 (attached to network interface: Subnet11) Impacts 1 subnets, 0 network interfaces Add inbound port rule

| Priority | Name                          | Port | Protocol | Source            | Destination    | Action                                   |
|----------|-------------------------------|------|----------|-------------------|----------------|--|
| 100      | Allow_131.107.100.50          | 443  | TCP      | 131.107.100.50    | VirtualNetwork | <span style="color: green;">Allow</span> |
| 200      | BlockAllOther443              | 443  | Any      | Any               | Any            | <span style="color: red;">Deny</span>    |
| 65000    | AllowVnetInBound              | Any  | Any      | VirtualNetwork    | VirtualNetwork | <span style="color: green;">Allow</span> |
| 65001    | AllowAzureLoadBalancerInBound | Any  | Any      | AzureLoadBalancer | Any            | <span style="color: green;">Allow</span> |
| 65500    | DenyAllInBound                | Any  | Any      | Any               | Any            | <span style="color: red;">Deny</span>    |

You discover that connections to App1 from 131.107.100.50 over TCP port 443 fail.

You verify that the Load Balancer rules are configured correctly.

You need to ensure that connections to App1 can be established successfully from 131.107.100.50 over TCP port 443.

Solution: You create an inbound security rule that allows any traffic from the AzureLoadBalancer source and has a cost of 150.

Does this meet the goal?

A. Yes Most Voted

B. No Most Voted

[Hide Solution](#)

[Discussion \(80\)](#)

**Correct Answer: A**

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview>

Community vote distribution

B (50%)

A (50%)

The rule with priority 200 blocks all inbound traffic. This involves the Azure Load Balancer health probe directed to the VM. That results in VM2 being considered unhealthy and the LB does not route traffic to it (hence the issue). By placing a rule with the priority 150 that allows the AzureLoadBalancer traffic tag, VM2 is discovered as functional/healthy, the LB directs traffic to it => problem solved.

Agree, the NSG is attached to subnet as can be seen in exhibit, hence either of the VMs are unhealthy for the LB due to rule 200.

The new rule priority 150 will be placed on position 2 so LB HC will be ok so flow OK response -->A: yes

Question #69

Topic 5

You have an Azure subscription that contains a policy-based virtual network gateway named GW1 and a virtual network named VNet1.

You need to ensure that you can configure a point-to-site connection from an on-premises computer to VNet1.

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

NOTE: Each correct selection is worth one point.

- A. Add a service endpoint to VNet1
- B. Reset GW1
- C. Create a route-based virtual network gateway **Most Voted**
- D. Add a connection to GW1
- E. Delete GW1 **Most Voted**
- F. Add a public IP address space to VNet1

[Hide Solution](#)

[Discussion](#) 42

Correct Answer: CE 🏆

Answer in proper order: E, C

Point to site is only supported by route-based VPN gateway.

Policy-based VPN: (IKEv1): 1 S2S/connection tunnel; no P2S

Yes Delete Existing GW and create new route-based GW

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

| Name  | Type                               |
|-------|------------------------------------|
| VMRG  | Resource group                     |
| VNet1 | Virtual network                    |
| VNet2 | Virtual network                    |
| VM5   | Virtual machine connected to VNet1 |
| VM6   | Virtual machine connected to VNet2 |

In Azure, you create a private DNS zone named adatum.com. You set the registration virtual network to VNet2. The adatum.com zone is configured as shown in the following exhibit:

|   |  |            |   |
|---|--|------------|---|
| Resource group ( <a href="#">change</a> )<br><a href="#">vmrg</a>         | Name server 1<br>-                       |            |   |
| Subscription ( <a href="#">change</a> )<br><a href="#">Azure Pass</a>     | Name server 2<br>-                       |            |   |
| Subscription ID<br>a4fde29b-d56a-4f6c-8298-6c53cd0b720c                   | Name server 3<br>-<br>Name server 4<br>- |            |   |
| Tags ( <a href="#">change</a> )<br><a href="#">Click here to add tags</a> |  |            |   |
| <hr/>   |  |            |   |
| <input type="text"/> Search record sets                                   |  |            |   |
| <b>Name</b>   | <b>Type</b>                              | <b>TTL</b> | <b>VALUE</b>  |
| @   | SOA                                      | 3600       | Email: azuredns-hostmaster.microsoft.com<br>Host: internal.cloudapp.net<br>Refresh: 3600<br>Retry: 300<br>Expire: 2419200<br>Minimum TTL: 300<br>Serial number: 1 |
| vm1   | A  | 3600       | 10.1.0.4  |
| vm9   | A  | 3600       | 10.1.0.12   |

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

NOTE: Each correct selection is worth one point.

## Answer Area

| Statements  | Yes                              | No                               |
|---|----------------------------------|----------------------------------|
| The A record for VM5 will be registered automatically in the adatum.com zone. | <input type="radio"/>            | <input checked="" type="radio"/> |
| VM5 can resolve VM9.adatum.com.   | <input type="radio"/>            | <input checked="" type="radio"/> |
| VM6 can resolve VM9.adatum.com.   | <input checked="" type="radio"/> | <input type="radio"/>            |

Agreed, there is no mention of VNet peering, thus we can assume the two VNet's is not connected.

1. VM5 is in VNet1 - answer is NO.

2. VM5 is in VNet1 - answer is NO.

3. VM6 is in VNet2 - answer is YES.

VNet2 which is linked to the private DNS zone.

You have an Azure subscription that contains the virtual networks shown in the following table.

| Name  | Location |
|-------|----------|
| VNET1 | West US  |
| VNET2 | West US  |
| VNET3 | East US  |

The subscription contains the private DNS zones shown in the following table.

| Name      | Location |
|-----------|----------|
| Zone1.com | West US  |
| Zone2.com | West US  |
| Zone3.com | East US  |

You add virtual network links to the private DNS zones as shown in the following table.

| Name  | Private DNS zone | Virtual network | Enable auto registration |
|-------|------------------|-----------------|--------------------------|
| Link1 | Zone1.com        | VNET1           | Yes                      |
| Link2 | Zone2.com        | VNET2           | No                       |
| Link3 | Zone3.com        | VNET3           | No                       |

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

## Answer Area

| Statements  | Yes                   | No                    |
|---|-----------------------|-----------------------|
| You can enable auto registration for Link2.   | <input type="radio"/> | <input type="radio"/> |
| You can add a virtual network link for VNET1 to Zone3.com.                              | <input type="radio"/> | <input type="radio"/> |
| You can add a virtual network link for VNET2 to Zone1.com and enable auto registration. | <input type="radio"/> | <input type="radio"/> |

A virtual network can be linked to private DNS zone as a registration or as a resolution virtual network.

Registration virtual network:

A private DNS zone can have multiple registration virtual networks. However, every virtual network can only have one registration zone associated with it.

Resolution virtual network:

One private DNS zone can have multiple resolution virtual networks and a virtual network can have multiple resolution zones associated to it.

1. Yes

No registration zone for VNET2.

2. Yes

A virtual network can have multiple resolution zones associated to it.

3. Yes

No registration zone for VNET2.

You have an Azure subscription.

You plan to use an Azure Resource Manager template to deploy a virtual network named VNET1 that will use Azure Bastion.

How should you complete the template? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

```
{  
  "type": "Microsoft.Network/virtualNetworks",  
  "name": "VNET1",  
  "apiVersion": "2019-02-01",  
  "location": "[resourceGroup().location]",  
  "properties": {  
    "addressSpace": {  
      "addressPrefixes": ["10.10.10.0/24"]  
    },  
    "subnets": [  
      {  
        "name": : 

|                     |
|---------------------|
| AzureBastionSubnet  |
| AzureFirewallSubnet |
| LAN01               |
| RemoteAccessSubnet  |

  
        "properties": {  
          "addressPrefix": : 

|               |
|---------------|
| 10.10.10.0/27 |
| 10.10.10.0/29 |
| 10.10.10.0/30 |

  
        }  
      },  
      {  
        "name": "LAN02",  
        "properties": {  
          "addressPrefix": "10.10.10.128/25"  
        }  
      }  
    ]  
  }  
}
```

Correct. Have just gone to create a new Bastion resource in my lab. This info message is given: To associate a virtual network with a Bastion, it must contain a subnet with name AzureBastionSubnet and a prefix of at least /26.

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

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

You manage a virtual network named VNet1 that is hosted in the West US Azure region.

VNet1 hosts two virtual machines named VM1 and VM2 that run Windows Server.

You need to inspect all the network traffic from VM1 to VM2 for a period of three hours.

Solution: From Azure Network Watcher, you create a packet capture.

Does this meet the goal?

A. Yes **Most Voted**

B. No

[Hide Solution](#)

[Discussion 47](#)

**Correct Answer:** A 

You manage a virtual network named VNet1 that is hosted in the West US Azure region.

VNet1 hosts two virtual machines named VM1 and VM2 that run Windows Server.

You need to inspect all the network traffic from VM1 to VM2 for a period of three hours.

Solution: From Azure Network Watcher, you create a connection monitor.

Does this meet the goal?

A. Yes

B. No **Most Voted**

[Hide Solution](#)

[Discussion 29](#)

**Correct Answer:** A 

Reference:

<https://azure.microsoft.com/en-us/updates/general-availability-azure-network-watcher-connection-monitor-in-all-public-regions/>

*Community vote distribution*

B (90%)

10%

**\*\*Packet Capture\*\*:** Is run on a VM to monitor the in and out flows of IP traffic. It is not used to monitor traffic BETWEEN two VMs. MS Docs: ("Packet Capture enables you to capture all traffic on a VM in your virtual network.")

**\*\*Connection Monitor\*\*:** Is used to monitor connectivity and latency between VMs over a period of time. MS Docs: ("Connection Monitor allows you to monitor connectivity and latency between a VM and another network resource.")

Answer B - No "You need to inspect \*\*all\*\* the network traffic from VM1 to VM2 for a period of three hours." You will need Packet Capture. As it has an option to specify ALL protocols.

Question #76

Topic 5

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

| Name | Type                         | Description                           |
|------|------------------------------|---------------------------------------|
| vm1  | Virtual machine              | Uses a basic public IP address        |
| vm2  | Virtual machine              | Uses a basic public IP address        |
| nsg1 | Network security group (NSG) | Allows incoming traffic from port 443 |
| lb1  | Azure Standard Load Balancer | <b>Not applicable</b>                 |

You need to load balance HTTPS connections to vm1 and vm2 by using lb1.

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

Select and Place:

## Actions

## Answer Area

Remove nsg1.

Remove the public IP addresses from vm1 and vm2.

Create a health probe and backend pool on lb1.

Create a load balancing rule on lb1.

Create an availability set.



Answer is correct:

- 1) Remove the Public IP addresses. They are basic Public IPs and we're using a Standard Load Balancer which aren't compatible.
- 2) Create a backend pool and health probes
- 3) Create a load balancer rule.

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

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

You manage a virtual network named VNet1 that is hosted in the West US Azure region.

VNet1 hosts two virtual machines named VM1 and VM2 that run Windows Server.

You need to inspect all the network traffic from VM1 to VM2 for a period of three hours.

Solution: From Azure Monitor, you create a metric on Network In and Network Out.

Does this meet the goal?

A. Yes

B. No **Most Voted**

[Hide Solution](#)

[Discussion 11](#)

**Correct Answer:** **B** 

Reference:

<https://azure.microsoft.com/en-us/updates/general-availability-azure-network-watcher-connection-monitor-in-all-public-regions/>

*Community vote distribution*

B (100%)

You have an Azure subscription that contains two on-premises locations named site1 and site2. You need to connect site1 and site2 by using an Azure Virtual WAN.

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

Select and Place:

| Actions                                  |
|--|
|  |
|  |
| Connect the virtual networks to the hub. |
|  |
|  |

| Answer Area                       |
|-----------------------------------|
| Create a Virtual WAN resource.    |
| Create a virtual hub.             |
| Create VPN sites.                 |
| Connect the VPN sites to the hub. |

Correct answer:

1. Create Azure Virtual WAN
2. Create Virtual Hub
3. Create VPN sites
4. Connect VPN sites to virtual hub

You have an app named App1 that is installed on two Azure virtual machines named VM1 and VM2. Connections to App1 are managed by using an Azure Load Balancer.

The effective network security configurations for VM2 are shown in the following exhibit.

The screenshot shows the Azure portal interface for VM2 - Networking. On the left, there's a sidebar with links like Home, Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Networking selected), Disks, Size, Security, and Extensions. The main content area is titled "Network Interface: VM2-NIC1" and shows "Effective security rules" and "Topology". It indicates the Virtual network/subnet is Vnet1/Subnet11, NIC Public IP is empty, NIC Private IP is 10.240.11.5, and Accelerated networking is Disabled. Below this, there are tabs for Inbound port rules, Outbound port rules, Application security groups, and Load balancing. Under Inbound port rules, it says "Network security group NSG2 (attached to network interface: Subnet11) Impacts 1 subnets, 0 network interfaces". There is a button "Add inbound port rule". A table lists the rules:

| Priority | Name                          | Port | Protocol | Source            | Destination    | Action             | ... |
|----------|-------------------------------|------|----------|-------------------|----------------|--------------------|-----|
| 100      | Allow_131.107.100.50          | 443  | TCP      | 131.107.100.50    | VirtualNetwork | <span>Allow</span> | ... |
| 200      | BlockAllOther441              | 443  | Any      | Any               | Any            | <span>Deny</span>  | ... |
| 65000    | AllowVnetInBound              | Any  | Any      | VirtualNetwork    | VirtualNetwork | <span>Allow</span> | ... |
| 65001    | AllowAzureLoadBalancerInBound | Any  | Any      | AzureLoadBalancer | Any            | <span>Allow</span> | ... |
| 65500    | DenyAllInBound                | Any  | Any      | Any               | Any            | <span>Deny</span>  | ... |

You discover that connections to App1 from 131.107.100.50 over TCP port 443 fail. You verify that the Load Balancer rules are configured correctly.

You need to ensure that connections to App1 can be established successfully from 131.107.100.50 over TCP port 443.

Solution: You create an inbound security rule that denies all traffic from the 131.107.100.50 source and has a priority of 64999.

Does this meet the goal?

