

Valentine's Day Offer | Flat 25% OFF on All Courses | Use Coupon - WHIZ25SITE

[Home](#) > [My Courses](#) > [Microsoft Azure Administrator\(AZ-103\)](#) > [Practice Test 2](#) > [Report](#)

Search Courses



## Practice Test 2

Completed on 12-February-2021



Attempt



Marks Obtained



Your score



Time Taken



Result

12

0 / 55

0.0%

00 H 00 M 06 S

Failed

## Domains wise Quiz Performance Report

Join us on [Slack community](#)

No	Domain	Total Question	Correct	Incorrect	Unattempted	Marked as Review
1	Configure and Manage Virtual Networks	19	0	0	19	0
2	Deploying and Managing Virtual Machines	10	0	1	9	0
3	Manage Identities	7	0	0	7	0
4	Implementing and Managing Storage	11	0	0	11	0
5	Managing Azure Subscriptions and Resources	8	0	0	8	0
Total	All Domain	55	0	1	54	0

Review the Answers

Sorting by

All

## Question 1

Unattempted

Domain :Configure and Manage Virtual Networks

Your company has an Azure account and subscription. The subscription contains a virtual machine named demovm877. You have a computer named Computer1 that runs Windows 10.

Computer1 is connected to the Internet. You add a network interface to the virtual machine as shown in the exhibit below.

**Network Interface: demovm877**    [Effective security rules](#)    [Topology](#)

Virtual network/subnet: demonew-vnet/default    Public IP: [demovm-ip](#)    Private IP: **10.0.0.4**    Accelerated networking: **Disabled**

**APPLICATION SECURITY GROUPS** [Edit](#)

[Configure the application security groups](#)

**INBOUND PORT RULES** [Edit](#)

Network security group [demovm-nsg](#) (attached to network interface: [demovm877](#))  
Impacts 0 subnets, 1 network interfaces

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION
300	<a href="#">⚠ RDP</a>	3389	TCP	Any	Any
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any
65500	DenyAllInBound	Any	Any	Any	Any

**OUTBOUND PORT RULES** [Edit](#)

Network security group [demovm-nsg](#) (attached to network interface: [demovm877](#))  
Impacts 0 subnets, 1 network interfaces

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork
65001	AllowInternetOutBound	Any	Any	Any	Internet
65500	DenyAllOutBound	Any	Any	Any	Any

From Computer1, you attempt to connect to demovm877 by using Remote Desktop, but the connection fails. You need to establish a Remote Desktop connection to demovm. What should you do first?

- A. Start demovm. ✓
- B. Attach a network interface.
- C. Delete the DenyAllOutBound outbound port rule.
- D. Delete the DenyAllInBound inbound port rule.

### Explanation:

Answer – A

Here the main issue is that the VM is not started and allocated an IP address. When you start the VM, you will get a public IP address which will be assigned to the Network Interface. The Network security groups are fine for allowing RDP access.

The public IP is allocated for a VM in the running state. This is also required for connectivity purposes

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION	...
300	⚠️ RDP	3389	TCP	Any	Any	Allow	...
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	...
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow	...
65500	DenyAllInBound	Any	Any	Any	Any	Deny	...

Option B is incorrect because adding a new interface will not solve the connectivity issue

Options C and D are incorrect since you cannot delete the built-in network security group rules

For more information on Network security groups, please go to the below URL

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

Ask our Experts

Rate this Question?

**View Queries**

open ▾

**Question 2**

**Unattempted**

Domain :Configure and Manage Virtual Networks

Your company has an Azure account and subscription. The subscription contains a virtual machine named demovm877. You have a computer named Computer1 that runs Windows 10. Computer1 is connected to the Internet. You add a network interface to the virtual machine as shown in the exhibit below

<b>Network Interface:</b> demovm877	<a href="#">Effective security rules</a>	<a href="#">Topology</a>
Virtual network/subnet: demonew-vnet/default	Public IP: <a href="#">demovm-ip</a>	Private IP: 10.0.0.4      Accelerated networking: Disabled

#### APPLICATION SECURITY GROUPS [\(1\)](#)

[Configure the application security groups](#)

#### INBOUND PORT RULES [\(1\)](#)

Network security group [demovm-nsg](#) (attached to network interface: [demovm877](#))  
Impacts 0 subnets, 1 network interfaces

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION
300	RDP	3389	TCP	Any	Any
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any
65500	DenyAllInBound	Any	Any	Any	Any

#### OUTBOUND PORT RULES [\(1\)](#)

Network security group [demovm-nsg](#) (attached to network interface: [demovm877](#))  
Impacts 0 subnets, 1 network interfaces

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork
65001	AllowInternetOutBound	Any	Any	Any	Internet
65500	DenyAllOutBound	Any	Any	Any	Any

From Computer1 you want to be able to also access a web service running on port 80 after demovm877 is started. Which of the following must be done for this to work?

- A. Attach a network interface.
- B. Add an incoming network security group rule for allowing traffic on port 80
- C. Add an outgoing network security group rule for allowing traffic on port 80
- D. Delete the DenyAllOutBound outbound port rule.
- E. Delete the DenyAllInBound inbound port rule.

#### Explanation:

Answer – B

Here you need to add an incoming rule to allow traffic on port 80

 Add inbound security rule X

demovm-nsg

 Basic

---

\* Source i  
Any

\* Source port ranges i  
\*

\* Destination i  
Any

\* Destination port ranges i  
80 ✓

\* Protocol  
 Any  TCP  UDP

\* Action  
 Allow  Deny

\* Priority i  
310

\* Name  
Port\_80 ✓

Description

Option A is incorrect since this needs to be done for the current attached network interface

Option C is incorrect since the incoming traffic needs to be allowed

Options D and E are incorrect since you cannot delete the built-in network security group rules

For more information on Network security groups, please go to the below URL

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

Ask our Experts

Rate this Question?  

[View Queries](#)[open ▾](#)**Question 3****Unattempted****Domain :Deploying and Managing Virtual Machines**

Your company has an Azure account and subscription. The subscription contains the resources in the following table:

Name	Type
whizlabstore	Storage container
whizlabs-rg	Resource Group
documents	BLOB container
demo	File share

Your IT administrator has deployed a virtual machine called demovm and a storage account called whizlabs-temp by using a single Azure Resource Manager template. You want to do a review of the template that was used for the deployment. Which of the following resource blade could be used to view the template that was used for the deployment?

