➢ **Vendor: Microsoft**

➢ **Exam Code: AZ-303**

➢ **Exam Name: Microsoft Azure Architect Technologies**

➢ **New Updated Questions from Braindump2go (Updated in Oct./2020)**

Visit Braindump2go and Download Full Version AZ-303 Exam Dumps

QUESTION 151
A company hosts virtual machines (VMs) in an on-premises datacenter and in Azure. The on- premises and Azure-based VMs communicate using ExpressRoute. The company wants to be able to continue regular operations if the ExpressRoute connection fails. Failover connections must use the Internet and must not require Multiprotocol Label Switching (MPLS) support.
You need to recommend a solution that provides continued operations.
What should you recommend?

A. Set up a second ExpressRoute connection.
B. Increase the bandwidth of the existing ExpressRoute connection.
C. Increase the bandwidth for the on-premises internet connection.
D. Set up a VPN connection.

Answer: D
Explanation:
https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/expressroutevpn-failover

QUESTION 152
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. Create a new virtual machine scale set in the Azure portal.
B. Create an automation account.
C. Upload a configuration script.
D. Modify the extensionProfile section of the Azure Resource Manager template.
E. Create an Azure policy.

Answer: AD
Explanation:
https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/tutorial-install-apps-template

QUESTION 153
You have an Azure subscription that contains a resource group named RG1.
RG1 contains multiple resources.
You need to trigger an alert when the resources in RG1 consume $1,000 USD.
What should you do?

A. From Cost Management + Billing, add a cloud connector.
B. From the subscription, create an event subscription.
C. From Cost Management + Billing create a budget.
D. From RG1, create an event subscription.