A. Yes

B. No

[Hide Solution](#)

[Discussion \(14\)](#)

**Correct Answer: B**

Reference:

<https://fastreroute.com/azure-network-security-groups-explained/>

Community vote distribution

**B (100%)**

You have an Azure subscription that contains the virtual networks shown in the following table.

| Name  | Peered with | DNS server               |
|-------|-------------|--------------------------|
| VNET1 | VNET2       | Default (Azure-provided) |
| VNET2 | VNET1       | 10.10.0.4                |

You have the virtual machines shown in the following table.

| Name    | IP address  | Network interface | Connects to   |
|---------|-------------|-------------------|---------------|
| Server1 | 10.10.0.4   | NIC1              | VNET1/Subnet1 |
| Server2 | 172.16.0.4  | NIC2              | VNET1/Subnet2 |
| Server3 | 192.168.0.4 | NIC3              | VNET2/Subnet2 |

You have the virtual network interfaces shown in the following table.

| Name | DNS server                   |
|------|------------------------------|
| NIC1 | Inherit from virtual network |
| NIC2 | 10.10.0.4                    |
| NIC3 | Inherit from virtual network |

Server1 is a DNS server that contains the resources shown in the following table.

| Name              | Type             | Value          |
|-------------------|------------------|----------------|
| contoso.com       | Primary DNS zone | Not applicable |
| Host1.contoso.com | A record         | 131.107.10.15  |

You have an Azure private DNS zone named contoso.com that has a virtual network link to VNET2 and the records shown in the following table.

| Name  | Type     | Value          |
|-------|----------|----------------|
| Host1 | A record | 131.107.200.20 |
| Host2 | A record | 131.107.50.50  |

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

## Answer Area

| Statements   | Yes                              | No                               |
|--|----------------------------------|----------------------------------|
| Server2 resolves host2.contoso.com to 131.107.50.50. | <input type="radio"/>            | <input checked="" type="radio"/> |
| Server2 resolves host1.contoso.com to 131.107.10.15. | <input checked="" type="radio"/> | <input type="radio"/>            |
| Server3 resolves host2.contoso.com to 131.107.50.50. | <input type="radio"/>            | <input checked="" type="radio"/> |

1-No

Server2 uses Server1 for DNS. Server1 has no host2.contoso.com record for 131.107.50.50. It would work if VNET1 had a virtual network link to the private zone contoso.com.

2- Yes

Server2 uses Server1 for DNS. Server1 has a host1.contoso.com record for 131.107.10.15

3- No

Server3 uses 10.10.0.4 as DNS (inherited from VNET2). 10.10.0.4 (Server1) has no record for host2.contoso.com. The virtual network link for the private zone contoso.com on VNET2 won't be used since the DNS from VNET1 is set on VNET2. VNET1 DNS is not aware of the private zone contoso.com. It would work if VNET1 had a virtual network link to the private zone contoso.com.

N Y N

1. Server2 > NIC2 > VNET1. NIC2 has DNS 10.0.0.4 which has no host2 record.
2. Server2 > NIC2 > VNET1. NIC2 has DNS 10.0.0.4 which has host1 record.
3. Server3 > NIC3 > VNET2. VNET2 has DNS 10.0.0.4 which has no host2 record.

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

| Name | IP address | Virtual network |
|------|------------|-----------------|
| VM1  | 10.0.0.4   | VNET1           |
| VM2  | 10.0.0.5   | VNET1           |

VNET1 is linked to a private DNS zone named contoso.com that contains the records shown in the following table.

| Name  | Type  | TTL  | Value             | Auto registered |
|-------|-------|------|-------------------|-----------------|
| comp1 | TXT   | 3600 | 10.0.0.5          | False           |
| comp2 | A     | 3600 | 10.0.0.5          | False           |
| comp3 | CNAME | 3600 | comp1.contoso.com | False           |
| comp4 | PTR   | 3600 | 10.0.0.5          | False           |

You need to ping VM2 from VM1.

Which DNS names can you use to ping VM2?

- A. comp2.contoso.com and comp4.contoso.com only
- B. comp1.contoso.com, comp2.contoso.com, comp3.contoso.com, and comp4.contoso.com
- C. comp2.contoso.com only **Most Voted**
- D. comp1.contoso.com and comp2.contoso.com only
- E. comp1.contoso.com, comp2.contoso.com, and comp4.contoso.com only

[Hide Solution](#)

[Discussion 39](#)

**Correct Answer C: comp2.contoso.com only**

A record: Is used to map a DNS/domain name to an IP

TXT records in a lot of cases get used to prove ownership of a domain, it has other purposes too.

PTR: A Reverse DNS lookup is used by remote hosts to determine who 'owns' an IP address.

CNAME records get used to redirect a DNS name or subdomain name to another DNS name or domain name or subdomain name.

You have a network security group (NSG) named NSG1 that has the rules defined in the exhibit. (Click the Exhibit tab.)

```
PS C:\> Get-AzNetworkSecurityGroup -Name "NSG1" -ResourceGroupName "RG1" | Select -ExpandProperty SecurityRules
```

|                                      |   |   |
|--------------------------------------|---|---|
| Name                                 | : | ALLOW_HTTPS   |
| Id                                   | : | /subscriptions/09d06b22-ff51-48b7-a8be-947f15cbd69d/resourceGroups/RG1/providers/Microsoft.Network/networkSecurityGroups/NSG1/securityRules/ALLOW_HTTPS |
| Etag                                 | : | W/"8e3e9995-aa78-41e2-bfea-44b50c389873"  |
| ProvisioningState                    | : | Succeeded   |
| Description                          | : |   |
| Protocol                             | : | TCP   |
| SourcePortRange                      | : | {*}   |
| DestinationPortRange                 | : | {443}   |
| SourceAddressPrefix                  | : | {*}   |
| DestinationAddressPrefix             | : | {*}   |
| SourceApplicationSecurityGroups      | : | []  |
| DestinationApplicationSecurityGroups | : | []  |
| Access                               | : | Allow   |
| Priority                             | : | 100   |
| Direction                            | : | Inbound   |
| <br>                                 |   |   |
| Name                                 | : | DENY_PING   |
| Id                                   | : | /subscriptions/09d06b22-ff51-48b7-a8be-947f15cbd69d/resourceGroups/RG1/providers/Microsoft.Network/networkSecurityGroups/NSG1/securityRules/DENY_PING   |
| Etag                                 | : | W/"8e3e9995-aa78-41e2-bfea-44b50c389873"  |
| ProvisioningState                    | : | Succeeded   |
| Description                          | : |   |
| Protocol                             | : | ICMP  |
| SourcePortRange                      | : | {*}   |
| DestinationPortRange                 | : | {*}   |
| SourceAddressPrefix                  | : | {VirtualNetwork}  |
| DestinationAddressPrefix             | : | {*}   |
| SourceApplicationSecurityGroups      | : | []  |
| DestinationApplicationSecurityGroups | : | []  |
| Access                               | : | Deny  |
| Priority                             | : | 111   |
| Direction                            | : | Outbound  |

NSG1 is associated to a subnet named Subnet1. Subnet1 contains the virtual machines shown in the following table.

| Name | IP address |
|------|------------|
| VM1  | 10.1.0.10  |
| VM2  | 10.1.0.11  |

You need to add a rule to NSG1 to ensure that VM1 can ping VM2. The solution must use the principle of least privilege.

How should you configure the rule? To answer, select the appropriate options in the answer area.

## Answer Area

|              |  |
|--------------|--|
| Direction:   | <input type="checkbox"/> Inbound<br><input checked="" type="checkbox"/> Outbound   |
| Source:      | <input type="checkbox"/> Any<br><input checked="" type="checkbox"/> 10.1.0.10<br><input type="checkbox"/> 10.1.0.11<br><input type="checkbox"/> 10.1.0.10; 10.1.0.11<br><input type="checkbox"/> 10.1.0.0/28 |
| Destination: | <input type="checkbox"/> Any<br><input type="checkbox"/> 10.1.0.10<br><input checked="" type="checkbox"/> 10.1.0.11<br><input type="checkbox"/> 10.1.0.10; 10.1.0.11<br><input type="checkbox"/> 10.1.0.0/28 |
| Priority:    | <input type="checkbox"/> 110<br><input checked="" type="checkbox"/> 111<br><input type="checkbox"/> 112  |

We need to undo the DENY\_PING rule with the principle of least privilege.

Direction: Outbound

Source 10.1.0.10 (VM1)

Destination: 10.1.0.11 (VM2)

Priority: 110

You have an Azure subscription that uses the public IP addresses shown in the following table.

| Name | IP version | SKU      | IP address assignment | Availability zone |
|------|------------|----------|-----------------------|-------------------|
| IP1  | IPv6       | Basic    | Static                | Not applicable    |
| IP2  | IPv6       | Basic    | Dynamic               | Not applicable    |
| IP3  | IPv6       | Standard | Static                | Zone-redundant    |

You need to create a public Azure Standard Load Balancer.

Which public IP addresses can you use?

- A. IP1, IP2, and IP3
- B. IP2 only
- C. IP3 only **Most Voted**
- D. IP1 and IP3 only

[Hide Solution](#)

[Discussion 12](#)

**Correct Answer:** C 

Matching SKUs are required for load balancer and public IP resources. You can't have a mixture of Basic SKU resources and standard SKU resources.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-addresses>

*Community vote distribution*

C (100%)

You have an Azure subscription.

You are deploying an Azure Kubernetes Service (AKS) cluster that will contain multiple pods. The pods will use kubernetes networking.

You need to restrict network traffic between the pods.

What should you configure on the AKS cluster?

- A. the Azure network policy
- B. the Calico network policy **Most Voted**
- C. pod security policies
- D. an application security group

[Hide Solution](#)

[Discussion 20](#)

**Correct Answer:** B 

Reference:

<https://docs.microsoft.com/en-us/azure/aks/use-network-policies>

*Community vote distribution*

B (100%)

You have an Azure subscription that contains a virtual network named VNet1. VNet1 uses an IP address space of 10.0.0.0/16 and contains the VPN Gateway and subnets in the following table:

| Name          | IP address range |
|---------------|------------------|
| Subnet0       | 10.0.0.0/24      |
| Subnet1       | 10.0.1.0/24      |
| Subnet2       | 10.0.2.0/24      |
| GatewaySubnet | 10.0.254.0/24    |

Subnet1 contains a virtual appliance named VM1 that operates as a router.

You create a routing table named RT1.

You need to route all inbound traffic from the VPN gateway to VNet1 through VM1.

How should you configure RT1? To answer, select the appropriate options in the answer area.

## Answer Area

|                |  |
|----------------|--|
| Address prefix | <input type="checkbox"/> 10.0.0.0/16             |
|                | <input type="checkbox"/> 10.0.1.0/24             |
|                | <input type="checkbox"/> 10.0.254.0/24           |
| Next hop type  | <input type="checkbox"/> Virtual appliance       |
|                | <input type="checkbox"/> Virtual network         |
|                | <input type="checkbox"/> Virtual network gateway |
| Assigned to    | <input type="checkbox"/> GatewaySubnet           |
|                | <input type="checkbox"/> Subnet0                 |
|                | <input type="checkbox"/> Subnet1 and Subnet2     |

Box 1: 10.0.0.0/16

Address prefix destination-> Vnet 1 (Address space of Vnet1)

Box 2: Virtual appliance

Next hop type VM1 ->Virtual Appliance. You can specify IP address of VM 1 when configuring next hop as Virtual appliance.

Box 3: Gateway Subnet

This route is to be followed by Gateway Subnet for the incoming traffic.

You can associate routing table to the Subnet from Rout Table -> subnet ->Associate.

Question #89

Topic 5

You have five Azure virtual machines that run Windows Server 2016. The virtual machines are configured as web servers.

You have an Azure load balancer named LB1 that provides load balancing services for the virtual machines.

You need to ensure that visitors are serviced by the same web server for each request.

What should you configure?

- A. Floating IP (direct server return) to Enabled
- B. Floating IP (direct server return) to Disabled
- C. a health probe
- D. Session persistence to Client IP and Protocol Most Voted

[Hide Solution](#)

[Discussion](#) 23

Correct Answer: D 

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

| Name | Operating system    | Connects to |
|------|---------------------|-------------|
| VM1  | Windows Server 2019 | Subnet1     |
| VM2  | Windows Server 2019 | Subnet2     |

VM1 and VM2 use public IP addresses. From Windows Server 2019 on VM1 and VM2, you allow inbound Remote Desktop connections.

Subnet1 and Subnet2 are in a virtual network named VNET1.

The subscription contains two network security groups (NSGs) named NSG1 and NSG2. NSG1 uses only the default rules.

NSG2 uses the default rules and the following custom incoming rule:

- Priority: 100
- Name: Rule1
- Port: 3389
- Protocol: TCP
- Source: Any
- Destination: Any
- Action: Allow

NSG1 is associated to Subnet1. NSG2 is associated to the network interface of VM2.

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

## Answer Area

| Statements   | Yes                              | No                               |
|--|----------------------------------|----------------------------------|
| From the Internet, you can connect to VM1 by using Remote Desktop. | <input type="radio"/>            | <input checked="" type="radio"/> |
| From the Internet, you can connect to VM2 by using Remote Desktop. | <input checked="" type="radio"/> | <input type="radio"/>            |
| From VM1, you can connect to VM2 by using Remote Desktop           | <input checked="" type="radio"/> | <input type="radio"/>            |

Box 1: No

VM1 has default rules which (Inbound rules) by default, there will be three inbound security rules (allow virtual network traffic, allow load balancer traffic, deny all other traffic) added to an NSG when you create NSG. All inbound traffic except the traffic from virtual network and Azure load balancer is not allowed.

Box 2: Yes

NSG2 has custom Rule1, allowing RDP port 3389 with TCP.

Box 3: Yes

VM1 and VM2 are in the same VNet. By default, communication is allowed.

Question #91

Topic 5

You have an Azure subscription that contains two virtual machines named VM1 and VM2. You create an Azure load balancer.

You plan to create a load balancing rule that will load balance HTTPS traffic between VM1 and VM2.

Which two additional load balancer resources should you create before you can create the **load balancing rule**? Each correct answer presents part of the solution.

- A. a frontend IP address
- B. an inbound NAT rule
- C. a virtual network
- D. a backend pool Most Voted
- E. a health probe Most Voted

[Hide Solution](#)

[Discussion](#) 12

**Correct Answer:** DE 

Reference:

<https://docs.microsoft.com/en-us/azure/load-balancer/components>

*Community vote distribution*

DE (82%)

Other

Question #92

Topic 5

You have an on-premises network that contains a database server named dbserver1.

You have an Azure subscription.

You plan to deploy three Azure virtual machines. Each virtual machine will be deployed to a separate availability zone.

You need to configure an Azure VPN gateway for a site-to-site VPN. The solution must ensure that the virtual machines can connect to dbserver1.

Which type of public IP address SKU and assignment should you use for the gateway?