- A. **whizlabs-rg** 
- B. **demovm**
- C. **whizlabs-temp**
- D. **whizlabstore**

**Explanation:**

Answer – A

If you go to the Resource Group, you can see the deployments made to that resource group. An example is shown below

**whizlabs-rg - Deployments**

**You can view all the deployments**

DEPLOYMENT NAME	STATUS	LAST MODIFIED	DURATION	RELATED EVENTS
NetworkInterface.secondary-2	Succeeded	1/13/2019, 5:11:42 PM	20 seconds	Related events
Microsoft.PublicIPAddress-201	Succeeded	1/13/2019, 4:54:47 PM	22 seconds	Related events
CreateVm-Canonical.UbuntuSe	Succeeded	1/13/2019, 4:40:01 PM	2 minutes 30 seconds	Related events
CreateVm-Canonical.UbuntuSe	Succeeded	1/13/2019, 4:31:53 PM	1 minute 51 seconds	Related events
CreateVm-MicrosoftWindowsS	Succeeded	1/13/2019, 10:07:19 AM	4 minutes 14 seconds	Related events
CreateVm-MicrosoftWindowsS	Succeeded	1/13/2019, 9:23:00 AM	4 minutes 9 seconds	Related events
Microsoft.NetworkInterface-2C	Succeeded	1/13/2019, 9:17:46 AM	19 seconds	Related events
Microsoft.NetworkInterface-2C	Succeeded	1/13/2019, 9:04:08 AM	20 seconds	Related events
Microsoft.NetworkSecurityGro	Succeeded	1/11/2019, 11:08:33 PM	24 seconds	Related events
NetworkInterface.secondary-2	Succeeded	1/11/2019, 6:35:11 PM	21 seconds	Related events

And if you go to any deployment you can go the Template and see the template used for the deployment.

**Microsoft.DnsZone-20190102191149 - Template**

**Template**

```

1 {
2   "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
3   "contentVersion": "1.0.0.0",
4   "parameters": {
5     "dnsZoneName": {
6       "type": "String",
7       "metadata": {
8         "description": "The name of the DNS zone."
9       }
10    }
11  },
12  "resources": [
13    {
14      "type": "Microsoft.Network/dnszones",
15      "name": "[parameters('dnsZoneName')]",
16      "apiVersion": "2016-04-01",
17      "location": "global",
18      "properties": {}
19    }
20  ]
21 }
```

The other options are incorrect because these will not give the overall template deployment

for multiple resources.

For more information on resource template deployments, please visit the below URL

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

Ask our Experts

Rate this Question?  

**View Queries**

open ▾

**Question 4**

**Unattempted**

Domain :Manage Identities

You have configured Azure AD Connect for Azure Active Directory Seamless Single Sign-On (Azure AD Seamless SSO) for an on-premises network for your company. But users are reporting that when they attempt to access myapps.microsoft.com, they are prompted multiple times to sign in and are forced to use an account name that ends with onmicrosoft.com. You discover that there is a UPN mismatch between Azure AD and the on-premises Active Directory. You need to ensure that the users can use single-sign-on (SSO) to access Azure resources. What should you do first?

- A. From the on-premises network, deploy Active Directory Federation Services in a clustered environment.
- B. From Azure AD, add and verify a custom domain name. 
- C. From the on-premises network, request a new certificate that contains the Active Directory domain name.
- D. From the server that runs Azure AD Connect, modify the filtering options

---

**Explanation:**

Answer – B

This is also given in the Microsoft documentation

## UPN in Azure AD

The UPN is used by Azure AD to allow users to sign-in. The UPN that a user can use, depends on whether or not the domain has been verified. If the domain has been verified, then a user with that suffix will be allowed to sign-in to Azure AD.

The attribute is synchronized by Azure AD Connect. During installation, you can view the domains that have been verified and the ones that have not.

The screenshot shows the Microsoft Azure Active Directory Connect interface. The left sidebar has a navigation menu with options: Welcome, Express Settings, Connect to Azure AD, Connect to AD DS, **Azure AD sign-in** (which is selected and highlighted in blue), and Configure. The main content area is titled "Azure AD sign-in configuration". It contains a note: "To use on-premises credentials for Azure AD sign-in, UPN suffixes should match one of the verified custom domains in Azure AD. The following table lists the UPN suffixes defined in your on-premises environment, along with the matching custom domain in Azure." Below this is a table:

Active Directory UPN Suffix	Azure AD Domain
fabrikam.com	Not Added ?
fabrikamonline.eu	Not Verified ?
fabrikamonline.com	Verified

Option A is incorrect since we don't need AD FS in this scenario

Option C is incorrect since we don't need the certificate for Azure AD Connect

Option D is incorrect since the filtering is used for which objects need to be synched

For more information on the UPN in Azure AD Connect, please visit the below URL

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-userprincipalname>

Ask our Experts

Rate this Question?

View Queries

open ▾

Question 5

Unattempted

Domain :Implementing and Managing Storage

Your company has an Azure subscription. In the subscription, you go ahead and create an Azure file share named share1. You also create a shared access signature (SAS) named

SASdemo as shown in the following exhibit.

[Learn more](#)

Allowed services 

Blob  File  Queue  Table

Allowed resource types 

Service  Container  Object

Allowed permissions 

Read  Write  Delete  List  Add  Create  Update  Process

Start and expiry date/time 

Start

2019-01-02  11:16:46 PM

End

2019-01-03  7:16:46 AM

(UTC+04:00) --- Current Time Zone --- 

Allowed IP addresses 

193.77.134.10-193.77.134.50 

Allowed protocols 

HTTPS only  HTTPS and HTTP

Signing key 

key1 

**Generate SAS and connection string**

If you run Microsoft Azure Storage Explorer on a computer that has an IP address of 193.77.134.1 and you use SASdemo to connect to the storage account, then you

- A. will be prompted for the credentials
- B. will have no access 
- C. will have read, write and list access
- D. will have read-only access