Answer: C
Explanation:
Create budgets to manage costs and create alerts that automatically notify you are your stakeholders of spending anomalies and overspending.
To set it up, go to the Azure Portal, select 'Cost Management + Billing' -> 'Cost Management' -> 'Go to Cost Management'.
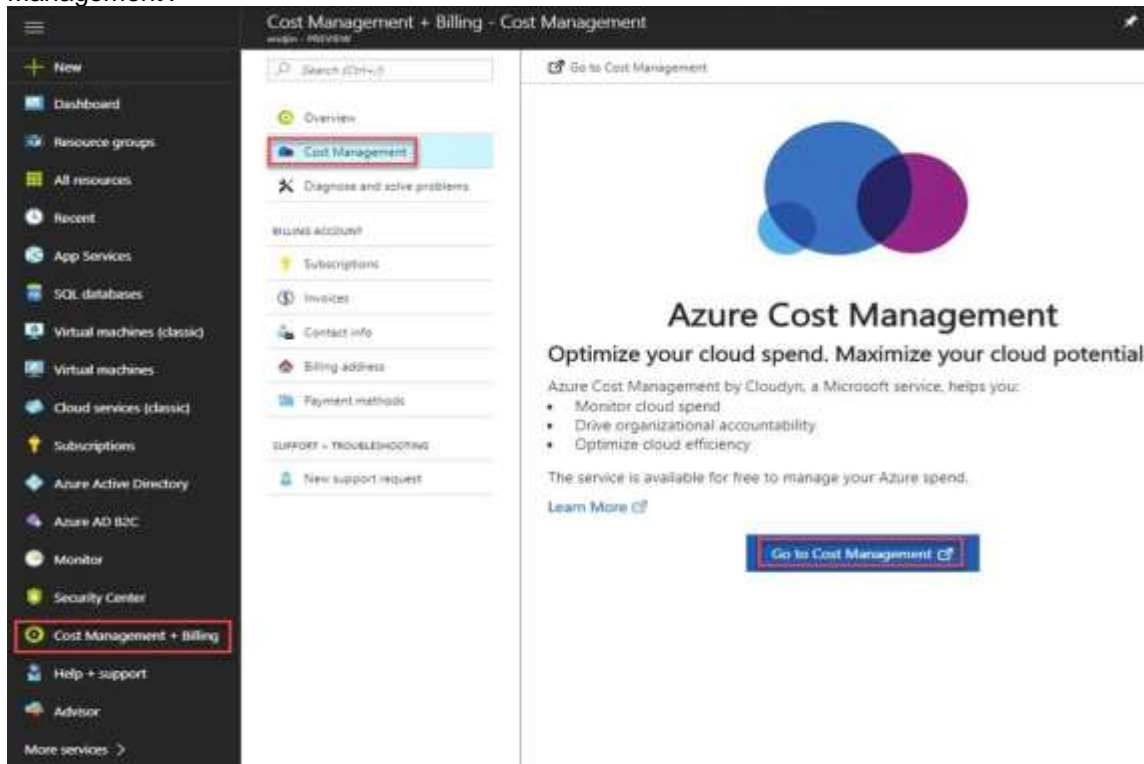
Note: Cost alerts are automatically generated based when Azure resources are consumed. Alerts show all active cost management and billing alerts together in one place. When your consumption reaches a given threshold, alerts are generated by Cost Management. There are three types of cost alerts: budget alerts, credit alerts, and department spending quota alerts.
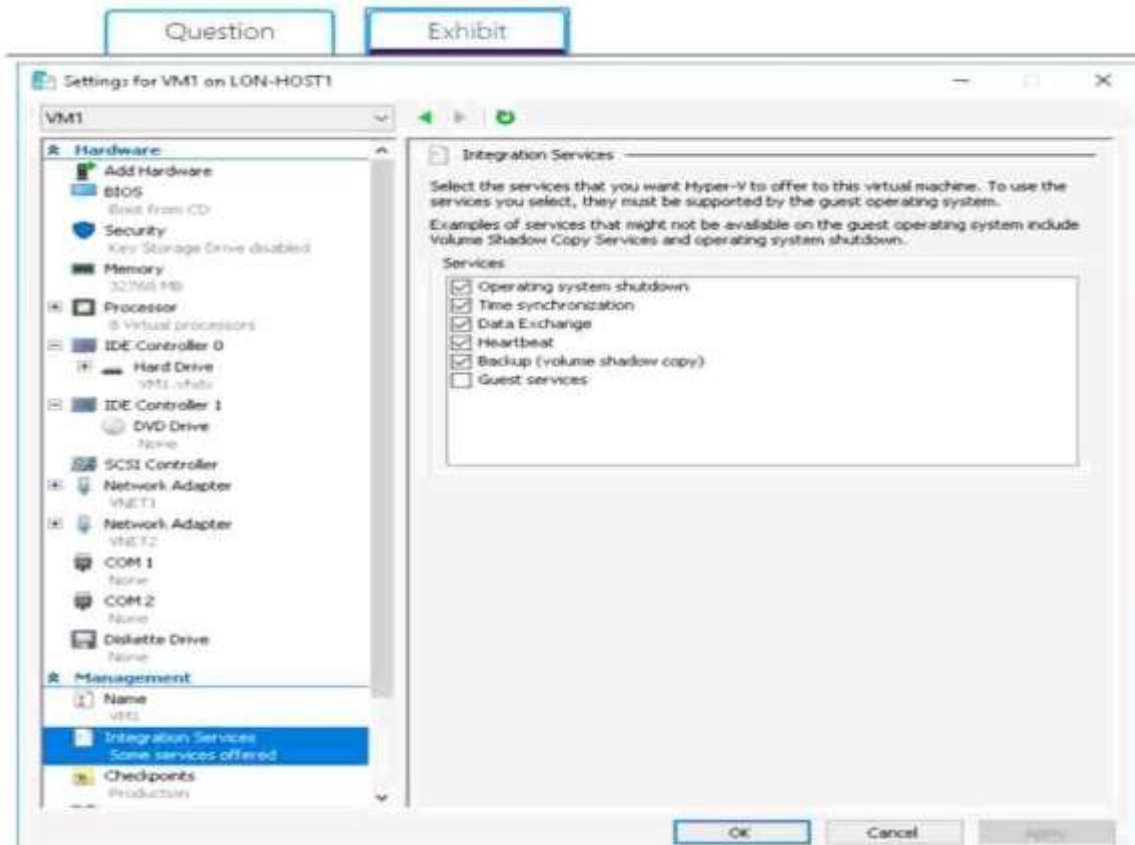Reference:
https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/getting-started

QUESTION 154
You have an Azure subscription.
You have an on-premises virtual machine named VM1.
The settings for VM1 are shown in the exhibit.

You need to ensure that you can use the disks attached to VM1 as a template for Azure virtual machines.
What should you modify on VM1?