- A. a basic SKU and a static IP address assignment
- B. a standard SKU and a static IP address assignment Most Voted
- C. a basic SKU and a dynamic IP address assignment

Answer is B. since the VMs are in AZ then VPN gateway will have to be in AZ which will rely on Azure public IP resource Standard SKU. And must be Static as Dynamic is only for non-AZ.

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

| Name | IP address  | Virtual network |
|------|-------------|-----------------|
| VM1  | 10.0.0.4    | VNET1           |
| VM2  | 172.16.0.4  | VNET2           |
| VM3  | 192.168.0.4 | VNET3           |
| VM4  | 192.168.0.5 | VNET3           |

VNET1, VNET2, and VNET3 are peered.

VNET1 and VNET2 are linked to an Azure private DNS zone named contoso.com that contains the records shown in the following table.

| Name    | Type | Value       |
|---------|------|-------------|
| Server1 | A    | 131.107.3.3 |
| Server2 | A    | 131.107.3.4 |

The virtual networks are configured to use the DNS servers shown in the following table.

| Virtual network | DNS server               |
|-----------------|--------------------------|
| VNET1           | Default (Azure-provided) |
| VNET2           | Custom: 192.168.0.5      |
| VNET3           | Custom: 192.168.0.5      |

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

- | Statements   | Yes                              | No                               |
|--|----------------------------------|----------------------------------|
| From VM1, server1.contoso.com resolves to 131.107.3.3. | <input checked="" type="radio"/> | <input type="radio"/>            |
| From VM2, server1.contoso.com resolves to 131.107.3.3. | <input type="radio"/>            | <input checked="" type="radio"/> |
| From VM3, server2.contoso.com resolves to 131.107.2.4. | <input type="radio"/>            | <input checked="" type="radio"/> |

YNN

VM3 is part of VNET3 which has 192.168.0.5 as DNS server this is the IP of VM4 which is in VNET3 and doesn't have any record of server 2 so the correct answer would be No for the last one.

Question #94

Topic 5

You have two Azure virtual machines as shown in the following table.

| Name | Operating system                           | Private IP address | Public IP address | DNS suffix configured in the operating system | Connected to |
|------|--|--------------------|-------------------|---|--------------|
| vm1  | Windows Server 2019                        | 10.0.1.4           | 131.107.50.20     | Contoso.com                                   | vnet1        |
| vm2  | SUSE Linux Enterprise Server 15 (SLES) SP2 | 10.0.1.5           | 131.107.90.80     | <b>None</b>                                   | vnet1        |

You create the Azure DNS zones shown in the following table.

| Name         | Type             |
|--------------|------------------|
| Contoso.com  | DNS zone         |
| Fabrikam.com | Private DNS zone |

You perform the following actions:

☞ If I add a virtual network link to vnet1 and enable auto registration.

☞ For contoso.com, you assign vm1 and vm2 the Owner role.

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

**Statements**

**Yes**    **No**

The DNS A record for vm1 is added to contoso.com and has the IP address of 131.107.50.20.

The DNS A record for vm1 is added to fabrikam.com and has the IP address of 10.0.1.4.

The DNS A record for vm2 is added to fabrikam.com and has the IP address of 10.0.1.5.

1--N

Public IPs wont auto register DNS. Adding a VM with the OWNER role does not change anything in the name resolution process.

2—Y Auto registration is enabled

3---N Linux won't do auto registration

You have an on-premises datacenter and an Azure subscription. You plan to connect the datacenter to Azure by using ExpressRoute. You need to deploy an ExpressRoute gateway. The solution must meet the following requirements:

- Support up to 10 Gbps of traffic.
- Support availability zones.
- Support FastPath.
- Minimize costs.

Which SKU should you deploy?

- A. ERGw1AZ
- B. ERGw2
- C. ErGw3
- D. ErGw3AZ **Most Voted**

[Hide Solution](#)[Discussion 6](#)

Correct Answer: D 🎉

ErGw3AZ support fastpath

You have a virtual network named VNET1 that contains the subnets shown in the following table:

| Name    | Subnet       | Network security group (NSG) |
|---------|--------------|------------------------------|
| Subnet1 | 10.10.1.0/24 | NSG1                         |
| Subnet2 | 10.10.2.0/24 | <i>None</i>                  |

You have Azure virtual machines that have the network configurations shown in the following table:

| Name | Subnet  | IP address | NSG         |
|------|---------|------------|-------------|
| VM1  | Subnet1 | 10.10.1.5  | NSG2        |
| VM2  | Subnet2 | 10.10.2.5  | <i>None</i> |
| VM3  | Subnet2 | 10.10.2.6  | <i>None</i> |

For NSG1, you create the inbound security rule shown in the following table:

| Priority | Source       | Destination  | Destination port | Action |
|----------|--------------|--------------|------------------|--------|
| 101      | 10.10.2.0/24 | 10.10.1.0/24 | TCP/1433         | Allow  |

For NSG2, you create the inbound security rule shown in the following table:

| Priority | Source    | Destination | Destination port | Action |
|----------|-----------|-------------|------------------|--------|
| 125      | 10.10.2.5 | 10.10.1.5   | TCP/1433         | Block  |

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

## Answer Area

| Statements  | Yes                              | No                               |
|---|----------------------------------|----------------------------------|
| VM2 can connect to the TCP port 1433 services on VM1. | <input type="radio"/>            | <input checked="" type="radio"/> |
| VM1 can connect to the TCP port 1433 services on VM2. | <input checked="" type="radio"/> | <input type="radio"/>            |
| VM2 can connect to the TCP port 1433 services on VM3. | <input checked="" type="radio"/> | <input type="radio"/>            |

1. NO

The NSG2 on the NIC of VM1 blocks the request that passes through NSG1 which is attached on the subnet. There is no priority bypass between NSGs. Traffic is filtered independently between NSGs.

2. YES - For VM2 there are no NSGs applied neither on subnet or NIC level hence all traffic is allowed.
3. YES - For VM3 there are no NSGs applied neither on subnet or NIC level hence all traffic is allowed.

You have an Azure subscription named Subscription1.

Subscription1 contains the virtual machines in the following table:

| Name | IP address |
|------|------------|
| VM1  | 10.0.1.4   |
| VM2  | 10.0.2.4   |
| VM3  | 10.0.3.4   |

Subscription1 contains a virtual network named VNet1 that has the subnets in the following table:

| Name    | Address space | Connected virtual machine |
|---------|---------------|---------------------------|
| Subnet1 | 10.0.1.0/24   | VM1                       |
| Subnet2 | 10.0.2.0/24   | VM2                       |
| Subnet3 | 10.0.3.0/24   | VM3                       |

VM3 has multiple network adapters, including a network adapter named NIC3. IP forwarding is enabled on NIC3. Routing is enabled on VM3.

You create a route table named RT1 that contains the routes in the following table:

| Address prefix | Next hop type     | Next hop address |
|----------------|-------------------|------------------|
| 10.0.1.0/24    | Virtual appliance | 10.0.3.4         |
| 10.0.2.0/24    | Virtual appliance | 10.0.3.4         |

You apply RT1 to Subnet1 and Subnet2.

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

NOTE: Each correct selection is worth one point.

## Answer Area

| Statements   | Yes                              | No                               |
|--|----------------------------------|----------------------------------|
| VM3 can establish a network connection to VM1.                       | <input checked="" type="radio"/> | <input type="radio"/>            |
| If VM3 is turned off, VM2 can establish a network connection to VM1. | <input type="radio"/>            | <input checked="" type="radio"/> |
| VM1 can establish a network connection to VM2.                       | <input checked="" type="radio"/> | <input type="radio"/>            |

Your on-premises network contains an SMB share named Share1.  
You have an Azure subscription that contains the following resources:  
 A web app named webapp1  
 A virtual network named VNET1  
You need to ensure that webapp1 can connect to Share1.  
What should you deploy?

- A. an Azure Application Gateway
- B. an Azure Active Directory (Azure AD) Application Proxy
- C. an Azure Virtual Network Gateway

**Correct Answer:** C 

A Site-to-Site VPN gateway connection can be used to connect your on-premises network to an Azure virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel. This type of connection requires a VPN device, a VPN gateway, located on-premises that has an externally facing public IP address assigned to it.

Incorrect Answers:

B: Application Proxy is a feature of Azure AD that enables users to access on-premises web applications from a remote client.

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal>

*Community vote distribution*

C (100%)

You plan to deploy several Azure virtual machines that will run Windows Server 2019 in a virtual machine scale set by using an Azure Resource Manager template.  
You need to ensure that NGINX is available on all the virtual machines after they are deployed.  
What should you use?

- A. the Publish-AzVMDscConfiguration cmdlet
- B. Azure Application Insights
- C. Azure Custom Script Extension Most Voted
- D. the New-AzConfigurationAssignment cmdlet

Note:

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

1. a Desired State Configuration (DSC) extension
2. Azure Custom Script Extension

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

- Deployment Center in Azure App Service
- a Microsoft Intune device configuration profile

Question #100

Topic 5

Your on-premises network contains a VPN gateway.

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

| Name     | Type                    | Description   |
|----------|-------------------------|---|
| vgw1     | Virtual network gateway | Gateway for Site-to-Site VPN to the on-premises network |
| storage1 | Storage account         | Standard performance tier                               |
| Vnet1    | Virtual network         | Enabled forced tunneling                                |
| VM1      | Virtual machine         | Connected to Vnet1                                      |

You need to ensure that all the traffic from VM1 to storage1 travels across the Microsoft backbone network.

What should you configure?

A. a network security group (NSG)

B. service endpoints **Most Voted**

C. Azure Peering Service

D. Azure Firewall

[Hide Solution](#)

[Discussion 10](#)

Correct Answer: A 

Community vote distribution

B (100%)

You plan to deploy route-based Site-to-Site VPN connections between several on-premises locations and an Azure virtual network. Which tunneling protocol should you use?

- A. IKEv1
- B. PPTP
- C. IKEv2 Most Voted
- D. L2TP

[Hide Solution](#)[Discussion 4](#)

Correct Answer: C 

A Site-to-Site (S2S) VPN gateway connection is used to connect your on-premises network to an Azure virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel. IKEv2 supports 10 S2S connections, while IKEv1 only supports 1.

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

| Name  | Type            | Description  |
|-------|-----------------|--|
| VNET1 | Virtual network | Azure region: US East<br>Contains the following subnets: <ul style="list-style-type: none"><li>Subnet1: 172.16.1.0/24</li><li>Subnet2: 172.16.2.0/24</li><li>Subnet3: 172.16.3.0/24</li></ul>  |
| VNET2 | Virtual network | Azure region: West US<br>Contains the following subnets: <ul style="list-style-type: none"><li>DemoSubnet1: 172.16.1.0/24</li><li>RecoverySubnetA: 172.16.5.0/24</li><li>RecoverySubnetB: 172.16.3.0/24</li><li>TestSubnet1: 172.16.2.0/24</li></ul> |
| VM1   | Virtual machine | Connected to Subnet2   |

You configure Azure Site Recovery to replicate VM1 between the US East and West US regions.

You perform a test failover of VM1 and specify VNET2 as the target virtual network.

When the test version of VM1 is created, to which subnet will the virtual machine be connected?

- A. TestSubnet1
- B. DemoSubnet1
- C. RecoverySubnetA
- D. RecoverySubnetB

Hide SolutionDiscussion 3

Correct Answer: A 

You have an Azure subscription that contains 20 virtual machines, a network security group (NSG) named NSG1, and two virtual networks named VNET1 and VNET2 that are peered.

You plan to deploy an Azure Bastion Basic SKU host named Bastion1 to VNET1.

You need to configure NSG1 to allow inbound access to the virtual machines via Bastion1.

Which port should you configure for the inbound security rule?

A. 22

B. 443

C. 389

D. 8080

[Hide Solution](#)

[Discussion](#) 7

**Correct Answer:** B 🎉

*Community vote distribution*

B (100%)

- **Egress Traffic to target VMs:** Azure Bastion will reach the target VMs over private IP. The NSGs need to allow egress traffic to other target VM subnets for port 3389 and 22. If you are using the custom port feature as part of Standard SKU, the NSGs will instead need to allow egress traffic to other target VM subnets for the custom value(s) you have opened on your target VMs.

<https://learn.microsoft.com/en-us/azure/bastion/bastion-nsg>

| Priority | Name                       | Port      | Protocol | Source         | Destination    | Action               | ... |
|----------|----------------------------|-----------|----------|----------------|----------------|----------------------|-----|
| 100      | AllowSshRdpOutbound        | 22,3389   | Any      | Any            | VirtualNetwork | <span>✓ Allow</span> | ... |
| 110      | AllowAzureCloudOutbound    | 443       | TCP      | Any            | AzureCloud     | <span>✓ Allow</span> | ... |
| 120      | AllowBastionCommunication  | 8080,5701 | Any      | VirtualNetwork | VirtualNetwork | <span>✓ Allow</span> | ... |
| 130      | AllowGetSessionInformation | 80        | Any      | Any            | Internet       | <span>✓ Allow</span> | ... |

Your network contains an on-premises Active Directory Domain Services (AD DS) domain named contoso.com. The domain contains the servers shown in the following table.

| Name    | IP address      | Role                            |
|---------|-----------------|---------------------------------|
| DC1     | 192.168.2.1/16  | Domain controller<br>DNS server |
| Server1 | 192.168.2.50/16 | Member server                   |

You plan to migrate contoso.com to Azure.

You create an Azure virtual network named VNET1 that has the following settings:

- Address space: 10.0.0.0/16
- Subnet:
  - Name: Subnet1
  - IPv4: 10.0.1.0/24

You need to move DC1 to VNET1. The solution must ensure that the member servers in contoso.com can resolve AD DS DNS names.

How should you configure DC1? To answer, select the appropriate options in the answer area.

## Answer Area

IP address

▼

Obtain an IP address automatically

Use 10.0.1.3

Use 10.0.2.1

Use 192.168.2.1

Name resolution

▼

Configure VNET1 to use a custom DNS server

Configure VNET1 to use the default Azure-provided DNS server

Create an Azure Private DNS zone named contoso.com

Create an Azure public DNS zone named contoso.com

You have an Azure subscription that contains the virtual networks shown in the following table.

| Name  | Azure region | Resource group |
|-------|--------------|----------------|
| VNET1 | West US      | RG1            |
| VNET2 | Central US   | RG1            |
| VNET3 | Central US   | RG2            |
| VNET4 | West US      | RG2            |

You need to deploy an Azure firewall named AF1 to RG1 in the West US Azure region.

