AZ-104$^{\text{Q\&As}}$

Microsoft Azure Administrator

Pass Microsoft AZ-104 Exam with 100% Guarantee

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

https://www.pass2lead.com/az-104.html

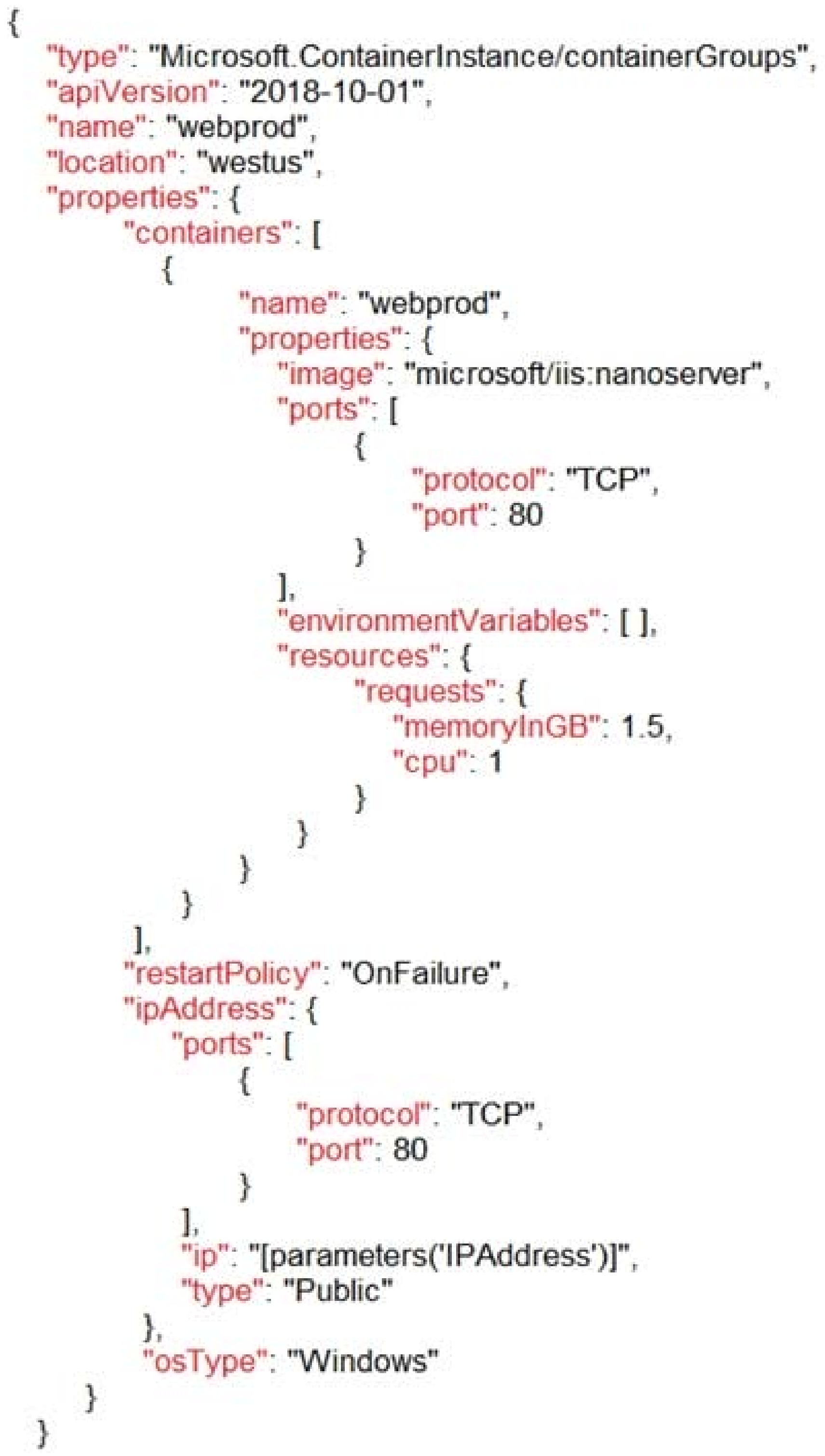
100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