A. the hard drive
B. Integration Services
C. the memory
D. the network adapters
E. the processor

Answer: A
Explanation:
From the exhibit we see that the disk is in the VHDX format. Before you upload a Windows virtual machines (VM) from on-premises to Microsoft Azure, you must prepare the virtual hard disk (VHD or VHDX). Azure supports only generation 1 VMs that are in the VHD file format and have a fixed sized disk. The maximum size allowed for the VHD is 1,023 GB. You can convert a generation 1 VM from the VHDX file system to VHD and from a dynamically expanding disk to fixed-sized.
References:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/prepare-for-upload-vhd-image?toc=azurevirtual-machines windows toc.json

QUESTION 155
You have an Azure subscription that contains the storage accounts shown in the following table.

Name	Contains
Storagecontoso1	A blob service and a table service
Storagecontoso2	A blob service and a file service
Storagecontoso3	A queue service
Storagecontoso4	A file service and a queue service
Storagecontoso5	A table service

You enable Azure Advanced Threat Protection (ATP) for all the storage accounts.
You need to identify which storage accounts will generate Azure ATP alerts.
Which two storage accounts should you identify? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. storagecontoso1
B. storagecontoso2
C. storagecontoso3
D. storagecontoso4
E. storaaecontoso5

Answer: AB
Explanation:
Advanced threat protection for Azure Storage is currently available only for Blob Storage.
https://docs.microsoft.com/en-us/azure/storage/common/storage-advanced-threat-protection?tabs=azure-portal

QUESTION 156
Note: This question is part of 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 that contains a group named Group1.
You need to enable multi-factor authentication (MFA) for the users in Group1 only.
Solution: From the Azure portal, you configure an authentication method policy.
Does this meet the goal?

A. Yes
B. No

Answer: B
Explanation:
We should use a Conditional Access policy.
Note: There are two ways to secure user sign-in events by requiring multi-factor authentication in Azure AD. The first, and preferred, option is to set up a Conditional Access policy that requires multi- factor authentication under certain conditions. The second option is to enable each user for Azure Multi-Factor Authentication. When users are enabled individually, they perform multi-factor authentication each time they sign in (with some exceptions, such as when they sign in from trusted IP addresses or when the remembered devices feature is turned on). Enabling Azure Multi-Factor Authentication using Conditional Access policies is the recommended approach. Changing user states is no longer recommended unless your licenses don't include Conditional Access as it requires users to perform MFA every time they sign in.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates

QUESTION 157
Note: This question is part of 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 that contains a group named Group1.

You need to enable multi-factor authentication (MFA) for the users in Group1 only.

Solution: From Multi-Factor Authentication, you select Bulk update, and you provide a CSV file that contains the members of Group1.

Does this meet the goal?

A. Yes
B. No

Answer: B
Explanation:
We should use a Conditional Access policy.

Note: There are two ways to secure user sign-in events by requiring multi-factor authentication in Azure AD. The first, and preferred, option is to set up a Conditional Access policy that requires multi- factor authentication under certain conditions. The second option is to enable each user for Azure Multi-Factor Authentication. When users are enabled individually, they perform multi-factor authentication each time they sign in (with some exceptions, such as when they sign in from trusted IP addresses or when the remembered devices feature is turned on). Enabling Azure Multi-Factor Authentication using Conditional Access policies is the recommended approach. Changing user states is no longer recommended unless your licenses don't include Conditional Access as it requires users to perform MFA every time they sign in.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates

QUESTION 158
Hotspot Question
You have the Azure SQL Database servers shown in the following table.

Name	Elastic pool
sqlserver1	Pool1
sqlserver2	Pool1, Pool2

You have the Azure SQL databases shown in the following table.