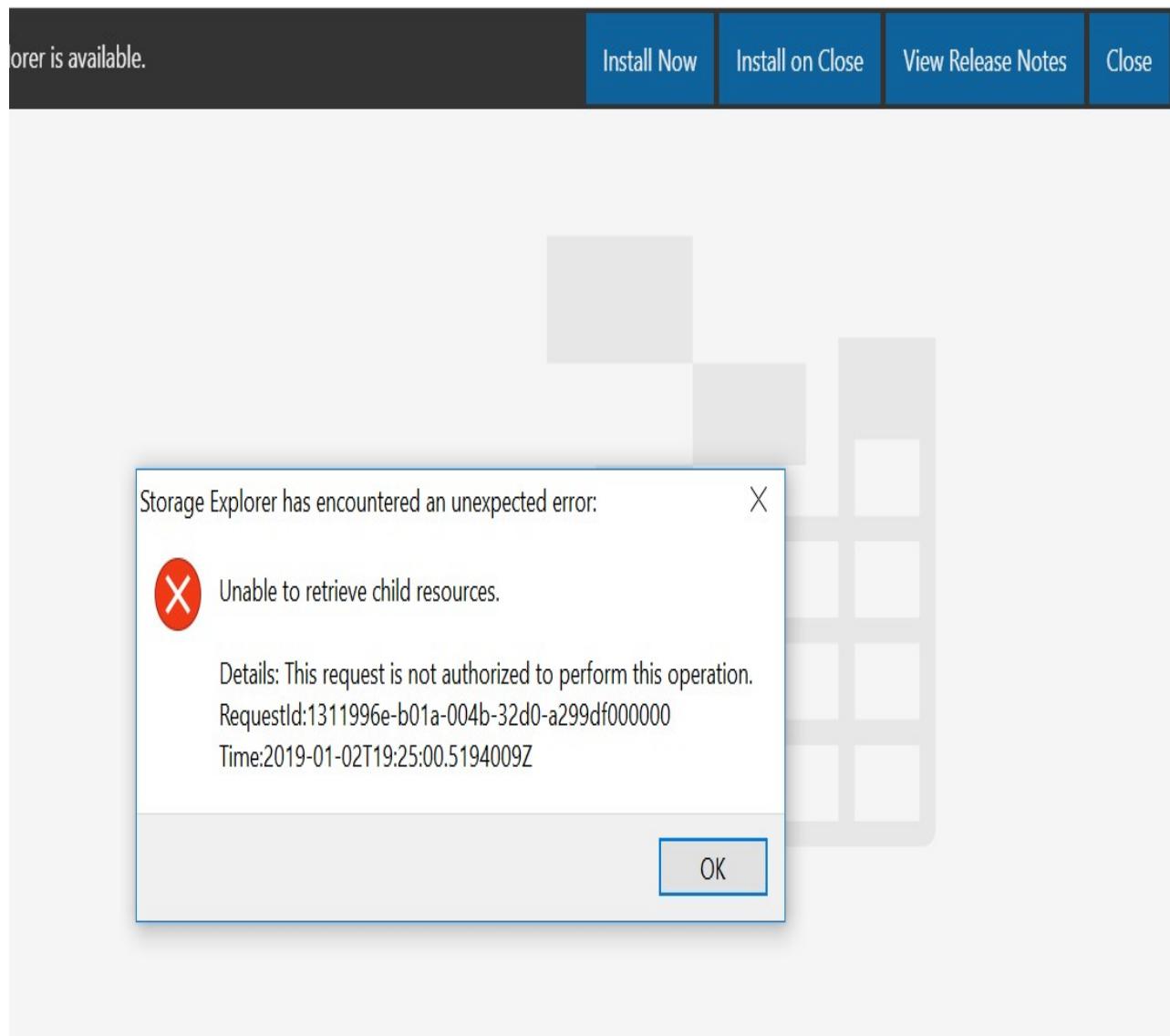
---

**Explanation:**

Answer – B

Since the IP address is not in the valid IP address range defined by the SAS url , you will be denied access.

You will get the below error in Azure Storage Explorer



Since this is the result of the SAS , all other options are incorrect.

For more information on Shared access signatures, please go to the below URL

<https://docs.microsoft.com/en-us/azure/storage/common/storage-dotnet-shared-access-signature-part-1>

[Ask our Experts](#)

Rate this Question? 😊 😢

[View Queries](#)

open ▾

**Question 6****Unattempted****Domain :Implementing and Managing Storage**

Your company has an Azure subscription. In the subscription, you go ahead and create an Azure file share named share1. You also create a shared access signature (SAS) named SASdemo as shown in the following exhibit.

[Learn more](#)**Allowed services** ⓘ Blob  File  Queue  Table**Allowed resource types** ⓘ Service  Container  Object**Allowed permissions** ⓘ Read  Write  Delete  List  Add  Create  Update  Process**Start and expiry date/time** ⓘ

Start

2019-01-02		11:16:46 PM
------------	--	-------------

End

2019-01-03		7:16:46 AM
------------	--	------------

(UTC+04:00) --- Current Time Zone ---

**Allowed IP addresses** ⓘ

193.77.134.10-193.77.134.50

**Allowed protocols** ⓘ HTTPS only  HTTPS and HTTP**Signing key** ⓘ

key1

**Generate SAS and connection string**

If you use the net use command on a computer that has an IP address of 193.77.134.50 and then use SASdemo to connect to share1, then you

A. will be prompted for the credentials

B. will have no access

C. will have read,write and list access 

D. will have read-only access

#### Explanation:

Answer – C

Since the IP address is in the valid IP address range, you will get the desired access that is specified in the SAS signature

```
net use : \\file.core.windows.net\ /u:  
example :  
net use z: \\samples.file.core.windows.net\logs /u:samples
```

For more information on Shared access signatures, please go to the below URL

<https://docs.microsoft.com/en-us/azure/storage/common/storage-dotnet-shared-access-signature-part-1>

Ask our Experts

Rate this Question?  

**View Queries**

open ▾

#### Question 7

Unattempted

Domain :Configure and Manage Virtual Networks

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 required?

A. 5 

B. 10

C. 15

D. 20

#### Explanation:

Answer – A

So, when you attach or have a network interface for a Virtual Machine, that network interface can have both a private and public IP address.

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
300	RDP	3389	TCP	Any	Any	<span>Allow</span>
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	<span>Allow</span>

So, by this measure, we only need to define 5 network interface cards, one for each virtual machine. Hence all the other options are incorrect

For more information on the virtual network interfaces in Azure, please visit the below URL

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

Ask our Experts

Rate this Question?

**View Queries**

open ▾

**Question 8**

**Unattempted**

Domain :Configure and Manage Virtual Networks

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 security groups that you require?