HOTSPOT

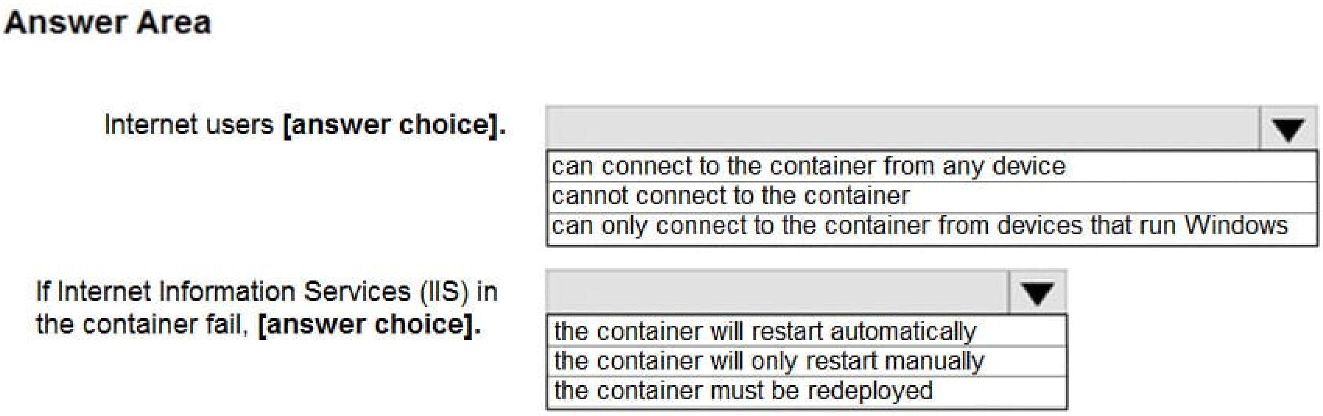
You plan to deploy an Azure container instance by using the following Azure Resource Manager template.



```
{
   "type": "Microsoft.ContainerInstance/containerGroups",
   "apiVersion": "2018-10-01",
   "name": "webprod",
   "location": "westus",
   "properties": {
         "containers": [
            {
                  "name": "webprod",
                  "properties": {
                     "image": "microsoft/iis:nanoserver",
                     "ports": [
                           {
                                 "protocol": "TCP",
                                 "port": 80
                           }
                     ],
                     "environmentVariables": [ ],
                     "resources": {
                           "requests": {
                              "memoryInGB": 1.5,
                              "cpu": 1
                           }
                     }
                  }
            }
         ],
         "restartPolicy": "OnFailure",
         "ipAddress": {
            "ports": [
                  {
                        "protocol": "TCP",
                        "port": 80
                  }
            ],
            "ip": "[parameters('IPAddress')]",
            "type": "Public"
         },
         "osType": "Windows"
   }
}
```

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

Hot Area:



Answer Area

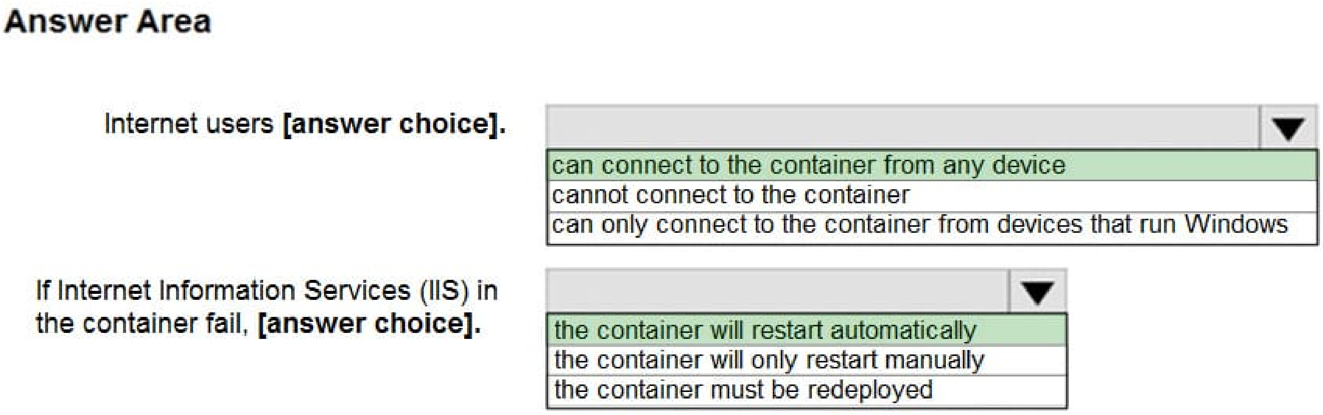
Internet users **[answer choice].**

- can connect to the container from any device
- cannot connect to the container
- can only connect to the container from devices that run Windows