Name	Azure SQL Database server	Elastic pool
DB1	sqlserver1	None
DB2	sqlserver1	Pool1
DB3	sqlserver2	Pool1
DB4	sqlserver2	Pool2

You create a failover group named failover1 that has the following settings:
- Primary server: sqlserver1
- Secondary server: sqlserver2
- Read/Write failover policy: Automatic
- Read/Write grace period (hours): 1 hour

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

| Statements	Yes	No
You can add DB1 to failover1.	○	○
You can add DB3 to failover1.	○	○
Sqlserver1 and sqlserver2 are in the same Azure region.	○	○

Answer:

Statements	Yes	No
You can add DB1 to failover1.	⦿	○
You can add DB3 to failover1.	○	⦿
Sqlserver1 and sqlserver2 are in the same Azure region.	⦿	○

QUESTION 159
Hotspot Question
You have a hierarchy of management groups and Azure subscriptions as shown in the following table.
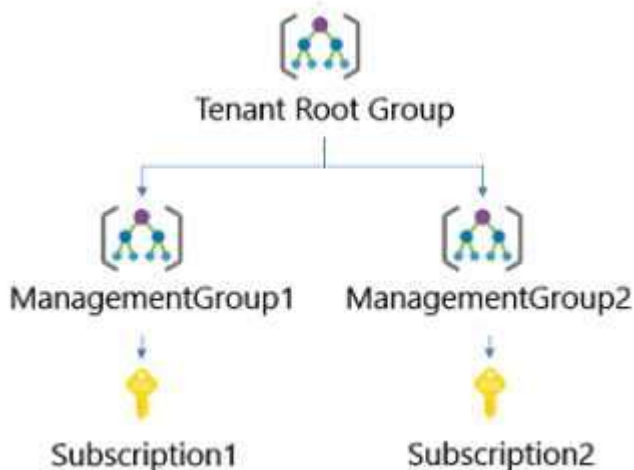
You create the Azure resources shown in the following table.

Name	Type	Created in
RG1	Resource group	Subscription1
RG2	Resource group	Subscription2
VM2	Virtual machine	RG2

You assign roles to users as shown in the following table.

User name	Role	On resource
User1	Contributor	ManagementGroup1
User2	Contributor	ManagementGroup2
User3	Reader	Tenant Root Group

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

Statements	Yes	No
You can remove User1 from the Contributor role for RG1.	○	○
User2 can delete VM2.	○	○
You can add User3 as a Contributor for RG1.	○	○

Answer:

Statements	Yes	No
You can remove User1 from the Contributor role for RG1.	●	○
User2 can delete VM2.	●	○
You can add User3 as a Contributor for RG1.	●	○

QUESTION 160
Hotspot Question
You have an Azure subscription that contains a resource group named RG1.
You have a group named Group1 that is assigned the Contributor role for RG1.
You need to enhance security for the virtual machines in RG1 to meet the following requirements:
– Prevent Group1 from assigning external IP addresses to the virtual machines.
– Ensure that Group1 can establish an RDP connection to the virtual machines through a shared external IP address.
What should you use to meet each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Prevent Group1 from assigning external IP addresses to the virtual machines:

Azure Policy
Azure Bastion
Virtual network service endpoints
Azure Firewall
Azure Web Application Firewall (WAF)

Ensure that Group1 can establish an RDP connection to the virtual machines through a shared external IP address:

Azure Policy
Azure Bastion
Virtual network service endpoints
Azure Firewall
Azure Web Application Firewall (WAF)

Answer:

Prevent Group1 from assigning external IP addresses to the virtual machines:

Azure Policy
Azure Bastion
Virtual network service endpoints
Azure Firewall
Azure Web Application Firewall (WAF)

Ensure that Group1 can establish an RDP connection to the virtual machines through a shared external IP address:

Azure Policy
Azure Bastion
Virtual network service endpoints
Azure Firewall
Azure Web Application Firewall (WAF)

QUESTION 161
Hotspot Question
Your network contains an on-premises Active Directory domain named contoso.com that contains a user named User1. The domain syncs to Azure Active Directory (Azure AD). You have the Windows 10 devices shown in the following table.

Name	Joined to
Device1	On-premises Active Directory
Device2	Azure AD
Device3	Workgroup

The User Sign-In settings are configured as shown in the following exhibit.

PROVISION FROM ACTIVE DIRECTORY

Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

Manage provisioning (Preview)

Azure AD Connect sync

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled

USER SIGN-IN

Federation	Disabled	0 domains
Seamless single sign-on	Enabled	1 domain
Pass-through authentication	Disabled	0 agents

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

Statements	Yes	No
When accessing the Azure portal from Device1, User1 will sign in automatically by using SSO.	○	○
When accessing the Azure portal from Device2, User1 will sign in automatically by using SSO.	○	○
When accessing the Azure portal from Device3, User1 will sign in automatically by using SSO.	○	○

Answer:

Statements	Yes	No
When accessing the Azure portal from Device1, User1 will sign in automatically by using SSO.	◉	○
When accessing the Azure portal from Device2, User1 will sign in automatically by using SSO.	○	◉
When accessing the Azure portal from Device3, User1 will sign in automatically by using SSO.	○	◉

QUESTION 162
Hotspot Question
You create a virtual machine scale set named Scale1. Scale1 is configured as shown in the following exhibit.
The subscription contains the Azure SQL databases shown in the following table.