A. 1 

B. 2

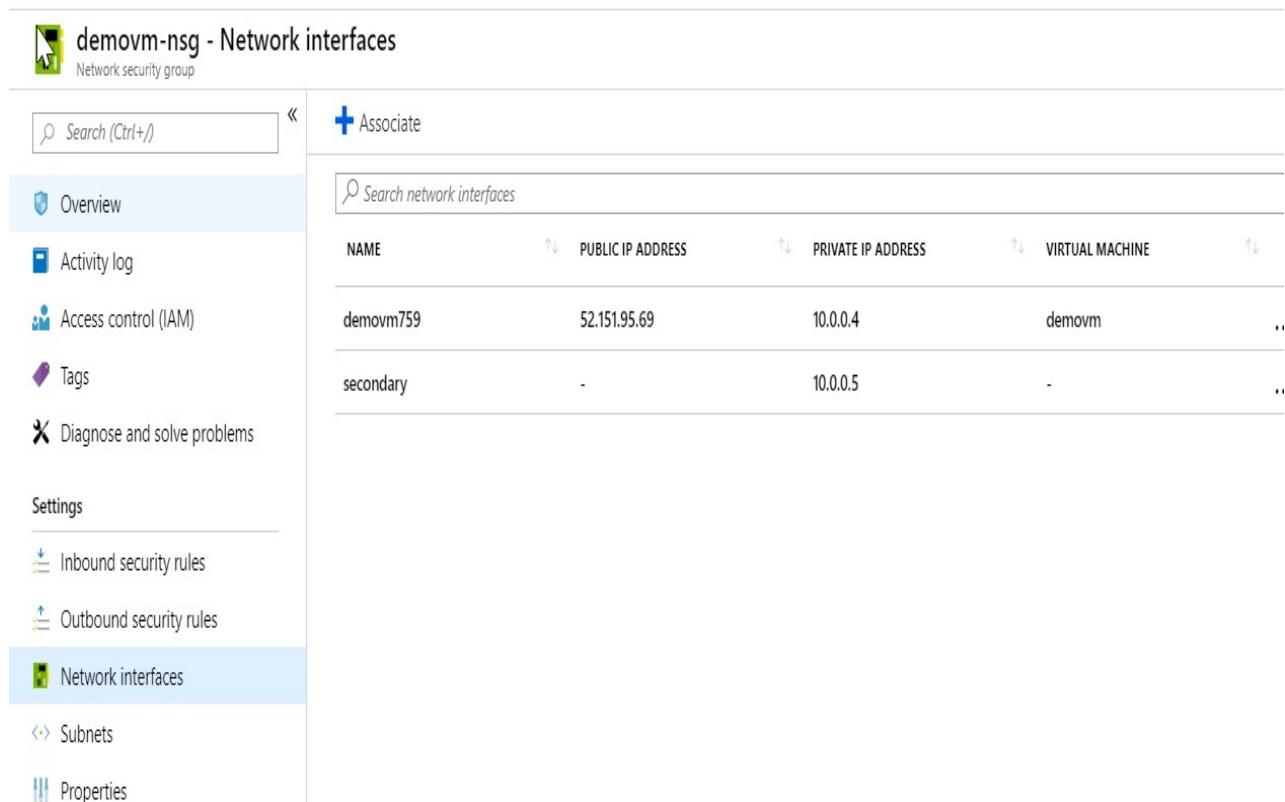
C. 5

D. 10

### Explanation:

Answer – A

A network security group can have multiple network interfaces assigned to it as shown in the below diagram



The screenshot shows the Azure portal interface for managing a Network Security Group (NSG). The left sidebar navigation bar is visible, showing options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Inbound security rules, Outbound security rules, Network interfaces (which is selected and highlighted in blue), Subnets, and Properties.

The main content area displays the 'demovm-nsg - Network interfaces' page. At the top, there's a search bar labeled 'Search (Ctrl+ /)' and a 'Associate' button. Below that is a table titled 'Search network interfaces' with columns: NAME, PUBLIC IP ADDRESS, PRIVATE IP ADDRESS, and VIRTUAL MACHINE.

NAME	PUBLIC IP ADDRESS	PRIVATE IP ADDRESS	VIRTUAL MACHINE
demovm759	52.151.95.69	10.0.0.4	demovm
secondary	-	10.0.0.5	-

Since the question clearly states that the virtual machines all require the same inbound and outbound security rules, hence we should use just the same network security group for all network interfaces

For more information on network security groups, please visit the below URL

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-vnet-plan-design-arm>

Ask our Experts

Rate this Question?  

[View Queries](#)[open ▾](#)**Question 9****Unattempted****Domain :Configure and Manage Virtual Networks**

You have a virtual network named VNet2 that has the configuration shown in the following exhibit.

```
Name          : VNET2
ResourceGroupName : demonew
Location       : uksouth
Id            : /subscriptions/baaa99b3-1d19-4c5e-90e1-39d55de5fc6e/resourceGroups/demonew/providers/Microsoft.Network/virtualNetworks/VNET2
Etag          : W/"b0b5ef85-4e7e-4d99-a2be-16f35e4fdc0a"
ResourceGuid   : 164448dd-357b-4c2b-8762-885ef8e90084
ProvisioningState : Succeeded
Tags          :
AddressSpace   : {
    "AddressPrefixes": [
        "10.2.0.0/16"
    ]
}
DhcpOptions   : {}
Subnets        : [
    {
        "Name": "default",
        "Etag": "W/"b0b5ef85-4e7e-4d99-a2be-16f35e4fdc0a"",
        "Id": "/subscriptions/baaa99b3-1d19-4c5e-90e1-39d55de5fc6e/resourceGroups/demonew/providers/Microsoft.Network/virtualNetworks/VNET2/subnets/default",
        "AddressPrefix": "10.2.0.0/24",
        "IpConfigurations": [],
        "ResourceNavigationLinks": [],
        "ServiceEndpoints": [],
        "ProvisioningState": "Succeeded"
    }
]
VirtualNetworkPeerings : []
EnableDdosProtection : false
DdosProtectionPlan   : null
```

Before a virtual machine on VNET2 can receive an IP address from 192.168.1.0/24 you must first