If Internet Information Services (IIS) in the container fail, **[answer choice].**

- the container will restart automatically
- the container will only restart manually
- the container must be redeployed

Correct Answer:



Answer Area

Internet users **[answer choice].**

- can connect to the container from any device
- cannot connect to the container
- can only connect to the container from devices that run Windows

If Internet Information Services (IIS) in the container fail, **[answer choice].**

- the container will restart automatically
- the container will only restart manually
- the container must be redeployed

Box 1: can connect to the container from any device

In the policy "osType": "window" refer that it will create a container in a container group that runs Windows but it won\\'t block access depending on device type.

Box 2: the container will restart automatically

Docker provides restart policies to control whether your containers start automatically when they exit, or when Docker restarts. Restart policies ensure that linked containers are started in the correct order. Docker recommends that you use

restart policies, and avoid using process managers to start containers.

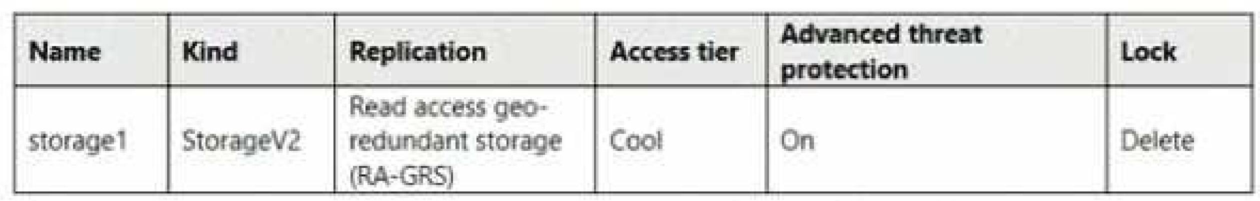
on-failure : Restart the container if it exits due to an error, which manifests as a non-zero exit code. As the flag is mentioned as "on-failure" in the policy, so it will restart automatically

Reference:

https://docs.microsoft.com/en-us/cli/azure/container?view=azure-cli-latest https://docs.docker.com/config/containers/start-containers-automatically/

QUESTION 2

You have an Azure subscription that contains the following storage account:



Name	Kind	Replication	Access tier	Advanced threat protection	Lock
storage1	StorageV2	Read access geo-redundant storage (RA-GRS)	Cool	On	Delete

You need 10 create a request to Microsoft Support to perform a live migration of storage1 to Zone Redundant Storage (ZRS) replication. How should you modify storage1 before the Live migration?