INSTANCES

* Instance count ❶	4
* Instance size (View full pricing details) ❶	DS1_v2 (1 vCPU, 3.5 GB)
Deploy as low priority ❶	No / Yes
Use managed disks ❶	No / Yes

~ Show advanced settings

AUTOSCALE

Autoscale ❶	Disabled / Enabled
* Minimum number of VMs ❶	2
* Maximum number of VMs ❶	20

Scale out

* CPU threshold (%) ❶	80
* Number of VMs to increase by ❶	2

Scale in

* CPU threshold (%) ❶	30
* Number of VMs to decrease by ❶	4

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.

If Scale1 is utilized at 85 percent for six minutes, Scale1 will be running [answer choice].

2 virtual machines
4 virtual machines
6 virtual machines
8 virtual machines
10 virtual machines

If Scale1 is first utilized at 25 percent for six minutes, and then utilized at 50 percent for six minutes, Scale1 will be running [answer choice].

2 virtual machines
4 virtual machines
6 virtual machines
8 virtual machines
10 virtual machines

Answer:

If Scale1 is utilized at 85 percent for six minutes, Scale1 will be running [answer choice].

2 virtual machines
4 virtual machines
6 virtual machines
8 virtual machines
10 virtual machines

If Scale1 is first utilized at 25 percent for six minutes, and then utilized at 50 percent for six minutes, Scale1 will be running [answer choice].

2 virtual machines
4 virtual machines
6 virtual machines
8 virtual machines
10 virtual machines

Explanation:
Box 1:
The Autoscale scale out rule increases the number of VMs by 2 if the CPU threshold is 80% or higher. The initial instance count is 4 and rises to 6 when the 2 extra instances of VMs are added.
Box 2:
The Autoscale scale in rule decreases the number of VMs by 4 if the CPU threshold is 30% or lower. The initial instance count is 4 and thus cannot be reduced to 0 as the minimum instances is set to 2. Instances are only added when the CPU threshold reaches 80%.
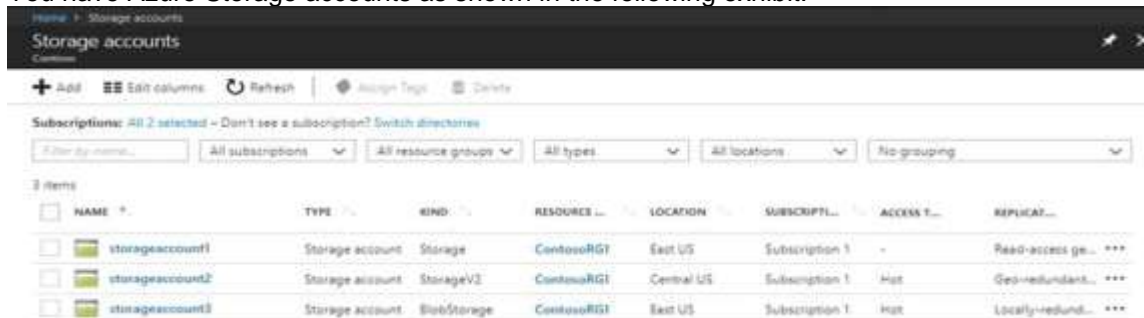References:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/autoscale-overview
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/autoscale-best-practices
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/autoscale-common-scale-patterns

QUESTION 163
Hotspot Question
You have Azure Storage accounts as shown in the following exhibit.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.