- A. Add a network interface
- B. Add a subnet

C. Add an address space ✓

D. Delete a subnet

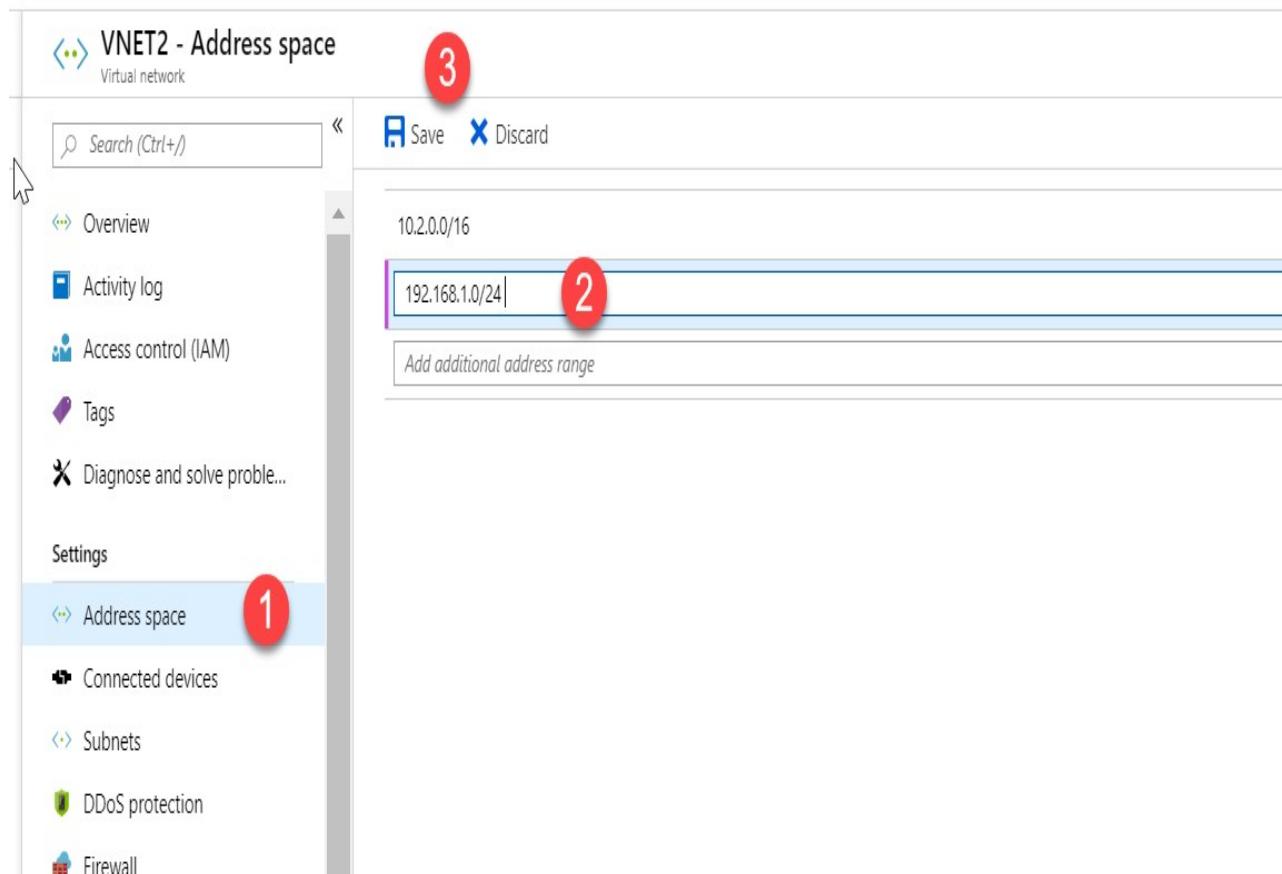
E. Delete an address space

### Explanation:

Answer – C

The Virtual Network has no address space which is relative to 192.168.1.0/24 as per the powershell output given in the Exhibit.

Hence first, you need to add an address space as shown below.



After you save the address space, create a new subnet with the address space and then ensure the VM is put in the new subnet

Option A is incorrect since the network interface can only receive an address from 10.2.0.0/24 as per the powershell output given in the Exhibit.

Option B is incorrect since you need to add the address space 192.168.1.0/24 before adding the subnet

Options D and E are incorrect since you need to add the address space and subnet and not delete the address space and subnet

For more information on Virtual Networks, please go to the below URL

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

---

Ask our Experts

Rate this Question?  

---

**View Queries**

open 

**Question 10**

**Unattempted**

Domain :Configure and Manage Virtual Networks

You have a virtual network named VNet2 that has the configuration shown in the following exhibit.

```
Name          : VNET2
ResourceGroupName : demonew
Location       : uksouth
Id            : /subscriptions/baaa99b3-1d19-4c5e-90e1-39d55de5fc6e/resourceGroups/demonew/providers/Microsoft.Network/virtualNetworks/VNET2
Etag          : W/"b0b5ef85-4e7e-4d99-a2be-16f35e4fdc0a"
ResourceGuid   : 164448dd-357b-4c2b-8762-885ef8e90084
ProvisioningState : Succeeded
Tags          :
AddressSpace   : {
    "AddressPrefixes": [
        "10.2.0.0/16"
    ]
}
DhcpOptions    : {}
Subnets        : [
    {
        "Name": "default",
        "Etag": "W/"b0b5ef85-4e7e-4d99-a2be-16f35e4fdc0a"",
        "Id": "/subscriptions/baaa99b3-1d19-4c5e-90e1-39d55de5fc6e/resourceGroups/demonew/providers/Microsoft.Network/virtualNetworks/VNET2/subnets/default",
        "AddressPrefix": "10.2.0.0/24",
        "IpConfigurations": [],
        "ResourceNavigationLinks": [],
        "ServiceEndpoints": [],
        "ProvisioningState": "Succeeded"
    }
]
VirtualNetworkPeerings : []
EnableDdosProtection : false
DdosProtectionPlan   : null
```

Before a virtual machine on VNET2 can receive an IP address from 10.2.1.0/24 you must first

- A. Add a network interface
- B. Add a subnet
- C. Add an address space
- D. Delete a subnet
- E. Delete an address space

#### Explanation:

Answer – B

Here you need to add a new subnet as shown below

The screenshot shows the Azure portal interface for managing subnets. On the left, there's a list of existing subnets under 'VNET2': 'default' (Address Range: 10.2.0.0/24, Available Addresses: 251). On the right, a 'Add subnet' dialog is open, showing fields for 'Name' (newsubnet), 'Address range (CIDR block)' (10.2.1.0/24), and other options like 'Network security group' (None) and 'Service endpoints' (None).

And then you can add the new VM as part of the new subnet so that it receives the address from the 10.2.1.0/24 address space.

Option A is incorrect since the network interface can only receive an address from 10.2.0.0/24 as per the powershell output given in the Exhibit.

Option C is incorrect since we already have the required address space

Options D and E are incorrect since you need to add the subnet and not delete the address space and subnet

For more information on Virtual Networks, please go to the below URL

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

Ask our Experts

Rate this Question?

View Queries

open ▾

Question 11

Unattempted

Domain :Implementing and Managing Storage

A company has an Azure subscription that contains the resources in the following table.

Name	Type
whizlabs-rg	Resource Group
whizlabstore	Azure Storage account
whizlabsync	Azure File Sync

whizlabstore contains a file share named documents. The document file share contains 1000 files.

You need to synchronize the files in documents to an on-premises server named whizlabserver. Which of the following would need to be implemented to fulfil this requirement? Choose 3 answers from the options given below

- A. Download an automation script.
- B. Create a container instance.
- C. Create a sync group.
- D. Register whizlabserver.
- E. Install the Azure File Sync agent on whizlabserver.

---

#### Explanation:

Answer – C, D and E

So, the Microsoft documentation gives the list of steps for using the Azure File Sync service

## In this article

### Prerequisites

[Prepare Windows Server to use with Azure File Sync](#)

[Install the Azure File Sync agent](#)

[Deploy the Storage Sync Service](#)

[Register Windows Server with Storage Sync Service](#)

[Create a sync group and a cloud endpoint](#)

[Create a server endpoint](#)

[Onboarding with Azure File Sync](#)

[Migrate a DFS Replication \(DFS-R\) deployment to Azure File Sync](#)

Since this is clearly given in the Microsoft documentation, all other options are incorrect

For more information on deploying Azure File Sync share, please go to the below URL

<https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-deployment-guide?tabs=portal>

---

Ask our Experts

Rate this Question?  

---

**View Queries**

open ▾

---

**Question 12**

**Unattempted**

Domain :Managing Azure Subscriptions and Resources

You have an Azure subscription.

You need to implement a custom policy that meet the following requirements:

Ensures that each new resource group in the subscription has a tag named organization set to a value of whizlabs

Ensures that resource group can be created from the Azure portal.