A. Set the replication to Locally-redundant storage (IRS)

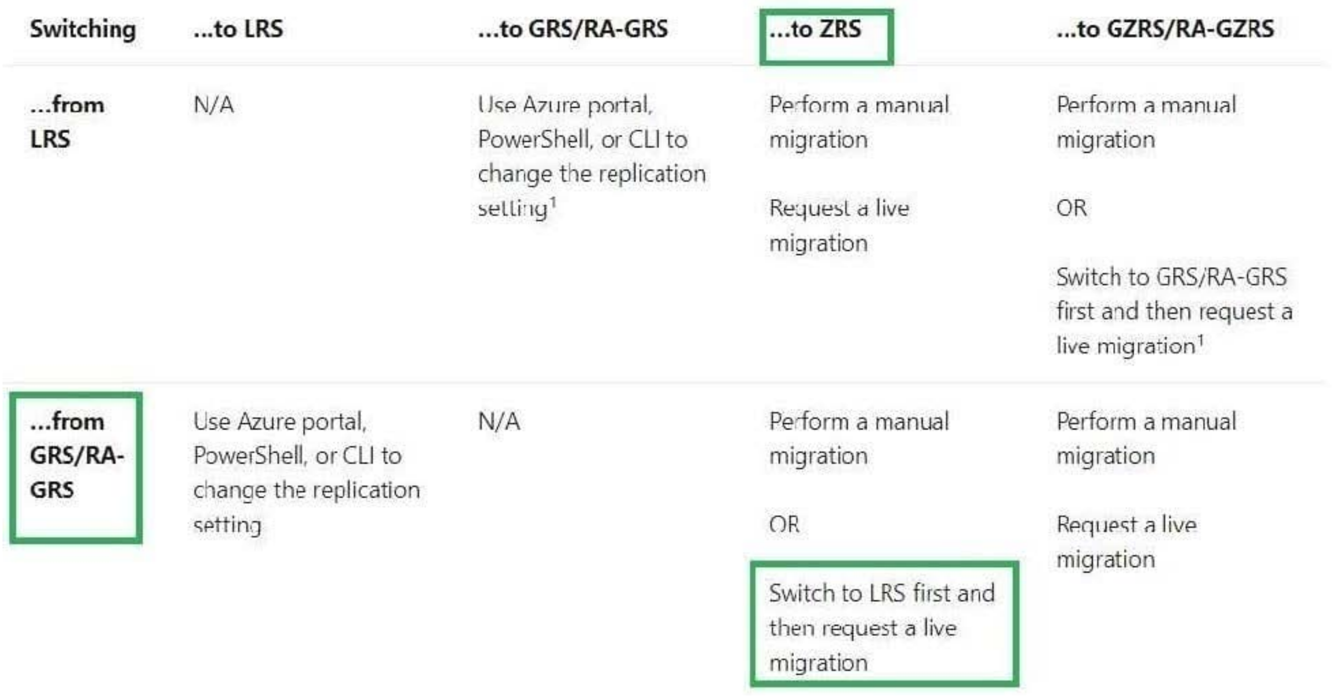
B. Disable Advanced threat protection

C. Remove the lock

D. Set the access tier to Hot

Correct Answer: A

If you want to live migration from RA-GRS to ZRS, at first you have to Switch the storage tier to LRS and then only you can request a live migration.



Switching	...to LRS	...to GRS/RA-GRS	...to ZRS	...to GZRS/RA-GZRS
...from LRS	N/A	Use Azure portal, PowerShell, or CLI to change the replication setting[1]	Perform a manual migration Request a live migration	Perform a manual migration OR Switch to GRS/RA-GRS first and then request a live migration[1]
...from GRS/RA-GRS	Use Azure portal, PowerShell, or CLI to change the replication setting	N/A	Perform a manual migration OR Switch to LRS first and then request a live migration	Perform a manual migration Request a live migration

Reference:

https://docs.microsoft.com/en-us/azure/storage/common/redundancy-migration?toc=%2Fazure%2Fstorage%2Fblobs%2Ftoc.jsonandtabs=portal

QUESTION 3

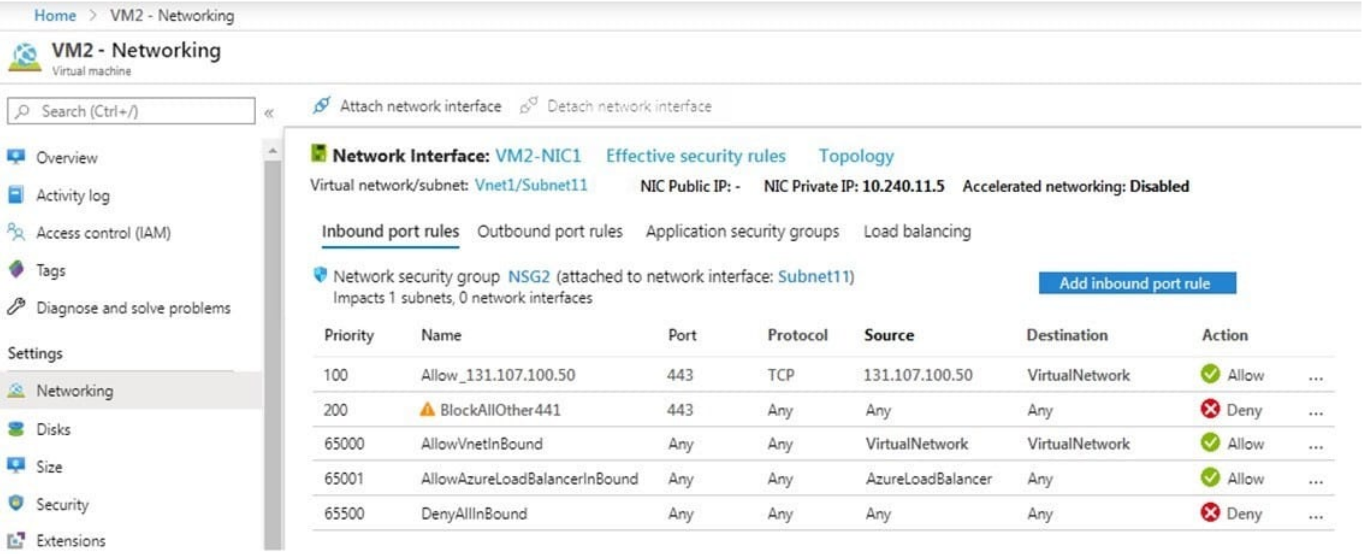
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while