You can use [answer choice] for Azure Table Storage.

storageaccount1 only
storageaccount2 only
storageaccount3 only
storageaccount1 and storageaccount2 only
storageaccount2 and storageaccount3 only

You can use [answer choice] for Azure Blob storage.

storageaccount3 only
storageaccount2 and storageaccount3 only
storageaccount1 and storageaccount3 only
all the storage accounts

Answer:

You can use [answer choice] for Azure Table Storage.

storageaccount1 only
storageaccount2 only
storageaccount3 only
storageaccount1 and storageaccount2 only
storageaccount2 and storageaccount3 only

You can use [answer choice] for Azure Blob storage.

storageaccount3 only
storageaccount2 and storageaccount3 only
storageaccount1 and storageaccount3 only
all the storage accounts

Explanation:
Note: The three different storage account options are: General-purpose v2 (GPv2) accounts, General-purpose v1 (GPv1) accounts, and Blob storage accounts.
General-purpose v2 (GPv2) accounts are storage accounts that support all of the latest features for blobs, files, queues, and tables.
- Blob storage accounts support all the same block blob features as GPv2, but are limited to supporting only block blobs.
- General-purpose v1 (GPv1) accounts provide access to all Azure Storage services, but may not have the latest features or the lowest per gigabyte pricing.
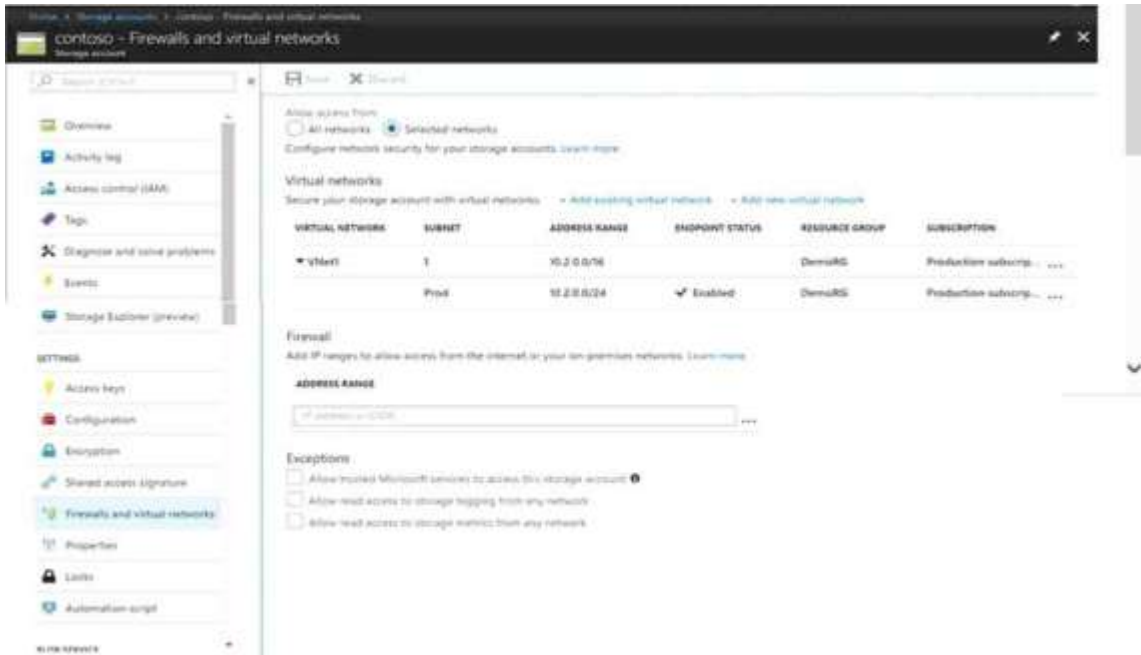References:
https://docs.microsoft.com/en-us/azure/storage/common/storage-account-options

QUESTION 164
Hotspot Question
You have several Azure virtual machines on a virtual network named VNet1. You configure an Azure Storage account as shown in the following exhibit.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:
Box 1: Never
Box 2: Never
After you configure firewall and virtual network settings for your storage account, select Allow trusted Microsoft services to access this storage account as an exception to enable Azure Backup service to access the network restricted storage account.