Ensures that compliance reports in the Azure portal are accurate.

You need to complete the below policy to match this requirement

```
1  {
2    "mode": "all",
3    "policyRule": {
4      "if": {
5        "allOf": [
6          {
7            "field": "tags['organization']",
8            "notEquals": "whizlabs"
9          },
10         {
11           "field": "type",
12           "equals": 1
13         }
14       ],
15     },
16     "then": {
17       "effect": 2
18     }
19   },
```

Which of the following would be the value in position 1 for the "equals" field?

- A. "Microsoft.Resources/deployments"
- B. "Microsoft.Resources/subscriptions"
- C. "Microsoft.Resources/subscriptions/resourceGroups" 
- D. resourceGroups

---

#### Explanation:

Answer – C

If you look at the default policy which is in place for enforcing tags, you can see that the Provider that needs to be used is the Resource groups.

## Enforce tag and its value on resource groups

Policy definition

Assign Edit definition Duplicate definition Delete definition

Enforces a required tag and its value on resource groups. /providers/Microsoft...

Effect: Deny, Type: Built-in  
Category: General, Mode: All

Definition (JSON) [Parameters](#)

```
1  {
2    "if": {
3      "allOf": [
4        {
5          "field": "[concat('tags[', parameters('tagName'), ']')]",
6          "notEquals": "[parameters('tagValue')]"
7        },
8        {
9          "field": "type",
10         "equals": "Microsoft.Resources/subscriptions/resourceGroups"
11       }
12     ]
13   },
14   "then": {
15     "effect": "deny"
16   }
17 }
```

1

Since this option is clearly mentioned in the Azure in-built policy, all other options are incorrect

For more information on Azure Policies, please visit the below URL

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

Ask our Experts

Rate this Question?

View Queries

open ▾

**Question 13****Unattempted****Domain :Managing Azure Subscriptions and Resources**

You have an Azure subscription.

You need to implement a custom policy that meet the following requirements:

Ensures that each new resource group in the subscription has a tag named organization set to a value of whizlabs

Ensures that resource group can be created from the Azure portal.

Ensures that compliance reports in the Azure portal are accurate.

You need to complete the below policy to match this requirement

```
1  {
2      "mode": "all",
3      "policyRule": {
4          "if": {
5              "allOf": [
6                  {
7                      "field": "tags['organization']",
8                      "notEquals": "whizlabs"
9                  },
10                 {
11                     "field": "type",
12                     "equals": 1
13                 }
14             ]
15         },
16         "then": {
17             "effect": 2
18         }
19     },
20 }
```

Which of the following would be the value in position 2 for the "effect" field?

- A. "Append"
- B. "Deny"
- C. "DeployIfNotExists"
- D. o

**Explanation:**

Answer – B

If you look at the default policy which is in place for enforcing tags, you can see that the effect should be Deny

## Enforce tag and its value on resource groups

Policy definition

Assign Edit definition Duplicate definition Delete definition

Enforces a required tag and its value on resource groups. /providers/Microsoft...

Effect: Deny; Type: Built-in

Category: General; Mode: All

Definition (JSON) [Parameters](#)

```
1  {
2    "if": {
3      "allOf": [
4        {
5          "field": "[concat('tags[', parameters('tagName'), ']')]",
6          "notEquals": "[parameters('tagValue')]"
7        },
8        {
9          "field": "type",
10         "equals": "Microsoft.Resources/subscriptions/resourceGroups"
11       }
12     ]
13   },
14   "then": {
15     "effect": "deny"
16   }
17 }
```

2

Since this option is clearly mentioned in the Azure in-built policy, all other options are incorrect

For more information on Azure Policies, please visit the below URL

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

Ask our Experts

Rate this Question?

View Queries

open ▾

**Question 14****Unattempted****Domain :Manage Identities**

You sign up for Azure Active Directory (Azure AD) Premium. You need to add a user named whizlabs-usr1@whizlabs.com as an administrator on all the computers that will be joined to the Azure AD domain. Where should you go in Azure AD to configure this setting?

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

**Explanation:**

Answer – A

If you go to the Devices blade in Azure AD , you can see the option to add local administrators

The screenshot shows the 'Devices' blade in the Azure portal. On the left, there's a sidebar with 'Manage' and several other options like 'All devices', 'Enterprise State Roaming', 'Audit logs', etc. The 'Device settings' option is highlighted with a red arrow and a circled '1'. The main area has a 'Save' and 'Discard' button at the top. It contains sections for 'Users may join devices to Azure AD' (with 'All' selected), 'Additional local administrators on Azure AD joined devices' (with 'Selected' selected), and 'Users may register their devices with Azure AD' (with 'All' selected). Below these are buttons for 'Yes' and 'No' under 'Require Multi-Factor Auth to join devices', and a dropdown for 'Maximum number of devices per user' set to '50'. At the bottom, there's a link to 'Enterprise State Roaming' and 'Manage Enterprise State Roaming settings'. Red arrows point from the numbered labels to the respective sections: arrow 1 points to the 'Device settings' link in the sidebar, and arrow 2 points to the 'Additional local administrators...' section.

Since this is the way to achieve this requirement, all other options are incorrect

For more information on device settings, please visit the below URL

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

Ask our Experts

Rate this Question?  

**View Queries**

open ▾

**Question 15**

**Unattempted**

Domain :Implementing and Managing Storage

A company needs to create a storage account that needs to conform to the following requirements

Users should be able to add files such as images and videos

Ability to store archive data

File shares need to be in place which can be accessed across several VM's

The data needs to be available even if a region goes down

The solution needs to be cost effective

Which of the following type of storage account would you create for this purpose?

- A. BLOB storage
- B. General Purpose(v1)
- C. General Purpose(v2) 
- D. Block blob storage

---

**Explanation:**

Answer – C

The below snapshot from the Microsoft documentation shows the different types of storage accounts

The following table describes the types of storage accounts and their capabilities:

Storage account type	Supported services	Supported performance tiers	Supported access tiers	Replication options	Deployment model <sup>1</sup>	Encryption <sup>2</sup>
General-purpose V2	Blob, File, Queue, Table, and Disk	Standard, Premium	Hot, Cool, Archive <sup>3</sup>	LRS, ZRS <sup>4</sup> , GRS, RA-GRS	Resource Manager	Encrypted
General-purpose V1	Blob, File, Queue, Table, and Disk	Standard, Premium	N/A	LRS, GRS, RA-GRS	Resource Manager, Classic	Encrypted
Blob storage	Blob (block blobs and append blobs only)	Standard	Hot, Cool, Archive <sup>3</sup>	LRS, GRS, RA-GRS	Resource Manager	Encrypted

Over here we can see that only General Purpose v2 supports all of the requirements. Hence all other options are incorrect.