To which virtual networks can you deploy AF1?

- A. VNET1, VNET2, VNET3, and VNET4
- B. VNET1 and VNET2 only
- C. VNET1 only 
- D. VNET1, VNET2, and VNET4 only
- E. VNET1 and VNET4 only 

[Hide Solution](#)

 Discussion 5

Correct Answer: C 

You have an on-premises network.

You have an Azure subscription that contains three virtual networks named VNET1, VNET2, and VNET3. The virtual networks are peered and connected to the on-premises network. The subscription contains the virtual machines shown in the following table.

| Name | Location   | Connected to |
|------|------------|--------------|
| VM1  | West US    | VNET1        |
| VM2  | West US    | VNET1        |
| VM3  | West US    | VNET2        |
| VM4  | Central US | VNET3        |

You need to monitor connectivity between the virtual machines and the on-premises network by using Connection Monitor.

What is the minimum number of connection monitors you should deploy?

A. 1 

B. 2

C. 3

D. 4

[Hide Solution](#)

 Discussion 4

Correct Answer: B 

Community vote distribution

B (50%)

A (50%)

You plan to deploy the following Azure Resource Manager (ARM) template.

```
{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {},
  "variables": {
    "vnetId": "[resourceId('Microsoft.Network/virtualNetworks/', 'VNET1')]",
    "lbId": "[resourceId('Microsoft.Network/loadBalancers/', 'LB1')]",
    "sku": "Standard",
    "netname": "APP1"
  },
  "resources": [
    {
      "apiVersion": "2017-08-01",
      "type": "Microsoft.Network/loadBalancers/",
      "name": "LB1",
      "location": "EastUS",
      "sku": {
        "name": "[variables('sku')]"
      },
      "properties": {
        "frontendIPConfiguration": [
          {
            "name": "[variables('netname')]",
            "properties": {
              "subnet": {
                "id": "[concat(variables('vnetId'), '/subnets/', variables('netname'))]"
              },
              "privateIPAllocationMethod": "Dynamic"
            }
          }
        ],
        "backendAddressPools": [
          {
            "name": concat(variables('netname'), '-Servers')"
          }
        ],
        "loadBalancingRules": [
          {
            "name": "APP1",
            "properties": {
              "frontendIPConfiguration": {
                "id": "[concat(variables('lbId'), '/frontendIPConfigurations/', variables('netname'))]"
              },
              "backendAddressPool": {
                "id": "[concat(variables('lbId'), '/backendAddressPool/', variables('netname'))]"
              },
              "probe": {
                "id": "[concat(variables('lbId'), '/probes/probe')]"
              },
              "backendPort": 8080,
              "protocol": "Tcp",
              "frontendPort": 80,
              "enableFloatingIP": false,
              "idleTimeoutInMinutes": 4,
              "loadDistribution": "SourceIPProtocol"
            }
          }
        ],
        "probes": [
          {
            "name": "probe",
            "properties": {
              "protocol": "Tcp",
              "port": 8080,
              "intervalInSeconds": 15,
              "numberOfProbes": 2
            }
          }
        ]
      }
    }
  ]
}
```

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

### Answer Area

| Statements   | Yes                              | No                               |
|--|----------------------------------|----------------------------------|
| LB1 will be connected to a subnet named VNET1/netname  | <input type="radio"/>            | <input checked="" type="radio"/> |
| LB1 can be deployed only to the resource group that contains VNET1   | <input checked="" type="radio"/> | <input type="radio"/>            |
| The value of the sku variable can be provided as a parameter when the template is deployed from a command prompt | <input type="radio"/>            | <input checked="" type="radio"/> |

### Question #112

Topic 5

You have an Azure subscription that contains a storage account. The account stores website data.

You need to ensure that inbound user traffic uses the Microsoft point-of-presence (POP) closest to the user's location.

What should you configure?

- A. private endpoints
- B. Azure Firewall rules
- C. Routing preference
- D. load balancing

[Hide Solution](#)

[Discussion](#) 3

**Correct Answer:** C 📦

*Community vote distribution*

C (75%)

A (25%)

You have two Azure virtual machines named VM1 and VM2 that run Windows Server. The virtual machines are in a subnet named Subnet1. Subnet1 is in a virtual network named VNet1.

You need to prevent VM1 from accessing VM2 on port 3389.

What should you do?

- A. Create a network security group (NSG) that has an outbound security rule to deny destination port 3389 and apply the NSG to the network interface of VM1.
- B. Configure Azure Bastion in VNet1.
- C. Create a network security group (NSG) that has an outbound security rule to deny source port 3389 and apply the NSG to Subnet1.
- D. Create a network security group (NSG) that has an inbound security rule to deny source port 3389 and apply the NSG to Subnet1.

Correct Answer: A 

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

| Name      | Type             | Description                                   |
|-----------|------------------|---|
| App1      | App Service      | Virtual network integration enabled for VNET1 |
| ASP1      | App Service plan | Standard SKU                                  |
| VNET1     | Virtual network  | None  |
| Firewall1 | Azure Firewall   | Connected to VNET1                            |

You need to manage outbound traffic from VNET1 by using Firewall1.

What should you do first?

- A. Configure the Hybrid Connection Manager.
- B. Upgrade ASP1 to the Premium SKU.
- C. Create a route table.
- D. Create an Azure Network Watcher.

[Hide Solution](#)

[Discussion](#) 3

Correct Answer: C 

## Topic 6 - Question Set 6

### Question #1

Topic 6

You have an Azure subscription that has a Recovery Services vault named Vault1. The subscription contains the virtual machines shown in the following table:

| Name | Operating system        | Auto-shutdown |
|------|-------------------------|---------------|
| VM1  | Windows Server 2012 R2  | Off           |
| VM2  | Windows Server 2016     | 19:00         |
| VM3  | Ubuntu Server 18.04 LTS | Off           |
| VM4  | Windows 10              | 19:00         |

You plan to schedule backups to occur every night at 23:00.

Which virtual machines can you back up by using Azure Backup?

- A. VM1 and VM3 only
- B. VM1, VM2, VM3 and VM4 Most Voted
- C. VM1 and VM2 only
- D. VM1 only

[Hide Solution](#)

[Discussion](#) 19

Correct Answer: B 

You create a Recovery Services vault backup policy named Policy1 as shown in the following exhibit:

### Policy1

Associated items

#### Backup schedule

- \* Frequency      \* Time      \* Timezone

Daily

11:00 PM

(UTC) Coordinated Universal Time

#### Retention range

Retention of daily backup point

- \* At                  For

11:00 PM

30



Day(s)

Retention of weekly backup point

- \* On                  \* At                  For

Sunday

11:00 PM

10



Week(s)

Retention of monthly backup point

Week Based  Day Based

- \* On                  \* At                  For

1

11:00 PM

36



Month(s)

Retention of yearly backup point

Week Based  Day Based

- \* In                  \* On                  \* At                  For

March

1

11:00 PM

10



Year(s)

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

NOTE: Each correct selection is worth one point.

## Answer Area

The backup that occurs on Sunday, March 1, will be retained for [answer choice].

▼

|                 |
|-----------------|
| 30 days         |
| 10 weeks        |
| 36 months       |
| <b>10 years</b> |

The backup that occurs on Sunday, November 1, will be retained for [answer choice].

▼

|                  |
|------------------|
| 30 days          |
| 10 weeks         |
| <b>36 months</b> |
| 10 years         |

Answer is correct. 10 years and 36 months. Azure retention policy takes the longest period of retention for each backup. In case of conflict between 2 different policies.

### Question #3

### Topic 6

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 **Most Voted**
- B. Create a storage account
- C. Configure the extensions for VM3 and VM4
- D. Create a new backup policy

[Hide Solution](#)

[Discussion \(21\)](#)

Correct Answer: A

You have an Azure subscription that contains an Azure Storage account named storage1 and the users shown in the following table.

| Name  | Member of |
|-------|-----------|
| User1 | Group1    |
| User2 | Group2    |
| User3 | Group1    |

You plan to monitor storage1 and to configure email notifications for the signals shown in the following table.

| Name                   | Type         | Users to notify         |
|------------------------|--------------|-------------------------|
| Ingress                | Metric       | User1 and User3 only    |
| Egress                 | Metric       | User1 only              |
| Delete storage account | Activity log | User1, User2, and User3 |
| Restore blob ranges    | Activity log | User1 and User3 only    |

You need to identify the minimum number of alert rules and action groups required for the planned monitoring. How many alert rules and action groups should you identify? To answer, select the appropriate options in the answer area.

## Answer Area

Alert rules:

|   |
|---|
| 1 |
| 2 |
| 3 |
| 4 |

Action groups:

|   |
|---|
| 1 |
| 2 |
| 3 |
| 4 |

Box 1: 4

You need 1 alert rule per 1 signal (1xIngress, 1xEgress, 1xDelete storage account, 1xRestore blob ranges).

Box 2: 3

You need 3 Action Groups (1xUser1 and User3, 1xUser1 only, 1xUser1 User2 and User3). Check 'Users to notify' column.

Question #5

Topic 6

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

| Name       | Type             | Member of   |
|------------|------------------|-------------|
| User1      | User             | <i>None</i> |
| User2      | User             | Group1      |
| Principal1 | Managed identity | <i>None</i> |
| Principal2 | Managed identity | Group1      |

User1, Principal1, and Group1 are assigned the Monitoring Reader role.

An action group named AG1 has the Email Azure Resource Manager Role notification type and is configured to email the Monitoring Reader role.

You create an alert rule named Alert1 that uses AG1.

You need to identify who will receive an email notification when Alert1 is triggered.

Who should you identify?

- A. User1 and Principal1 only
- B. User1, User2, Principal1, and Principal2
- C. User1 only Most Voted
- D. User1 and User2 only Most Voted

Correct Answer is D.

- \* User1, Principal1, and Group1 are assigned the Monitoring Reader role.
- \* AG1 is configured to email the Monitoring Reader role.
- \* User2 is a member of Group1. So User1 and User2 will receive an email notification.

You have an Azure virtual machine named VM1 and a Recovery Services vault named Vault1. You create a backup policy named Policy1 as shown in the exhibit. (Click the Exhibit tab.)

# Policy1

Associated items Delete Save Discard

## Backup schedule

\* Frequency **Daily** \* Time **2:00 AM** \* Timezone **(UTC) Coordinated Universal Time**

## Retention range

Retention of daily backup point.

\* At **2:00 AM** For **5** Day(s)

Retention of weekly backup point.

\* On **Sunday** \* At **2:00 AM** For **20** Week(s)

Retention of monthly backup point.

**Week Based** **Day Based**

\* On **2** \* At **2:00 AM** For **24** Month(s)

Retention of yearly backup point.

**Week Based** **Day Based**

\* In **January** \* On **9** \* At **2:00 AM** For **5** Year(s)

You configure the backup of VM1 to use Policy1 on Thursday, January 1 at 1:00 AM.

You need to identify the number of available recovery points for VM1.

How many recovery points are available on January 8 and January 15? To answer, select the appropriate options in the answer area.

## Answer Area

January 8 at 2:00 PM (14:00):

|   |
|---|
| 5 |
| 6 |
| 8 |
| 9 |

January 15 at 2:00 PM (14:00):

|    |
|----|
| 5  |
| 8  |
| 17 |
| 19 |

@8 JAN: 5 daily backups ( 1 weekly backup included) + 1 monthly = 6

15th January is Thursday. So:

5 daily backups (11th Sunday weekly backup included) + 1 weekly backup (4th Sunday) + 1 Monthly + 1 Yearly = 8 backups

Box 2: 8.

You have the web apps shown in the following table.

| Name | Web framework          | Hosting environment   |
|------|------------------------|---|
| App1 | Microsoft ASP.NET      | An on-premises physical server that runs Windows Server 2019 and has Internet Information Services (IIS) configured |
| App2 | Microsoft ASP.NET Core | An Azure virtual machine that runs Windows Server 2019 and has Internet Information Services (IIS) configured       |

You need to monitor the performance and usage of the apps by using Azure Application Insights. The solution must minimize modifications to the application code.

What should you do on each app? To answer, select the appropriate options in the answer area.

## Answer Area

App1:

- Install the Log Analytics agent
- Install the Azure Monitor agent
- Use the Application Insights SDK
- Install the Application Insights Agent

App2:

- Install the Log Analytics agent
- Install the Azure Monitor agent
- Use the Application Insights SDK
- Install the Application Insights Agent

You have an Azure virtual machine named VM1.

You use Azure Backup to create a backup of VM1 named Backup1.

After creating Backup1, you perform the following changes to VM1:

- Modify the size of VM1.
- Copy a file named Budget.xls to a folder named Data.
- reset the password for the built-in administrator account.
- Add a data disk to VM1.

An administrator uses the Replace existing option to restore VM1 from Backup1.

You need to ensure that all the changes to VM1 are restored.

Which change should you perform again?

- A. Modify the size of VM1.
- B. Reset the password for the built-in administrator account.
- C. Add a data disk. Most Voted
- D. Copy Budget.xls to Data. Most Voted

[Hide Solution](#)

[Discussion 29](#)

**Correct Answer:** D 

Reference:

<https://docs.microsoft.com/en-us/azure/backup/about-azure-vm-restore>

*Community vote distribution*

D (62%)

C (38%)

The correct answer is D, i.e., copy the file again.

- A. You don't need to resize the VM after backup. The latest size will be applicable.
- B. The latest credentials will work.
- C. This one is a bit ambiguous. The additional data disk will not be deleted after the restoration. However, you will have to attach it again to the VM.
- D. The file will be lost and needs to be created again.

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

| Name  | Member of      | Role assigned      |
|-------|----------------|--------------------|
| User1 | Group1         | <i>None</i>        |
| User2 | Group2         | <i>None</i>        |
| User3 | Group1, Group2 | User administrator |

You enable password reset for contoso.onmicrosoft.com as shown in the Password Reset exhibit. (Click the Password Reset tab.)

Self service password reset enabled ⓘ

None  Selected  All

Select group >

Group2

**i** These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.

You configure the authentication methods for password reset as shown in the Authentication Methods exhibit. (Click the Authentication Methods tab.)