Reference:
https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows
https://azure.microsoft.com/en-us/blog/azure-backup-now-supports-storage-accounts-secured-with-azure-storage-firewalls-and-virtual-networks/
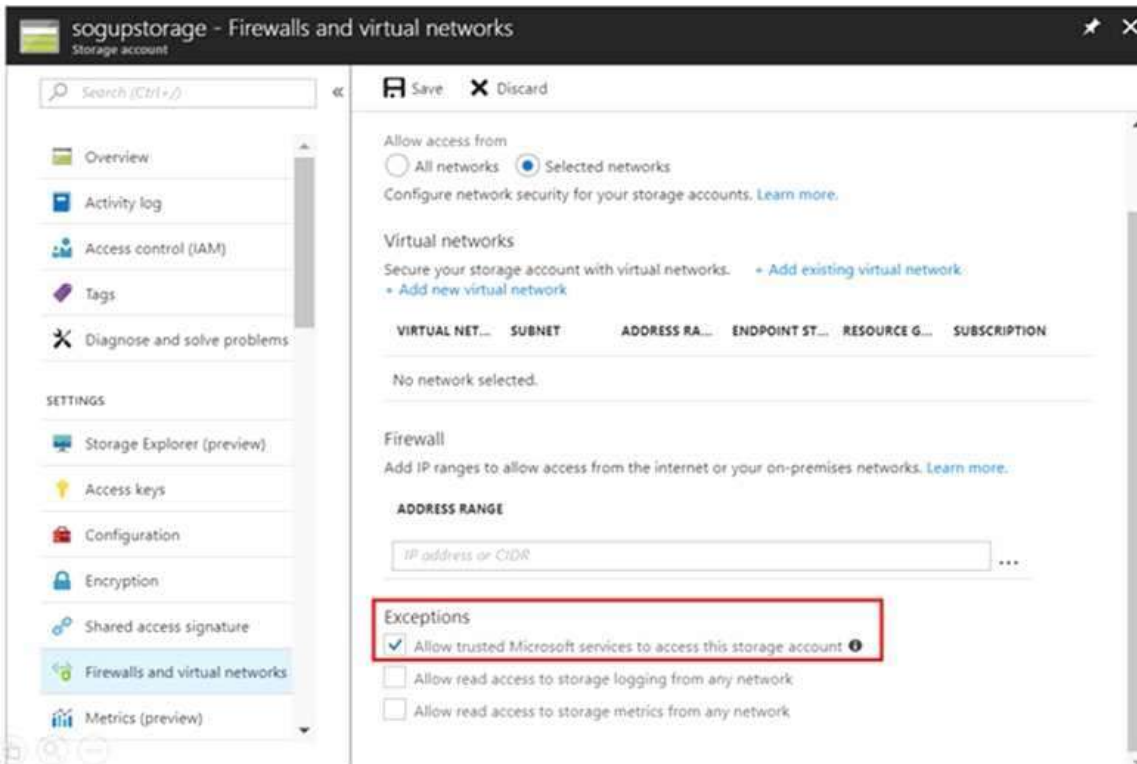
QUESTION 165
Hotspot Question
You have an Azure subscription that includes an Azure key vault named Vault1.
You create the Azure virtual machines shown in the following table.

Name	Operating system disk type	Use managed disks
VM1	Premium SSD	Yes
VM2	Standard HDD	Yes
VM3	Standard SSD	No

You enable Azure Disk Encryption for all the virtual machines and use the -VolumeType All parameter.
You add data disks to the virtual machines as shown in the following table.

Name	Virtual machine	Storage account type
VM1-Disk1	VM1	Premium SSD
VM2-Disk1	VM2	Standard SSD
VM3-Disk1	VM3	Standard HDD

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

Statements	Yes	No
VM1-Disk1 is encrypted automatically by using Azure Disk Encryption.	○	○
VM2-Disk1 is encrypted automatically by using Azure Disk Encryption.	○	○
VM3-Disk1 is encrypted automatically by using Azure Disk Encryption.	○	○

Answer:

Statements	Yes	No
VM1-Disk1 is encrypted automatically by using Azure Disk Encryption.	●	○
VM2-Disk1 is encrypted automatically by using Azure Disk Encryption.	●	○
VM3-Disk1 is encrypted automatically by using Azure Disk Encryption.	○	●

Explanation:
Premium and standard, but not basic, account types support disk encryption.
Disk encryption requires managed disks.
References:
https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-overview

QUESTION 166
Hotspot Question
You have an Azure subscription named Subscription1. Subscription1 contains the resources in the following table:

Name	Type
RG1	Resource group
RG2	Resource group
VNet1	Virtual network
VNet2	Virtual network

VNet1 is in RG1. VNet2 is in RG2. There is no connectivity between VNet1 and VNet2. An administrator named Admin1 creates an Azure virtual machine VM1 in RG1. VM1 uses a disk named Disk1 and connects to VNet1. Admin1 then installs a custom application in VM1.
You need to move the custom application to VNet2. The solution must minimize administrative effort.
Which two actions should you perform? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

First action:

	∨
Create a network interface in RG2.	
Detach a network interface.	
Delete VM1.	
Move a network interface to RG2.	