For more information on storage accounts, please visit the below URL

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

Ask our Experts

Rate this Question?  

**View Queries**

open ▾

**Question 16**

**Unattempted**

Domain :Implementing and Managing Storage

A company needs to create a storage account that needs to conform to the following requirements

Users should be able to add files such as images and videos

Ability to store archive data

File shares need to be in place which can be accessed across several VM's

The data needs to be available even if a region goes down

The solution needs to be cost effective

What is the type of replication that needs to be configured for the storage account?

- A. Locally redundant storage (LRS)
- B. Zone-redundant storage (ZRS)
- C. Geo-redundant storage (GRS) 
- D. Read-access geo-redundant storage (RA-GRS)

---

**Explanation:**

Answer – C

The Microsoft documentation mentions the following

Geo-redundant storage (GRS) is designed to provide at least 99.9999999999999% (16 9's) durability of objects over a given year by replicating your data to a secondary region that is hundreds of miles away from the primary region. If your storage account has GRS enabled, then your data is durable even in the case of a complete regional outage or a disaster in which the primary region isn't recoverable.

Options A and B are incorrect since these replication strategies don't replicate the data across regions

Option D is incorrect additional read access to data in another region is not mentioned and we also have to keep cost to a minimum.

For more information on storage redundancy, please visit the below URL

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

---

Ask our Experts

Rate this Question?  

---

**View Queries**

open ▾

---

**Question 17**

**Unattempted**

Domain :Deploying and Managing Virtual Machines

You need to deploy two Azure virtual machines named VM1 and VM2 based on the Windows server 2016. The deployment must meet the following requirements:

Provide a Service Level Agreement (SLA) of 99.95 percent availability.

Use managed disks

You propose a solution to create a scale set for the requirement.  
Would the solution meet the goal?

A. Yes 

B. No

---

**Explanation:**

Answer – A

Requirement is VM need

1. VM need 99.95% Availability
2. Manage Disk

Azure supports creating of scale sets with Managed Disks and coming to SLA it's linked with the VMs been used and as such there's no SLA defined for Managed Disk alone.

[https://azure.microsoft.com/en-in/support/legal/sla/managed-disks/v1\\_0/](https://azure.microsoft.com/en-in/support/legal/sla/managed-disks/v1_0/)

<https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-design-overview#:~:text=Scale%20sets%20with%20Azure%20Managed,of%20traditional%20Azure%20sto~text>You%20do%20not%20have%20to,VMs%20in%20your%20scale%20set.>

## SLA for Managed Disks

Last updated: February 2017

Managed Disks does not have a financially backed SLA itself. The availability of Managed Disks is based on the SLA of the underlying storage used and virtual machine to which it is attached. Please see the [Virtual Machines](#) and [Storage SLA](#) for more details.

In fact, currently there is no Scale Sets for Disk. So Scale Sets for Disk is not supported. Yes Availability Zone for Disk is available.

## Create managed disk

Select the disk type and size needed for your workload. Azure Disks are designed for 99.999% availability. Azure Managed Disks encrypt your data at rest, by default, using Storage Service Encryption. [Learn more about disks.](#)

### Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

* Subscription <small>?</small>	<input type="text" value="Pay-As-You-Go"/>
	<input type="button" value="Select existing..."/>
	<input type="button" value="Create new"/>

### Disk details

* Disk name <small>?</small>	<input type="text"/>
* Region <small>?</small>	<input type="text" value="(Asia Pacific) West India"/>
Availability zone	<input type="text" value="None"/>
Source type <small>?</small>	<input type="text" value="Storage blob"/>
Source subscription	<input type="text" value="Pay-As-You-Go"/>
* Source blob <small>?</small>	<input type="text"/> <a href="#">Browse</a>
OS type <small>?</small>	<input type="radio"/> Windows <input type="radio"/> Linux <input checked="" type="radio"/> None (data disk)
* Size <small>?</small>	<input type="text" value="1023 GiB"/> Premium SSD <a href="#">Change size</a>

No SLA For VM Deployed in Scale Sets.

[https://azure.microsoft.com/en-ca/support/legal/sla/virtual-machine-scale-sets/v1\\_1/](https://azure.microsoft.com/en-ca/support/legal/sla/virtual-machine-scale-sets/v1_1/)

## SLA for Virtual Machine Scale Sets

Last updated: October 2017

Virtual Machine Scale Sets is a free service, therefore, it does not have a financially backed SLA itself. However, if the Virtual Machine Scale Sets includes Virtual Machines in at least 2 Fault Domains, the availability of the underlying Virtual Machines SLA for two or more instances applies. If the scale set contains a single Virtual Machine, the availability for a Single Instance Virtual Machine applies. See the [Virtual Machines SLA](#) for more details.

[Ask our Experts](#)

Rate this Question?  

[View Queries](#)

open 

**Question 18**

**Unattempted**

**Domain :Deploying and Managing Virtual Machines**

You need to deploy two Azure virtual machines named VM1 and VM2 based on the Windows server 2016 image. The deployment must meet the following requirements:

Provide a Service Level Agreement (SLA) of 99.95 percent availability.

Use managed disks

You propose a solution to create an availability set for the requirement.

Would the solution meet the goal?

A. Yes 

B. No

**Explanation:**

Answer – A

The Microsoft documentation mentions the following

## Configure multiple virtual machines in an availability set for redundancy

To provide redundancy to your application, we recommend that you group two or more virtual machines in an availability set. This configuration within a datacenter ensures that during either a planned or unplanned maintenance event, at least one virtual machine is available and meets the 99.95% Azure SLA. For more information, see the [SLA for Virtual Machines](#).

For more information on availability sets, please visit the below URL

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

[Ask our Experts](#)

Rate this Question?  

[View Queries](#)

open ▾

**Question 19**

**Unattempted**

**Domain :Deploying and Managing Virtual Machines**

You need to deploy two Azure virtual machines named VM1 and VM2 based on the Windows server 2016. The deployment must meet the following requirements:

Provide a Service Level Agreement (SLA) of 99.95 percent availability.

Use managed disks

You propose a solution to create a Traffic Manager for the requirement.  
Would the solution meet the goal?

A. Yes

B. No 

---

### Explanation:

Answer – B

Azure Traffic manager is used for traffic distribution based on DNS queries. For achieving high availability, you need to use Availability sets.

For more information on Azure Traffic Manager, please visit the below URL

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

[Ask our Experts](#)

Rate this Question?  

---

[View Queries](#)

[open ▾](#)

### Question 20

**Unattempted**

Domain :Manage Identities

A company has an Azure account and subscription. They are planning on implementing Azure AD connect to sync their on-premise users to Azure AD. You have so far carried out the following steps

Installed Azure AD connect on a domain joined member server

Setup a custom domain in Azure AD

Ensured all user's objects conform to the synchronization using the IdFix tool

Successfully setup Pass through authentication and Single Sign-on using the Azure AD connect wizard

Have confirmed that users from the on-premise AD have been successfully synced to Azure AD

You are now trying out Single Sign-on from a few machines, but it not working as expected. You are still being prompted for a user name and password. Which of the following should also be considered during the deployment process?