Number of methods required to reset [?](#)

|   |   |
|---|---|
| 1 | 2 |
|---|---|

Methods available to users

- Mobile app notification
- Mobile app code
- Email
- Mobile phone
- Office phone
- Security questions

Number of questions required to register [?](#)

|   |   |   |
|---|---|---|
| 3 | 4 | 5 |
|---|---|---|

Number of questions required to reset [?](#)

|   |   |   |
|---|---|---|
| 3 | 4 | 5 |
|---|---|---|

---

Select security questions [>](#)

10 security questions selected

---

**i** These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.

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

### Answer Area

| Statements   | Yes                   | No                               |
|--|-----------------------|----------------------------------|
| After User2 answers three security questions correctly, he can reset his password immediately. | <input type="radio"/> | <input checked="" type="radio"/> |
| If User1 forgets her password, she can reset the password by using the mobile phone app.       | <input type="radio"/> | <input checked="" type="radio"/> |
| User3 can add security questions to the password reset process                                 | <input type="radio"/> | <input checked="" type="radio"/> |

Box 1: No

Two methods are required (Mobile phone and Security questions).

Box 2: No

Self-service password reset is only enabled for Group2, and User1 is not a member of Group2.

Box 3: No

To be able to add Security questions to the process, you need to be a Global Administrator. User3 is User Administrator, so User3 cannot add security questions to the reset process. User Administrator doesn't have MFA permissions.

Question #10

Topic 6

Your company has a main office in London that contains 100 client computers.

Three years ago, you migrated to Azure Active Directory (Azure AD).

The company's security policy states that all personal devices and corporate-owned devices must be registered or joined to Azure AD.

A remote user named User1 is unable to join a personal device to Azure AD from a home network.

You verify that User1 was able to join devices to Azure AD in the past.

You need to ensure that User1 can join the device to Azure AD.

What should you do?

- A. Assign the User administrator role to User1.
- B. From the Device settings blade, modify the Maximum number of devices per user setting. **Most Voted**
- C. Create a point-to-site VPN from the home network of User1 to Azure.
- D. From the Device settings blade, modify the Users may join devices to Azure AD setting.

[Hide Solution](#)

[Discussion 23](#)

Correct Answer: B 

You have two Azure App Service app named App1 and App2. Each app has a production deployment slot and a test deployment slot.

The Backup Configuration settings for the production slots are shown in the following table.

| App  | Backup Every | Start backup schedule from | Retention (Days) | Keep at least one backup |
|------|--------------|----------------------------|------------------|--------------------------|
| App1 | 1 Days       | January 6, 2021            | 0                | Yes                      |
| App2 | 1 Days       | January 6, 2021            | 30               | Yes                      |

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

## Answer Area

| Statements   | Yes                              | No                               |
|--|----------------------------------|----------------------------------|
| On January 15, 2021, App1 will have only one backup in storage.  | <input type="radio"/>            | <input checked="" type="radio"/> |
| On February 6, 2021, you can access the backup of the App2 test slot from January 15, 2021.                | <input type="radio"/>            | <input checked="" type="radio"/> |
| On January 15, 2021, you can restore the App2 production slot backup from January 6 to the App2 test slot. | <input checked="" type="radio"/> | <input type="radio"/>            |

1 -- N

If you go to Azure Portal -> App Service -> Backups then Set Schedule -> Retention you have information "Keep your backup files for up to 30 days, or enter 0 to keep them indefinitely", so there will be 9 backups.

2 — N

Test slot doesn't have any backups configured

3 – Y

From Azure Portal -> Backups -> Select backup and click 'Restore' -> you have "Choose destination" where you can choose App Service and Deployment slot (new or existing).

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant is synced to the on-premises Active Directory domain. The domain contains the users shown in the following table.

| Name       | Role                   |
|------------|------------------------|
| SecAdmin1  | Security administrator |
| BillAdmin1 | Billing administrator  |
| User1      | Reports reader         |

You enable self-service password reset (SSPR) for all users and configure SSPR to have the following authentication methods:

- Number of methods required to reset: 2
- Methods available to users: Mobile phone, Security questions
- Number of questions required to register: 3
- Number of questions required to reset: 3

You select the following security questions:

- What is your favorite food?
- In what city was your first job?
- What was the name of your first pet?

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

### Answer Area

| Statements   | Yes                              | No                               |
|--|----------------------------------|----------------------------------|
| SecAdmin1 must answer the following question during the self-service password reset:<br>In what city was your first job? | <input type="radio"/>            | <input checked="" type="radio"/> |
| BillAdmin1 must answer the following question during the self-service password reset:<br>What is your favorite food?     | <input type="radio"/>            | <input checked="" type="radio"/> |
| User1 must answer the following question during the self-service password reset:<br>What was the name of your first pet? | <input checked="" type="radio"/> | <input type="radio"/>            |

By default, administrator accounts are enabled for self-service password reset, and a strong default two-gate password reset policy is enforced. This policy may be different from the one you have defined for your users, and this policy can't be changed. You should always test password reset functionality as a user without any Azure administrator roles assigned.

With a two-gate policy, administrators don't have the ability to use security questions.

The two-gate policy requires two pieces of authentication data, such as an email address, authenticator app, or a phone number.

Therefore I would say N N Y as SecAdmin1 and BillAdmin1 are both administrators

#### Question #13

#### Topic 6

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

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

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

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

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

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

Solution: You instruct User1 to create the user accounts.

Does that meet the goal?

A. Yes Most Voted



B. No Most Voted

[Hide Solution](#)

[Discussion](#) 68

Correct Answer: A

**Question #14****Topic 6**

You have an existing Azure subscription that contains 10 virtual machines.

You need to monitor the latency between your on-premises network and the virtual machines.

What should you use?

- A. Service Map
- B. Connection troubleshoot
- C. Network Performance Monitor **Most Voted**
- D. Effective routes

**Hide Solution****Discussion 24****Correct Answer:** C 🎉

You have an Azure App Service plan named ASP1.  
CPU usage for ASP1 is shown in the following exhibit



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

## Answer Area

The average CPU percentage is calculated [answer choice] per day

|            |   |
|------------|---|
|            | ▼ |
| once       |   |
| four times |   |
| six times  |   |
| 24 times   |   |

ASP1 must be [answer choice] to optimize CPU usage

|             |   |
|-------------|---|
|             | ▼ |
| scaled up   |   |
| scaled down |   |
| scaled out  |   |

Look at the top right you can see it is auto updated every 6 hours so within 24hours it is checked 4 times ( $4 \times 6 = 24$ h) . It would need to scale up to have a bigger CPU to support the load that is getting as it is currently 100%

Box 1: look at the top right of the picture it says 6 hours so  $24\text{hours}/6\text{hours} = 4$  times

Box 2: This is App so you scale up only.

You have an Azure Linux virtual machine that is protected by Azure Backup. One week ago, two files were deleted from the virtual machine. You need to restore the deleted files to an on-premises Windows Server 2016 computer as quickly as possible. Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

**Actions**

- From the Azure portal, click **Restore VM** from the vault
- Mount a VHD
- Copy the files by using AZCopy

**Answer Area**

From the Azure portal, click **File Recovery** from the vault

Select a restore point that contains the deleted files

Download and run the script to mount a drive on the local computer

Copy the files by using File Explorer



Step 1: From the Azure portal, click File Recovery from the vault.

Step 2. Select a restore point that contains the deleted files

Step 3: Download and run the script to mount a drive on the local computer -Windows 2016, when you run it will download VHD and automatically mount it then you just need explorer to find the files

Step 4. Copy the files by using Explorer

You purchase a new Azure subscription named Subscription1.

You create a virtual machine named VM1 in Subscription1. VM1 is not protected by Azure Backup.

You need to protect VM1 by using Azure Backup. Backups must be created at 01:00 and stored for 30 days.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

Location in which to store the backups:

|                           |
|---------------------------|
| A blob container          |
| A file share              |
| A Recovery Services vault |
| A storage account         |

Object to use to configure the protection for VM1:

|                  |
|------------------|
| A backup policy  |
| A batch job      |
| A batch schedule |
| A recovery plan  |

## Question #18

Topic 6

You have an Azure virtual machine named VM1.

Azure collects events from VM1.

You are creating an alert rule in Azure Monitor to notify an administrator when an error is logged in the System event log of VM1.

Which target resource should you monitor in the alert rule?

- A. virtual machine extension
- B. virtual machine
- C. metric alert

D. Azure Log Analytics workspace Most Voted

[Hide Solution](#)

[Discussion 30](#)

**Correct Answer:** D 

For the first step to create the new alert rule, under the Create Alert section, you are going to select your Log Analytics workspace as the resource, since this is a log based alert signal.

Reference:

<https://docs.microsoft.com/en-us/windows-server/storage/storage-spaces/configure-azure-monitor>

*Community vote distribution*

D (100%)

## Question #19

Topic 6

You have an Azure subscription that contains 100 virtual machines.

You regularly create and delete virtual machines.

You need to identify unattached disks that can be deleted.

What should you do?

- A. From Azure Cost Management, view Cost Analysis
- B. From Azure Advisor, modify the Advisor configuration
- C. From Microsoft Azure Storage Explorer, view the Account Management properties

D. From Azure Cost Management, view Advisor Recommendations Most Voted

[Hide Solution](#)

[Discussion 20](#)

**Correct Answer:** D 

Correct Answer: D

From Home -> Cost Management + Billing -> Cost Management, scroll down on the options and select View Recommendations

## Question #20

Topic 6

You have an Azure web app named webapp1.

Users report that they often experience HTTP 500 errors when they connect to webapp1.

You need to provide the developers of webapp1 with real-time access to the connection errors. The solution must provide all the connection error details.

What should you do first?

- A. From webapp1, enable Web server logging
- B. From Azure Monitor, create a workbook
- C. From Azure Monitor, create a Service Health alert
- D. From webapp1, turn on Application Logging

[Hide Solution](#)

[Discussion 35](#)

**Correct Answer:** A 🎉

*Community vote distribution*

A (100%)

## Question #21

Topic 6

You have an Azure web app named App1.

You need to monitor the availability of App1 by using a multi-step web test.

What should you use in Azure Monitor?

- A. Azure Service Health
- B. Azure Application Insights **Most Voted**
- C. the Diagnostic settings
- D. metrics

[Hide Solution](#)

[Discussion 6](#)

**Correct Answer:** B 🎉

Upload the web test -

1. In the Application Insights portal on the Availability pane select Add Classic test, then select Multi-step as the SKU.
2. Upload your multi-step web test.
3. Set the test locations, frequency, and alert parameters.
4. Select Create.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/availability-multistep>

*Community vote distribution*

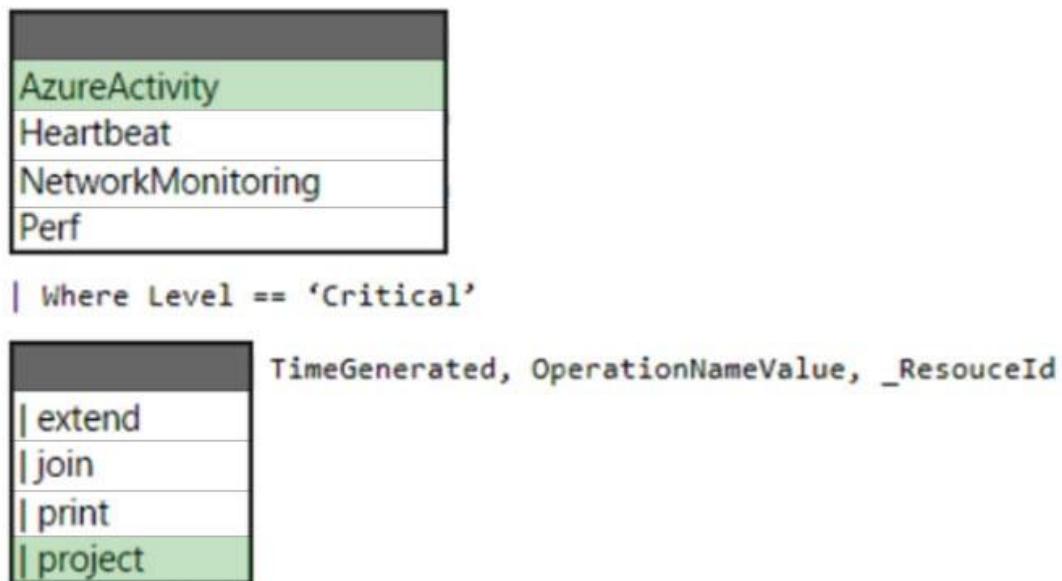
B (100%)

You have an Azure subscription that has diagnostic logging enabled and is configured to send logs to a Log Analytics workspace. You are investigating a service outage.

You need to view the event time, the event name, and the affected resources.

How should you complete the query? To answer, select the appropriate options in the answer area.

## Answer Area



Box 1: AzureActivity

The AzureActivity table has entries from the Azure activity log, which provides insight into subscription-level or management group-level events occurring in Azure. Let's see only Critical entries during a specific week.

Box 2: | project

Use project to include only the columns you want. Building on the preceding example, let's limit the output to certain columns

You have a Recovery Services vault named RSV1. RSV1 has a backup policy that retains instant snapshots for five days and daily backup for 14 days.

RSV1 performs daily backups of VM1. VM1 hosts a static website that was updated eight days ago.

You need to recover VM1 to a point eight days ago. The solution must minimize downtime.

What should you do first?

- A. Deallocate VM1.
- B. Restore VM1 by using the Replace existing restore configuration option.
- C. Delete VM1.
- D. Restore VM1 by using the Create new restore configuration option. **Most Voted**

Answer should be D

Restore option Details Create a new VM Quickly creates and gets a basic VM up and running from a restore point.

The B options needs you to shut down the VM first, causing downtime. We must minimize downtime.

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

| Name       | Type                    |
|------------|-------------------------|
| VM1        | Virtual machine         |
| storage1   | Storage account         |
| Workspace1 | Log Analytics workspace |
| DB1        | Azure SQL database      |

You plan to create a data collection rule named DCR1 in Azure Monitor.

Which resources can you set as data sources in DCR1, and which resources can you set as destinations in DCR1? To answer, select the appropriate options in the answer

### Answer Area

Data sources:

- VM1 only
- VM1 and storage1 only
- VM1, storage1, and DB1 only
- VM1, storage1, Workspace1, and DB1

Destinations:

- storage1 only
- Workspace1 only
- Workspace1 and storage1 only
- Workspace1, storage1, and DB1 only

Correct answer.