Second action:

	∨
Attach a network interface.	
Create a network interface in RG2.	
Create a new virtual machine.	
Move VM1 to RG2.	

Answer:

First action:

	∨
Create a network interface in RG2.	
Detach a network interface.	
Delete VM1.	
Move a network interface to RG2.	

Second action:

	∨
Attach a network interface.	
Create a network interface in RG2.	
Create a new virtual machine.	
Move VM1 to RG2.	

Explanation:
We cannot just move a virtual machine between networks. What we need to do is identify the disk used by the VM, delete the VM itself while retaining the disk, and recreate the VM in the target virtual network and then attach the original disk to it.
Reference:
https://blogs.technet.microsoft.com/canitpro/2014/06/16/step-by-step-move-a-vm-to-a-different-vnet-on-azure/
https://4sysops.com/archives/move-an-azure-vm-to-another-virtual-network-vnet/#migrate-an-azure-vm-between-vnets

QUESTION 167
Hotspot Question
You have a web server app named App1 that is hosted in three Azure regions.

You plan to use Azure Traffic Manager to distribute traffic optimally for App1.
You need to enable Real User Measurements to monitor the network latency data for App1.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

From the Traffic Manager profile: ▼

| Select Generate key. |
| Enable Traffic view. |
| Configure the Diagnostics settings. |
| Add a custom header. |

From App1: ▼

| Embed the Traffic Manager JavaScript code snippet. |
| Embed the Azure Application Insights JavaScript code snippet. |
| Configure the Diagnostics settings. |
| Configure the Application settings. |

Answer:

From the Traffic Manager profile: ▼

| **Select Generate key.** |
| Enable Traffic view. |
| Configure the Diagnostics settings. |
| Add a custom header. |

From App1: ▼

| **Embed the Traffic Manager JavaScript code snippet.** |
| Embed the Azure Application Insights JavaScript code snippet. |
| Configure the Diagnostics settings. |
| Configure the Application settings. |

Explanation:
Box 1: Select Generate key
You can configure your web pages to send Real User Measurements to Traffic Manager by obtaining a Real User Measurements (RUM) key and embedding the generated code to web page.
Obtain a Real User Measurements key
The measurements you take and send to Traffic Manager from your client application are identified by the service using a unique string, called the Real User Measurements (RUM) Key. You can get a RUM key using the Azure portal, a REST API, or by using the PowerShell or Azure CLI.
To obtain the RUM Key using Azure portal:
- From a browser, sign in to the Azure portal. If you don't already have an account, you can sign up for a free one-month trial.
- In the portal's search bar, search for the Traffic Manager profile name that you want to modify, and then click the Traffic Manager profile in the results that the displayed. ?In the Traffic Manager profile blade, click Real User Measurements under Settings.
- Click Generate Key to create a new RUM Key.
Box 2: Embed the Traffic Manager JavaScript code snippet.
Embed the code to an HTML web page
After you have obtained the RUM key, the next step is to embed this copied JavaScript into an HTML page that your end users visit.
This example shows how to update an HTML page to add this script. You can use this guidance to adapt it to your HTML source management workflow.
- Open the HTML page in a text editor
- Paste the JavaScript code you had copied in the earlier step to the BODY section of the HTML (the copied code is on line 8 & 9, see figure 3).

```
1  <HTML>
2  <HEAD>
3  <TITLE>Webpage powered by Azure</TITLE>
4  </HEAD>
5  <BODY BGCOLOR="FFFFFF">
6  <H1>Welcome</H1>
7  <P> <B>Hello!</B>
8  <script src="//www.atmrum.net/rum.js"></script>
9  <script>rum.start("0123456789abcdef0123456789abcdff");</script>
10 </BODY>
11 </HTML>
```

Reference:
https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-create-rum-web-pages