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.



Network Interface: VM2-NIC1

Virtual network/subnet: Vnet1/Subnet11 NIC Public IP: - NIC Private IP: 10.240.11.5 Accelerated networking: Disabled

Network security group NSG2 (attached to network interface: Subnet11)
Impacts 1 subnets, 0 network interfaces

Priority	Name	Port	Protocol	Source	Destination	Action
100	Allow_131.107.100.50	443	TCP	131.107.100.50	VirtualNetwork	Allow
200	BlockAllOther441	443	Any	Any	Any	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

You discover that connections to App1 from 131.107.100.50 over TCP port 443 fail.

You verify that the Load Balancer rules are configured correctly.

You need to ensure that connections to App1 can be established successfully from 131.107.100.50 over TCP port 443.

Solution: You modify the priority of the Allow_131.107.100.50 inbound security rule.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

llow_131.107.100.50 rule has a higher priority (100). The issue is not related with the priority of the rule.

QUESTION 4

You have an Azure subscription that contains a virtual machine named VM1 and an Azure key vault named KV1. You need to configure encryption for VM1. The solution must meet the following requirements:

1.

Store and use the encryption key in KV1.

2.

Maintain encryption if VM1 is downloaded from Azure.

3.

Encrypt both the operating system disk and the data disks. Which encryption method should you use?

A. customer-managed keys

B. Confidential disk encryption

C. Azure Disk Encryption

D. encryption at host

Correct Answer: C

Azure Disk Encryption helps protect and safeguard your data to meet your organizational security and compliance commitments. ADE encrypts the OS and data disks of Azure virtual machines (VMs) inside your VMs by using the DM-Crypt

feature of Linux or the BitLocker feature of Windows. ADE is integrated with Azure Key Vault to help you control and manage the disk encryption keys and secrets, with the option to encrypt with a key encryption key (KEK).

Note: There are several types of encryption available for your managed disks, including Azure Disk Encryption (ADE), Server-Side Encryption (SSE) and encryption at host.

Incorrect:

*

Confidential disk encryption

Confidential disk encryption binds disk encryption keys to the virtual machine\\'s TPM and makes the protected disk content accessible only to the VM. The TPM and VM guest state is always encrypted in attested code using keys released by

a secure protocol that bypasses the hypervisor and host operating system. Currently only available for the OS disk.

*

Encryption at host

Encryption at host is a Virtual Machine option that enhances Azure Disk Storage Server-Side Encryption to ensure that all temp disks and disk caches are encrypted at rest and flow encrypted to the Storage clusters.

When you enable encryption at host, that encryption starts on the VM host itself, the Azure server that your VM is allocated to. The data for your temporary disk and OS/data disk caches are stored on that VM host. After enabling encryption at

host, all this data is encrypted at rest and flows encrypted to the Storage service, where it is persisted. Essentially, encryption at host encrypts your data from end-to-end. Encryption at host does not use your VM\\'s CPU and doesn\\'t impact

your VM\\'s performance.

Reference:

https://learn.microsoft.com/en-us/azure/virtual-machines/disk-encryption-overview

QUESTION 5

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:

1.

Reader

2.

Security Admin

3.

Security Reader

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

What should you do?

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

B. Assign User1 the Owner role for VNet1.

C. Remove User1 from the Security Reader and Reader roles for Subscription1.

D. Assign User1 the Network Contributor role for RG1.

Correct Answer: B

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

Note:

There are several versions of this question in the exam. The question can have other incorrect answer options, including the following:

1.

Name Server (NS)

2.

Assign User1 the Contributor role for VNet1.

3.

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

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