First: You can only choose VM

Second: Only Workspace

You have the role assignment file shown in the following exhibit.

```
[  
 {  
   "RoleAssignmentId": "e3108585-0e5d-4572-91a3-aa5d2df73999",  
   "Scope": "/subscriptions/fb960108-fcdc-499b-886e-d9c31d3f26ff",  
   "DisplayName": "User1",  
   "SignInName": "User1@contoso.onmicrosoft.com",  
   "RoleDefinitionName": "Owner",  
   ...  
 },  
 {  
   "RoleAssignmentId": "3bab4763-16a9-4d5d-9fcf-eccc31a21e",  
   "Scope": "/subscriptions/fb960108-fcdc-499b-886e-d9c31d3f26ff/resourceGroups/RG2",  
   "DisplayName": "User2",  
   "SignInName": "User2@contoso.onmicrosoft.com",  
   "RoleDefinitionName": "Owner",  
   ...  
 },  
 {  
   "RoleAssignmentId": "a071c023-40a3-4b7f-8680-1109b40270c5",  
   "Scope": "/subscriptions/fb960108-fcdc-499b-886e-d9c31d3f26ff/resourceGroups/RG1/providers/  
Microsoft.Compute/virtualMachines/VM1",  
   "DisplayName": "User3",  
   "SignInName": "User3@contoso.onmicrosoft.com",  
   "RoleDefinitionName": "Owner",  
   ...  
 },  
 {  
   "RoleAssignmentId": "c5b9e7da-76d4-4888-93b5-8afb2bb780b4",  
   "Scope": "/subscriptions/fb960108-fcdc-499b-886e-d9c31d3f26ff/resourceGroups/RG1",  
   "DisplayName": "User4",  
   "SignInName": "User4@contoso.onmicrosoft.com",  
   "RoleDefinitionName": "Contributor",  
   ...  
 }]
```

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

### Answer Area

[Answer choice] assigned the Owner role for VM1

|                                |   |
|--------------------------------|---|
|                                | ▼ |
| User3 is                       |   |
| User3 and User4 are            |   |
| User1 and User3 are            |   |
| User1, User3, and User4 are    |   |
| User1, User2, User3, and User4 |   |

[Answer choice] can create a virtual machine in RG1

|                                |   |
|--------------------------------|---|
|                                | ▼ |
| User1 and User4                |   |
| User1, User2, and User3        |   |
| User1, User2, and User4        |   |
| User1, User3, and User4        |   |
| User1, User2, User3, and User4 |   |

Answers are correct:

User1 - Owner of the subscription. (He can manage any resources in the subscription.)

User 2 - Owner of RG2 (He can manage any resources in the RG2.)

User 3 - Owner of a single VM that is VM1. (He can manage VM1 only)

User 4 - Contributor of RG1. (He can manage everything in RG1, even he can delete VMs in RG1. But cannot change RABC)

Box1: Owner of VM1 - User1, User3

Box2: Create VM in RG1 - User1, User4

You have the following custom role-based access control (RBAC) role.

```
{  
  "id": "b988327b-7dae-4d00-8925-1cc14fd68be4",  
  "properties": {  
    "roleName": "Role1",  
    "description": "",  
    "assignableScopes": [  
      "/subscriptions/c691ad84-99f2-42fd-949b-58af7ef6ab3"  
    ],  
    "permissions": [  
      {  
        "actions": [  
          "Microsoft.Resources/subscription/resourceGroups/resources/read",  
          "Microsoft.Resources/subscription/resourceGroups/read",  
          "Microsoft.Resourcehealth/*",  
          "Microsoft.Authorization/*/read",  
          "Microsoft.Compute/*/read",  
          "Microsoft.Support/*",  
          "Microsoft.Authorization/*/read",  
          "Microsoft.Network/virtualNetworks/read",  
          "Microsoft.Resources/deployments/*",  
          "Microsoft.Resources/subscription/resourceGroups/read",  
          "Microsoft.Storage/storageAccounts/read",  
          "Microsoft.Compute/virtualMachines/start/action",  
          "Microsoft.Compute/virtualMachines/powerOff/action",  
          "Microsoft.Compute/virtualMachines/deallocate/action",  
          "Microsoft.Compute/virtualMachines/restart/action",  
          "Microsoft.Compute/virtualMachines/*",  
          "Microsoft.Compute/disks/*",  
          "Microsoft.Compute/availabilitySets/*",  
          "Microsoft.Network/virtualNetworks/subnets/join/action",  
          "Microsoft.Network/virtualNetworks/subnets/read",  
          "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",  
          "Microsoft.Network/networkInterfaces/*",  
          "Microsoft.Compute/snapshots/*"  
        ]  
      },  
      "notAction": [  
        "Microsoft.Authorization/*/Delete",  
        "Microsoft.Authorization/*/Write",  
        "Microsoft.Authorization/elevateAccess/Action"  
      ]  
    ]  
  }  
}
```

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

### Answer Area

| Statements  | Yes                              | No                               |
|---|----------------------------------|----------------------------------|
| Users that are assigned Role1 can assign Role1 to users.                        | <input type="radio"/>            | <input checked="" type="radio"/> |
| Users that are assigned Role1 can deploy new virtual machines.                  | <input checked="" type="radio"/> | <input type="radio"/>            |
| Users that are assigned Role1 can set a static IP address on a virtual machine. | <input checked="" type="radio"/> | <input type="radio"/>            |

Microsoft.Compute/virtualMachines/\* Perform all virtual machine actions including create, update, delete, start, restart, and power off virtual machines. Execute scripts on virtual machines.

N - ms.auth/\*/write is NOT allowed.

Y - ms.comp/vm/\* is allowed.

Y - ms.net/netint/\* is allowed.

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

| Name     | Type                        | Description                  |
|----------|-----------------------------|------------------------------|
| VNET1    | Virtual network             | Contains subnet1 and subnet2 |
| subnet1  | Subnet                      | IP address space 10.3.0.0/24 |
| subnet2  | Subnet                      | IP address space 10.4.0.0/24 |
| NSG1     | Network security group (NS) | None                         |
| vm1      | Virtual machine             | IP address 10.3.0.15         |
| vm2      | Virtual machine             | IP address 10.4.0.16         |
| storage1 | Storage account             | None                         |

NSG1 is configured as shown in the following exhibit.

^ Essentials JSON View

|   |   |
|---|---|
| Resource group (change) : RG1                       | Custom security rules : 1 inbound, 2 outbound     |
| Location : East US 2                                | Associated with : 1 subnets, 0 network interfaces |
| Subscription (change) : Microsoft Azure Sponsorship |   |
| Subscription ID :                                   |   |
| Tags (change) : Click here to add tags              |   |

▼ Inbound security rules

| Priority | Name                          | Port | Protocol | Source            | Destination    | Action                                    |
|----------|-------------------------------|------|----------|-------------------|----------------|---|
| 110      | HTTPS_VM1_Deny                | 443  | TCP      | Internet          | 10.3.0.15      | <input checked="" type="checkbox"/> Deny  |
| 65000    | AllowVnetInBound              | Any  | Any      | VirtualNetwork    | VirtualNetwork | <input checked="" type="checkbox"/> Allow |
| 65001    | AllowAzureLoadBalancerInBound | Any  | Any      | AzureLoadBalancer | Any            | <input checked="" type="checkbox"/> Allow |
| 65500    | DenyAllInBound                | Any  | Any      | Any               | Any            | <input checked="" type="checkbox"/> Deny  |

▼ Outbound security rules

| Priority | Name                  | Port | Protocol | Source         | Destination    | Action                                    |
|----------|-----------------------|------|----------|----------------|----------------|---|
| 145      | Storage_Access        | 443  | TCP      | VirtualNetwork | Storage        | <input checked="" type="checkbox"/> Allow |
| 150      | Block_Internet        | Any  | Any      | VirtualNetwork | Internet       | <input checked="" type="checkbox"/> Deny  |
| 65000    | AllowVnetOutBound     | Any  | Any      | VirtualNetwork | VirtualNetwork | <input checked="" type="checkbox"/> Allow |
| 65001    | AllowInternetOutBound | Any  | Any      | Any            | Internet       | <input checked="" type="checkbox"/> Allow |
| 65500    | DenyAllOutBound       | Any  | Any      | Any            | Any            | <input checked="" type="checkbox"/> Deny  |

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

### Answer Area

| Statements   | Yes                              | No                               |
|--|----------------------------------|----------------------------------|
| VM1 can access storage1.   | <input checked="" type="radio"/> | <input type="radio"/>            |
| VM2 can access VM1 by using the HTTPS protocol.                    | <input checked="" type="radio"/> | <input type="radio"/>            |
| The security rules for NSG1 apply to any virtual machine on VNET1. | <input type="radio"/>            | <input checked="" type="radio"/> |

I'm assuming that the NSG is applied to Subnet1.

Y. Outbound rules have 145 priority for allow storage1 access

Y. Inbound rules has default VNet to VNet allow so VM2 can access VM1. The deny rule 110 is for Internet traffic coming in.

N. We can see the NSG is associated to 1 subnet from the image.

Question #29

Topic 6

You have two Azure subscriptions named Sub1 and Sub2. Sub1 is in a management group named MG1. Sub2 is in a management group named MG2.

You have the resource groups shown in the following table.

| Name | Subscription |
|------|--------------|
| RG1  | Sub1         |
| RG2  | Sub2         |

You have the virtual machines shown in the following table.

| Name | Resource group |
|------|----------------|
| VM1  | RG1            |
| VM2  | RG2            |
| VM3  | RG2            |

You assign roles to users as shown in the following table.

| User  | Role                        | Resource |
|-------|-----------------------------|----------|
| User1 | Virtual Machine Contributor | MG1      |
| User1 | Virtual Machine User Login  | Sub2     |
| User2 | Virtual Machine Contributor | MG2      |
| User2 | Virtual Machine User Login  | Sub1     |
| User2 | Virtual Machine User Login  | VM3      |

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

### Answer Area

| Statements  | Yes                   | No                    |
|---|-----------------------|-----------------------|
| User1 can sign in to VM1.                         | <input type="radio"/> | <input type="radio"/> |
| User2 can manage disks and disk snapshots of VM1. | <input type="radio"/> | <input type="radio"/> |
| User2 can manage disks and disk snapshots of VM3. | <input type="radio"/> | <input type="radio"/> |

N - Effective rights are virtual machine contributor. This doesn't grant login.

N - Effective rights are virtual machine login. This doesn't grant disk management.

N - Effective rights are virtual machine contributor. This does not grant snapshot access.

=====

N - To sign in you need "VM user login". So. NOT to VM1 coz VM1 is in Sub1 > RG1.

N - User2 is VM contributor on MG2 > Sub2 > VM2. Not VM1.

N - User2 is VM contributor on MG2 > Sub2 > VM3. But apparently contributor cannot do disk snapshot.

You have an Azure Active Directory (Azure AD) tenant that is linked to 10 Azure subscriptions.

You need to centrally monitor user activity across all the subscriptions.

What should you use?

A. Azure Application Insights Profiler

B. access reviews

C. Activity log filters

D. a Log Analytics workspace Most Voted

[Hide Solution](#)

[Discussion](#) 9

**Correct Answer:** D 

*Community vote distribution*

D (100%)

You have an Azure subscription that contains a virtual machine name VM1. VM1 has an operating system disk named Disk1 and a data disk named Disk2. You need to back up Disk2 by using Azure Backup.

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

**Actions**

|                                    |
|------------------------------------|
|                                    |
|                                    |
| Create a Recovery Services vault   |
| Delegate permissions for the vault |
|                                    |

**Answer Area**

|   |
|---|
| Create an Azure Backup vault                    |
| Create a backup policy and configure the backup |
| Configure a managed identity                    |



Azure Recovery Services vaults can protect the following types of data sources:

Azure Virtual machines,

SQL in Azure VM

Azure Files (Azure Storage)

SAP HANA in Azure VM

Azure Backup Server

Azure Backup Agent

DPM

Azure Backup vaults can protect the following types of data sources:

Azure Database for PostgreSQL servers

Azure Blobs (Azure Storage)

Azure Disks

Kubernetes Service

AVS Virtual machines

- 1- Create an Azure backup vault.
- 2- Create a backup policy and configure the backup
- 3- Configure a managed identity

**Azure disk backup: Backup vault uses managed identity to access other Azure resources.**

Question #32

Topic 6

You have a subnet named Subnet1 that contains Azure virtual machines. A network security group (NSG) named NSG1 is associated to Subnet1. NSG1 only contains the default rules.

You need to create a rule in NSG1 to prevent the hosts on Subnet1 from connecting to the Azure portal. The hosts must be able to connect to other internet hosts.

To what should you set Destination in the rule?

- A. Application security group
- B. IP Addresses
- C. Service Tag **Most Voted**
- D. Any

[Hide Solution](#)

[Discussion 7](#)

Correct Answer: C 

Community vote distribution

C (100%)

C - "Azure portal" is in the list of Service tag.

You can use service tags to achieve network isolation and protect your Azure resources from the general Internet while accessing Azure services that have public endpoints.

### Question #33

Topic 6

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

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

Which query should you run in Workspace1?

A. search in (Event) "error" **Most Voted**

B. Event | where EventType is "error"

C. select \* from Event where EventType == "error"

D. Get-Event Event | where (\$\_.EventType == "error")

[Hide Solution](#)

[Discussion 4](#)

**Correct Answer:** A 

*Community vote distribution*

A (100%)

### Question #34

Topic 6

You have an Azure App Service web app named App1.

You need to collect performance traces for App1.

What should you use?

A. Azure Application Insights Profiler **Most Voted**

B. the Activity log

C. the Deployment center

D. the Diagnose and solve problems settings

[Hide Solution](#)

[Discussion 10](#)

**Correct Answer:** B 

*Community vote distribution*

A (100%)

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

| Name     | Kind             | Location   |
|----------|------------------|------------|
| storage1 | StorageV2        | Central US |
| storage2 | BlobStorage      | West US    |
| storage3 | BlockBlobStorage | West US    |
| storage4 | FileStorage      | East US    |

You deploy a web app named App1 to the West US Azure region.

You need to back up App1. The solution must minimize costs.

Which storage account should you use as the target for the backup?

A. storage1

B. storage2

C. storage3

D. storage4

[Hide Solution](#)

[Discussion](#) 6

Correct Answer: D 

Community vote distribution

A (67%)

B (33%)

You have an Azure subscription that is linked to an Azure AD tenant. The tenant contains two users named User1 and User2.

The subscription contains the resources shown in the following table.

| Name | Type            | Description    |
|------|-----------------|----------------|
| RG1  | Resource group  | None           |
| VM1  | Virtual machine | Created in RG1 |

The subscription contains the alert rules shown in the following table.

| Name   | Scope | Condition                     |
|--------|-------|-------------------------------|
| Alert1 | RG1   | All Administrative operations |
| Alert2 | VM1   | All Administrative operations |

The users perform the following action:

- User1 creates a new virtual disk and attaches the disk to VM1
- User2 creates a new resource tag and assigns the tag to RG1 and VM1

Which alert rules are triggered by each user? To answer, select the appropriate options in the answer area.

## Answer Area

User1:

|                                 |                                     |
|---------------------------------|-------------------------------------|
| No alert is triggered           | ▼                                   |
| Only Alert1 is triggered        |                                     |
| Only Alert2 is triggered        | <input checked="" type="checkbox"/> |
| Alert1 and Alert2 are triggered |                                     |

User2:

|                                 |                                     |
|---------------------------------|-------------------------------------|
| No alert is triggered           | ▼                                   |
| Only Alert1 is triggered        |                                     |
| Only Alert2 is triggered        | <input checked="" type="checkbox"/> |
| Alert1 and Alert2 are triggered | <input checked="" type="checkbox"/> |

You have an Azure subscription that contains eight virtual machines and the resources shown in the following table.

| Name      | Description  |
|-----------|--|
| storage1  | Storage account  |
| storage2  | Storage account  |
| KeyVault1 | Key vault  |
| VNET1     | Virtual network with a single subnet that has five virtual machines connected  |
| VNET2     | Virtual network with a single subnet that has three virtual machines connected |

You need to configure access for VNET1. The solution must meet the following requirements:

- The virtual machines connected to VNET1 must be able to communicate with the virtual machines connected to VNET2 by using the Microsoft backbone.
- The virtual machines connected to VNET1 must be able to access storage1, storage2, and Azure AD by using the Microsoft backbone.

What is the minimum number of service endpoints you should add to VNET1?

A. 1

B. 2 **Most Voted** 

C. 3

D. 5

**Hide Solution**

 Discussion 3

**Correct Answer: D** 

*Community vote distribution*

 B (100%)

### Question #39

You need to configure an Azure web app named contoso.azurewebsites.net to host www.contoso.com.

What should you do first?

- A. Create A records named www.contoso.com and asuid.contoso.com. 
- B. Create a TXT record named asuid that contains the domain verification ID.
- C. Create a CNAME record named asuid that contains the domain verification ID.
- D. Create a TXT record named www.contoso.com that has a value of contoso.azurewebsites.net.

[Hide Solution](#)

 Discussion 5

### Question #40

Topic 6

You have an Azure subscription that contains 10 network security groups (NSGs), 10 virtual machines, and a Log Analytics workspace named Workspace1. Each NSG is connected to a virtual machine.

You need to configure an Azure Monitor Network Insights alert that will be triggered when suspicious network traffic is detected.

What should you do first?

- A. Deploy Connection Monitor.
- B. Configure data collection endpoints.
- C. Configure a private link.
- D. Configure NSG flow logs.

[Hide Solution](#)

 Discussion 2

**Correct Answer: D** 

*Community vote distribution*

D (100%)

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

| Name    | Description  |
|---------|--|
| RG1     | Resource group   |
| Action1 | Action group that sends an email message to admin1@contoso.com |

Sub1 contains the following alert rule:

- Name: Alert1
- Scope: All resource groups in Sub1
- o Include all future resources
- Condition: All administrative operations
- Actions: Action1

Sub1 contains the following alert processing rule:

- Name: Rule1
- Scope: Sub1
- Rule type: Suppress notifications
- Apply the rule: On a specific time
  - o Start: August 10, 2022
  - o End: August 13, 2022

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

| Statements   | Yes                              | No                               |
|--|----------------------------------|----------------------------------|
| If you create a resource group in Sub1 on August 11, 2022, Alert1 is listed in the Azure portal.           | <input checked="" type="radio"/> | <input type="radio"/>            |
| If you create a resource group in Sub1 on August 12, 2022, an email message is sent to admin1@contoso.com. | <input type="radio"/>            | <input checked="" type="radio"/> |
| If you add a tag to RG1 on August 15, 2022, an email message is sent to admin1@contoso.com.                | <input checked="" type="radio"/> | <input type="radio"/>            |

## **Introductory Info**

Case study –

Overview –

Contoso, Ltd. is a manufacturing company that has offices worldwide. Contoso works with partner organizations to bring products to market.

Contoso products are manufactured by using blueprint files that the company authors and maintains.

Existing Environment –

Currently, Contoso uses multiple types of servers for business operations, including the following:

File servers

Domain controllers

Microsoft SQL Server servers

Your network contains an Active Directory forest named contoso.com. All servers and client computers are joined to Active Directory.

You have a public-facing application named App1. App1 is comprised of the following three tiers:

A SQL database

A web front end

A processing middle tier –

Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.

Requirements –

Planned Changes –

Contoso plans to implement the following changes to the infrastructure:

Move all the tiers of App1 to Azure.

Move the existing product blueprint files to Azure Blob storage.

Create a hybrid directory to support an upcoming Microsoft 365 migration project.

Technical Requirements –

Contoso must meet the following technical requirements:

Move all the virtual machines for App1 to Azure.

Minimize the number of open ports between the App1 tiers.

Ensure that all the virtual machines for App1 are protected by backups.

Copy the blueprint files to Azure over the Internet.

Ensure that the blueprint files are stored in the archive storage tier.

Ensure that partner access to the blueprint files is secured and temporary.

Prevent user passwords or hashes of passwords from being stored in Azure.

Use unmanaged standard storage for the hard disks of the virtual machines.

Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile

phone to verify their identity.

Minimize administrative effort whenever possible.

User Requirements -

Contoso identifies the following requirements for users:

Ensure that only users who are part of a group named Pilot can join devices to Azure AD.

Designate a new user named Admin1 as the service admin for the Azure subscription.

Admin1 must receive email alerts regarding service outages.

Ensure that a new user named User3 can create network objects for the Azure subscription.

### **Question-1**

You need to configure the Device settings to meet the technical requirements and the user requirements.

Which two settings should you modify? To answer, select the appropriate settings in the answer area.

## Answer Area

|  |   |   |
|--|---|---|
|  Save         |  Discard |  Got feedback? |
| <b>Users may join devices to Azure AD</b> ⓘ  |   |   |
| <input checked="" type="radio"/> All <input type="radio"/> Selected <input type="radio"/> None |   |   |
| Selected   |   |   |
| No member selected   |   |   |
| <b>Additional local administrators on Azure AD joined devices</b> ⓘ                            |   |   |
| <input type="radio"/> Selected <input checked="" type="radio"/> None                           |   |   |
| Selected   |   |   |
| No member selected   |   |   |
| <b>Users may register their devices with Azure AD</b> ⓘ  |   |   |
| <input checked="" type="radio"/> All <input type="radio"/> None                                |   |   |
| <b>Require Multi-Factor Auth to join devices</b> ⓘ   |   |   |
| <input type="radio"/> Yes <input checked="" type="radio"/> No                                  |   |   |
| <b>Maximum number of devices per user</b> ⓘ  |   |   |
| 50   |   |   |

Box 1: Selected

As per User requirements "Ensure that only users who are part of a group named Pilot can join devices to Azure AD." So, "Selected" must be selected for "User may join devices to Azure AD"

Box 2: Yes

As per User Requirements "Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity". So, "Yes" must be selected for "Require Multi-Factor Auth to join devices".

## Question-2

You need to meet the user requirement for Admin1.  
What should you do?

- A. From the Azure Active Directory blade, modify the Groups
- B. From the Azure Active Directory blade, modify the Properties
- C. From the Subscriptions blade, select the subscription, and then modify the Access control (IAM) settings Most Voted
- D. From the Subscriptions blade, select the subscription, and then modify the Properties Most Voted 

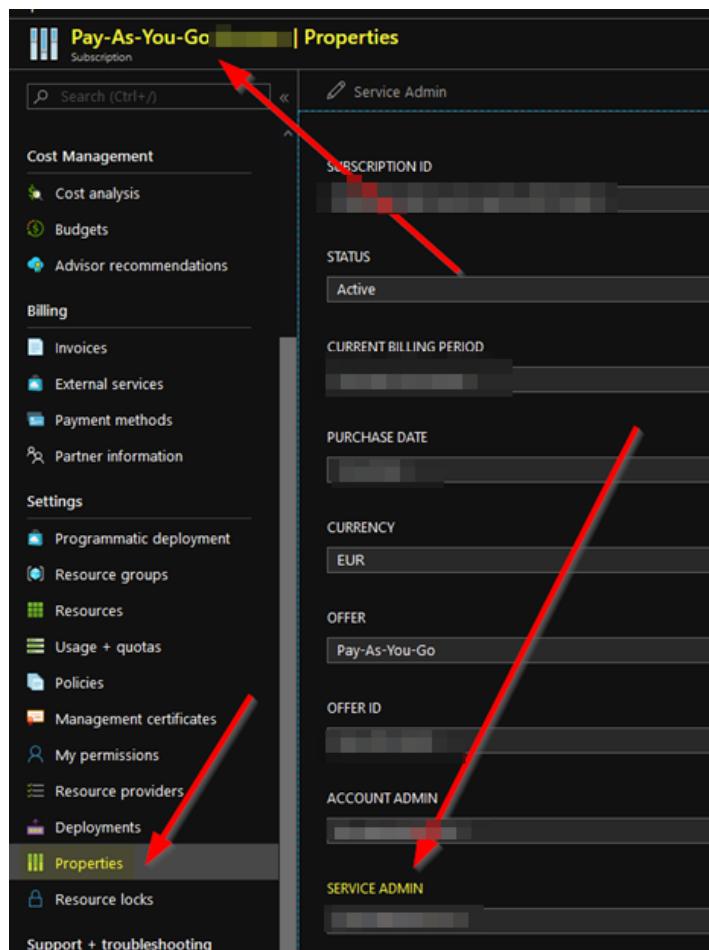
[Hide Solution](#)

[Discussion \(73\)](#)

Correct Answer: D 

Correct Answer: D

As per User Requirements "Designate a new user named Admin1 as the service admin for the Azure subscription." So, In the Azure portal, you can view or change the Service Administrator or view the Account Administrator on the properties blade of your subscription.



## Topic 8 - Testlet 10

Overview -

General Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York.

Environment -

Existing Environment -

Contoso has an Azure subscription named Sub1 that is linked to an Azure Active Directory (Azure AD) tenant.

The network contains an on-premises Active

Directory domain that syncs to the Azure AD tenant.

The Azure AD tenant contains the users shown in the following table.

| Name  | Type   | Role        |
|-------|--------|-------------|
| User1 | Member | <b>None</b> |
| User2 | Guest  | <b>None</b> |
| User3 | Member | <b>None</b> |
| User4 | Member | <b>None</b> |

Sub1 contains two resource groups named RG1 and RG2 and the virtual networks shown in the following table.

| Name  | Subnet           | Peered with  |
|-------|------------------|--------------|
| VNET1 | Subnet1, Subnet2 | VNET2        |
| VNET2 | Subnet1          | VNET1, VNET3 |
| VNET3 | Subnet1          | VNET2        |
| VNET4 | Subnet1          | <b>None</b>  |

User1 manages the resources in RG1. User4 manages the resources in RG2.

Sub1 contains virtual machines that run Windows Server 2019 as shown in the following table

| Name | IP address  | Location   | Connected to  |
|------|-------------|------------|---------------|
| VM1  | 10.0.1.4    | West US    | VNET1/Subnet1 |
| VM2  | 10.0.2.4    | West US    | VNET1/Subnet2 |
| VM3  | 172.16.1.4  | Central US | VNET2/Subnet1 |
| VM4  | 192.168.1.4 | West US    | VNET3/Subnet1 |
| VM5  | 10.0.22.4   | East US    | VNET4/Subnet1 |

No network security groups (NSGs) are associated to the network interfaces or the subnets. Sub1 contains the storage accounts shown in the following table.

| Name     | Kind                           | Location   | File share     | Identity-based access for file share                 |
|----------|--------------------------------|------------|----------------|--|
| storage1 | Storage (general purpose v1)   | West US    | sharea         | Azure Active Directory Domain Services (Azure AD DS) |
| storage2 | StorageV2 (general purpose v2) | East US    | shareb, sharec | Disabled   |
| storage3 | BlobStorage                    | East US 2  | Not applicable | Not applicable                                       |
| storage4 | FileStorage                    | Central US | shared         | Azure Active Directory Domain Services (Azure AD DS) |

Requirements -

Planned Changes -

Contoso plans to implement the following changes:

Create a blob container named container1 and a file share named share1 that will use the Cool storage tier.

Create a storage account named storage5 and configure storage replication for the Blob service.

Create an NSG named NSG1 that will have the custom inbound security rules shown in the following table.

| Priority | Port | Protocol | Source      | Destination    | Action |
|----------|------|----------|-------------|----------------|--------|
| 500      | 3389 | TCP      | 10.0.2.0/24 | Any            | Deny   |
| 1000     | Any  | ICMP     | Any         | VirtualNetwork | Allow  |

Associate NSG1 to the network interface of VM1.

Create an NSG named NSG2 that will have the custom outbound security rules shown in the following table.

| Priority | Port | Protocol | Source      | Destination    | Action |
|----------|------|----------|-------------|----------------|--------|
| 200      | 3389 | TCP      | 10.0.0.0/16 | VirtualNetwork | Deny   |
| 400      | Any  | ICMP     | 10.0.2.0/24 | 10.0.1.0/24    | Allow  |

Associate NSG2 to VNET1/Subnet2.

Technical Requirements -

Contoso must meet the following technical requirements:

Create container1 and share1.

Use the principle of least privilege.

Create an Azure AD security group named Group4.

Back up the Azure file shares and virtual machines by using Azure Backup.

Trigger an alert if VM1 or VM2 has less than 20 GB of free space on volume C.

Enable User1 to create Azure policy definitions and User2 to assign Azure policies to RG1.  
Create an internal Basic Azure Load Balancer named LB1 and connect the load balancer to VNET1/Subnet1  
Enable flow logging for IP traffic from VM5 and retain the flow logs for a period of eight months.  
Whenever possible, grant Group4 Azure role-based access control (Azure RBAC) read-only permissions to the Azure file shares.

### Question—1

You need to configure Azure Backup to back up the file shares and virtual machines.  
What is the minimum number of Recovery Services vaults and backup policies you should create? To answer, select the appropriate options in the answer area.

### Answer Area

Recovery Services vaults

|   |   |
|---|---|
|   | ▼ |
| 1 |   |
| 2 |   |
| 3 |   |
| 4 |   |
| 7 |   |

Backup policies

|   |   |
|---|---|
|   | ▼ |
| 1 |   |
| 2 |   |
| 3 |   |
| 4 |   |
| 5 |   |
| 6 |   |

To back up the file shares and virtual machines.

One vault per region. 3 vaults for 3 regions

File shares: 3 region. VMs: 3 region.

So

Vault = 3

Backup policies = 3FS + 3VM = 6

### Question --- 3

You need to configure the alerts for VM1 and VM2 to meet the technical requirements.

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

Select and Place:

| Actions   | Answer Area |
|---|-------------|
| Create a Log Analytics workspace.                                   | ▶           |
| Configure the Diagnostic settings.                                  |             |
| Create an alert rule.   | ◀           |
| Collect Windows performance counters from the Log Analytics agents. |             |
| Create an Azure SQL database.                                       | ↑           |
|   |             |

1. Create a log Analytics workspace.
2. Collect windows performance counters from the Log Analytics agents.
3. Create an alert rule.

## Topic 9 - Testlet 2

<https://www.examtopics.com/exams/microsoft/az-104/view/42/>

### Question

HOTSPOT -

You need to ensure that User1 can create initiative definitions, and User4 can assign initiatives to RG2. The solution must meet the technical requirements.

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

NOTE: Each correct selection is worth one point.

### Answer Area

User1:

|                                      |   |
|--------------------------------------|---|
|                                      | ▼ |
| Contributor for RG1                  |   |
| Contributor for Sub1                 |   |
| Security Admin for RG1               |   |
| Resource Policy Contributor for Sub1 |   |

User4:

|                                     |   |
|-------------------------------------|---|
|                                     | ▼ |
| Contributor for RG2                 |   |
| Contributor for Sub1                |   |
| Security Admin for Sub1             |   |
| Resource Policy Contributor for RG2 |   |

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

## Question

You need to ensure that you can grant Group4 Azure RBAC read only permissions to all the Azure file shares.

What should you do?

- A. On storage2, enable identity-based access for the file shares. **Most Voted**
- B. Recreate storage2 and set Hierarchical namespace to Enabled.
- C. On storage1 and storage4, change the Account kind type to StorageV2 (general purpose v2).
- D. Create a shared access signature (SAS) for storage1, storage2, and storage4.

[Hide Solution](#)

[Discussion](#) 15

**Correct Answer:** A 

I think is A, because storage1 and storage2 have enabled Azure Active Directory Domain services. I think that you have to enable in storage 2 identity-based access for the file shares too.

RBAC = Role Based Access Control and you will give Reader Role so you would need Azure AD for this, no? So A seems like a right answer

SAS does not go by Azure AD groups

The question is RBAC, D is SAS token

## Topic 10 - Testlet 3

<https://www.examtopics.com/exams/microsoft/az-104/view/42/>

### Question-1

You need to implement a backup solution for App1 after the application is moved. What should you create first?

- A. a recovery plan
- B. an Azure Backup Server
- C. a backup policy
- D. a Recovery Services vault

[Hide Solution](#)

[Discussion](#) 28

Correct Answer: D 

### Question-2

You need to move the blueprint files to Azure. What should you do?

- A. Generate an access key. Map a drive, and then copy the files by using File Explorer.
- B. Use Azure Storage Explorer to copy the files.
- C. Use the Azure Import/Export service.
- D. Generate a shared access signature (SAS). Map a drive, and then copy the files by using File Explorer.

[Hide Solution](#)

[Discussion](#) 42

Correct Answer: B 

Azure Storage Explorer is a free tool from Microsoft that allows you to work with Azure Storage data on Windows, macOS, and Linux. You can use it to upload and download data from Azure blob storage. It's the best solution, because copies data through Internet and minimizes administrative effort.

D: You can't use SAS with a mapped drive.

### Question-3

You need to identify the storage requirements for Contoso.

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

### Answer Area

| Statements  | Yes                              | No                               |
|---|----------------------------------|----------------------------------|
| Contoso requires a storage account that supports Blob storage.        | <input checked="" type="radio"/> | <input type="radio"/>            |
| Contoso requires a storage account that supports Azure Table storage. | <input type="radio"/>            | <input checked="" type="radio"/> |
| Contoso requires a storage account that supports Azure File Storage.  | <input type="radio"/>            | <input checked="" type="radio"/> |

As per requirements: - Move the existing product blueprint files to Azure Blob storage.

- Copy the blueprint files to Azure over the Internet.
- Ensure that the blueprint files are stored in the archive storage tier.
- Use unmanaged standard storage for the hard disks of the virtual machines.
- App1 is comprised of SQL database.

Box 1: Yes

Contoso is moving the existing product blueprint files to Azure Blob storage and requires using unmanaged standard storage for the hard disks of the virtual machines. We use Page Blobs for these. As mentioned, move the files to blob storage , in addition the unmanaged storage is used for VM's disks.

Box 2: No

Azure Tables are not needed as they act as structured NoSQL, which is not required with SQL on VM.

Box 3: No

Azure Files is not required here. As it is basically used for managed file shares accessed by NFS or SMB protocols. In addition, you can't archive them.

## Topic 11 - Testlet 4

<https://www.examtopics.com/exams/microsoft/az-104/view/42/>

### Question-1

HOTSPOT -

You need to create container1 and share1.

Which storage accounts should you use for each resource? To answer, select the appropriate options in the answer area.

### Answer Area

container1:

- storage2 only
- storage2 and storage3 only
- storage1, storage2, and storage3 only
- storage2, storage3, and storage4 only
- storage1, storage2, storage3, and storage4

share1:

- storage2 only
- storage4 only
- storage2 and storage4 only
- storage1, storage2, and storage4 only
- storage1, storage2, storage3, and storage4

Storage (general-purpose v1) doesn't support tier.

Standard (general-purpose v2) supports tier for Blob service and for Azure file.

Premium BlockBlobStorage doesn't support tier.

Legacy Standard BlobStorage supports tier.

Premium FileStorage doesn't support tier.

Container1 with tier: Can be created in storage2 (storagev2) and storage3. The question refers to BlobStorage (standard legacy one that supports tier) and not to BlockBlobStorage (Premium one that doesn't support tier).

Share1 with tier: Can be created in storage2 (storagev2) only.

## Question-2

You need to create storage5. The solution must support the planned changes.

Which type of storage account should you use, and which account should you configure as the destination storage account? To answer, select the appropriate options in the answer area.

### Answer Area

|                                |                                  |
|--------------------------------|----------------------------------|
| Account kind:                  | <input type="button" value="▼"/> |
| BlobStorage                    |                                  |
| BlockBlobStorage               |                                  |
| Storage (general purpose v1)   |                                  |
| StorageV2 (general purpose v2) |                                  |

|              |                                  |
|--------------|----------------------------------|
| Destination: | <input type="button" value="▼"/> |
| Storage1     |                                  |
| Storage2     |                                  |
| Storage3     |                                  |
| Storage4     |                                  |

"Before you configure object replication, create the source and destination storage accounts if they do not already exist. The source and destination accounts can be either general-purpose v2 storage accounts or premium block blob accounts (preview). "

## Question-2

You need to identify which storage account to use for the flow logging of IP traffic from VM5. The solution must meet the retention requirements. Which storage account should you identify?

- A. storage1
- B. storage2 Most Voted
- C. storage3
- D. storage4

[Hide Solution](#)

 Discussion 8

For at least two reasons, storage2 is the only candidate:

- Location: The storage account used must be in the same region as the NSG.
- Retention is available only if you use General Purpose v2 Storage accounts (GPv2).

## Topic 12 - Testlet 5

<https://www.examtopics.com/exams/microsoft/az-104/view/43/>

### Question-1

You discover that VM3 does NOT meet the technical requirements.  
You need to verify whether the issue relates to the NSGs.  
What should you use?

- A. Diagram in VNet1
- B. Diagnostic settings in Azure Monitor
- C. Diagnose and solve problems in Traffic Manager profiles
- D. The security recommendations in Azure Advisor
- E. IP flow verify in Azure Network Watcher

[Hide Solution](#)

[Discussion 10](#)

**Correct Answer:** E 🎉

Scenario: Contoso must meet technical requirements including:

Ensure that VM3 can establish outbound connections over TCP port 8080 to the applications servers in the Montreal office.

IP flow verify checks if a packet is allowed or denied to or from a virtual machine. The information consists of direction, protocol, local IP, remote IP, local port, and remote port. If the packet is denied by a security group, the name of the rule that denied the packet is returned. While any source or destination IP can be chosen, IP flow verify helps administrators quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment.

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview>

*Community vote distribution*

E (100%)

## Topic 13 - Testlet 6

<https://www.examtopics.com/exams/microsoft/az-104/view/43/>

### Question-1

You need to meet the connection requirements for the New York office.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

#### Answer Area

From the Azure portal:

- Create an ExpressRoute circuit only.
- Create a virtual network gateway only.
- Create a virtual network gateway and a local network gateway.**
- Create an ExpressRoute circuit and an on-premises data gateway.
- Create a virtual network gateway and an on-premises data gateway.

Correct Answer:

In the New York office:

- Deploy ExpressRoute.
- Deploy a DirectAccess server.
- Implement a Web Application Proxy.
- Configure a site-to-site VPN connection.**

## Topic 14 - Testlet 7

<https://www.examtopics.com/exams/microsoft/az-104/view/43/>

### Question-1

HOTSPOT -

You need to recommend a solution for App1. The solution must meet the technical requirements. What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

Number of virtual networks:

|   |
|---|
| 1 |
| 2 |
| 3 |

Number of subnets per virtual network:

|   |
|---|
| 1 |
| 2 |
| 3 |

As per requirements:

- You have a public-facing application named App1. App1 is comprised of the following three tiers: A SQL database, A web front end and A processing middle tier. Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.
- Move all the virtual machines for App1 to Azure.
- Minimize the number of open ports between the App1 tiers.

Box 1: 1

Box 2: 3

## Question-2

You are planning the move of App1 to Azure.  
You create a network security group (NSG).  
You need to recommend a solution to provide users with access to App1.  
What should you recommend?

- A. Create an incoming security rule for port 443 from the Internet. Associate the NSG to the subnet that contains the web servers. **Most Voted**
- B. Create an outgoing security rule for port 443 from the Internet. Associate the NSG to the subnet that contains the web servers.
- C. Create an incoming security rule for port 443 from the Internet. Associate the NSG to all the subnets.
- D. Create an outgoing security rule for port 443 from the Internet. Associate the NSG to all the subnets.

[Hide Solution](#)

[Discussion](#) 41

**Correct Answer:** A 

Incoming and the web server subnet only, as users access the web front end by using HTTPS only.

Note Scenario: You have a public-facing application named App1. App1 is comprised of the following three tiers:

- A SQL database
- A web front end
- A processing middle tier

Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.

*Community vote distribution*

A (100%)

## Topic 15 - Testlet 8

<https://www.examtopics.com/exams/microsoft/az-104/view/43/>

### Question-1

You implement the planned changes for NSG1 and NSG2.

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

#### Answer Area:

| Statements   | Yes                              | No                               |
|--|----------------------------------|----------------------------------|
| From VM1, you can establish a Remote Desktop session to VM2. | <input checked="" type="radio"/> | <input type="radio"/>            |
| From VM2, you can ping VM3.                                  | <input checked="" type="radio"/> | <input type="radio"/>            |
| From VM2, you can establish a Remote Desktop session to VM3. | <input type="radio"/>            | <input checked="" type="radio"/> |

VM1 has inbound rules, so no restriction on outbound.

VM2 has outbound rules, so no restrictions on inbound.

Hence VM1 can establish RDP to VM2.

VM2 —ping—> VM3: Yes (no restriction other than outbound RDP)

VM2 —RDP—> VM3: No(outbound RDP is not allowed on VM2)

## Question-2

You need to ensure that you can add VM1 and VM2 to the backend pool of LB1. What should you do first?

- A. Redeploy VM1 and VM2 to the same availability zone.
- B. Connect VM2 to VNET1/Subnet1.
- C. Create a new NSG and associate the NSG to VNET1/Subnet1.
- D. Redeploy VM1 and VM2 to the same availability set. **Most Voted**

[Hide Solution](#)

[Discussion](#) 10

**Correct Answer:** B 🎉

Need to connect VM2 to VNET1/Subnet1.

Scenario: Create an internal Basic Azure Load Balancer named LB1 and connect the load balancer to VNET1/Subnet1.

| Name | IP address | Location | Connected to  |
|------|------------|----------|---------------|
| VM1  | 10.0.1.4   | West US  | VNET1/Subnet1 |
| VM2  | 10.0.2.4   | West US  | VNET1/Subnet2 |

*Community vote distribution*



For a LB basic it is required that the virtual machines are in a single availability set or scale set of virtual machines

You're redeploying the entire VM, so just assign it a NIC in the right subnet (i.e. Subnet 1).

<https://learn.microsoft.com/en-us/azure/virtual-machines/windows/change-availability-set>

## Question-4

You need to ensure that VM1 can communicate with VM4. The solution must minimize administrative effort.

What should you do?

- A. Create a user-defined route from VNET1 to VNET3.
- B. Create an NSG and associate the NSG to VM1 and VM4.
- C. Assign VM4 an IP address of 10.0.1.5/24.
- D. Establish peering between VNET1 and VNET3.

[Hide Solution](#)

[Discussion 2](#)

**Correct Answer:** D 

*Community vote distribution*

D (100%)

<https://www.examtopics.com/exams/microsoft/az-104/view/44/> [10Q per page]

<https://www.examtopics.com/exams/microsoft/az-104/view/-Custom> view—printer friendly

### Question-1

HOTSPOT -

You need to implement Role1.

Which command should you run before you create Role1? To answer, select the appropriate options in the answer area.

### Answer Area

| -Name "Reader"   ▼       |
|--------------------------|
| Find-RoleCapability      |
| Get-AzureADDirectoryRole |
| Get-AzRoleDefinition     |
| Get-AzResourceProvider   |

-Name "Reader" |

| -Name "Reader"   ▼ |
|--------------------|
| ConvertFrom-Json   |
| ConvertFrom-String |
| ConvertTo-Json     |
| ConvertTo-Xml      |

### Question-2

You need to recommend a solution to automate the configuration for the finance department users. The solution must meet the technical requirements. What should you include in the recommendation?

- A. Azure AD B2C
- B. dynamic groups and conditional access policies** Most Voted
- C. Azure AD Identity Protection
- D. an Azure logic app and the Microsoft Identity Management (MIM) client

[Hide Solution](#)

 Discussion 72

**Correct Answer:** B 

Scenario: Ensure Azure Multi-Factor Authentication (MFA) for the users in the finance department only.

The recommendation is to use conditional access policies that can then be targeted to groups of users, specific applications, or other conditions.

Reference:

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

*Community vote distribution*

B (100%)