A. Install Azure AD connect on the domain controller

- B. Use password hash synchronization instead of pass through authentication
- C. Ensure a certificate is installed on the on-premise AD FS server
- D. Add "<https://autologon.microsoftazuread-sso.com>" to the Intranet zone settings by using Group Policy in Active Directory 

### Explanation:

Answer – D

This is mentioned in the Microsoft documentation as well as part of the steps required for implementing Single Sign-on

## Step 3: Roll out the feature

You can gradually roll out Seamless SSO to your users using the instructions provided below. You start by adding the following Azure AD URL to all or selected users' Intranet zone settings by using Group Policy in Active Directory:

- <https://autologon.microsoftazuread-sso.com>

In addition, you need to enable an Intranet zone policy setting called Allow updates to status bar via script through Group Policy.

### ① Note

The following instructions work only for Internet Explorer and Google Chrome on Windows (if it shares a set of trusted site URLs with Internet Explorer). Read the next section for instructions on how to set up Mozilla Firefox and Google Chrome on macOS.

### Why do you need to modify users' Intranet zone settings?

By default, the browser automatically calculates the correct zone, either Internet or Intranet, from a specific URL. For example, <http://contoso/> maps to the Intranet zone, whereas <http://intranet.contoso.com/> maps to the Internet zone (because the URL contains a period). Browsers will not send Kerberos tickets to a cloud endpoint, like the Azure AD URL, unless you explicitly add the URL to the browser's Intranet zone.

Option A is incorrect since Azure AD Connect should be installed on a domain joined member server and not on a domain controller.

Option B is incorrect since Single-Sign On can also be used for Pass through authentication

Option C is incorrect since for Azure AD Connect , you don't need an AD FS Server

For more information on Single Sign-On, one can go to the below URL

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-quick-start>

Ask our Experts

Rate this Question?  

**View Queries**

**open ▾**

**Question 21**

**Unattempted**

Domain :Deploying and Managing Virtual Machines

**View Case Study**

Which of the following should be used to ensure an SLA of 99.95% for the availability of Virtual Machines? Choose 2 answers from the options given below

- A. Azure Managed Disks 
- B. Azure Network Interfaces
- C. Azure Availability sets 
- D. Azure scale sets

---

#### **Explanation:**

Answer – A and C

The Microsoft documentation mentions the following

To provide redundancy to your application, we recommend that you group two or more virtual machines in an availability set. This configuration within a datacenter ensures that during either a planned or unplanned maintenance event, at least one virtual machine is available and meets the 99.95% Azure SLA

Managed disks provide better reliability for Availability Sets by ensuring that the disks of VMs in an Availability Set are sufficiently isolated from each other to avoid single points of failure. It does this by automatically placing the disks in different storage fault domains (storage clusters) and aligning them with the VM fault domain. If a storage fault domain fails due to hardware or software failure, only the VM instance with disks on the storage fault domain fails.

Option B is incorrect. Having multiple network interfaces can be used for recovery of application on virtual machines since you can move network interfaces across virtual machines. But then here to ensure that you are guaranteed an SLA of 99.5% uptime, you should use a combination of Azure Managed Disks and Azure availability sets

Option D is incorrect since this can be used to scale your application and can be used for high availability. But then here to ensure that you are guaranteed an SLA of 99.5% uptime, you should use a combination of Azure Managed Disks and Azure availability sets

For more information on managing availability for Virtual Machines, one can go to the below URL

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

---

Ask our Experts

Rate this Question?  

---

**View Queries**

open 

---

### Question 22

**Unattempted**

Domain :Implementing and Managing Storage

**View Case Study**

Which of the following account kind should be used for the storage account?

- A. **BLOB storage**
- B. **General Purpose v1**
- C. **General Purpose v2** 
- D. o

---

### Explanation:

Answer – C

Since the requirement is for "**document store**" where users will upload and download files, this is the correct answer. Reason, this storage type fulfills our business requirement and it's the one which is referred by Azure now.

The below snapshot from the Microsoft documentation shows the details of the different account types

Storage account type	Supported services	Supported performance tiers	Supported access tiers	Replication options	Deployment model <sup>1</sup>	Encryption <sup>2</sup>
General-purpose V2	Blob, File, Queue, Table, and Disk	Standard, Premium	Hot, Cool, Archive <sup>3</sup>	LRS, ZRS <sup>4</sup> , GRS, RA-GRS	Resource Manager	Encrypted
General-purpose V1	Blob, File, Queue, Table, and Disk	Standard, Premium	N/A	LRS, GRS, RA-GRS	Resource Manager, Classic	Encrypted
Blob storage	Blob (block blobs and append blobs only)	Standard	Hot, Cool, Archive <sup>3</sup>	LRS, GRS, RA-GRS	Resource Manager	Encrypted

For more information on storage accounts, one can go to the below URL

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

Ask our Experts

Rate this Question?  

**View Queries**

open ▾

**Question 23**

**Unattempted**

Domain :Manage Identities

**View Case Study**

You need to install the Azure AD Connect health agent on a domain joined member server. Which of the following role can be assigned to a user in Azure AD to perform this operation. You need to follow the least privilege rule when assigning roles.

- A. Service Administrator
- B. Global Administrator 
- C. User Administrator
- D. Compliance Administrator

**Explanation:**

Answer – B

The Microsoft documentation mentions that only the Global administrator can perform this operation

## Requirements

The following table is a list of requirements for using Azure AD Connect Health.

Requirement	Description
Azure AD Premium	Azure AD Connect Health is an Azure AD Premium feature and requires Azure AD Premium.  For more information, see <a href="#">Getting started with Azure AD Premium</a> To start a free 30-day trial, see <a href="#">Start a trial</a> .
You must be a global administrator of your Azure AD to get started with Azure AD Connect Health	By default, only the global administrators can install and configure the health agents to get started, access the portal, and perform any operations within Azure AD Connect Health. For more information, see <a href="#">Administering your Azure AD directory</a> .  Using Role Based Access Control you can allow access to Azure AD Connect Health to other users in your organization. For more information, see <a href="#">Role Based Access Control for Azure AD Connect Health</a> .  <b>Important:</b> The account used when installing the agents must be a work or school account. It cannot be a Microsoft account. For more information, see <a href="#">Sign up for Azure as an organization</a>

Since this is clearly mentioned in the documentation, all other options are invalid.

For more information on how to use Azure AD health agent, one can go to the below URL

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install>

Ask our Experts

Rate this Question?  

View Queries

open ▾

Question 24

Unattempted

Domain :Deploying and Managing Virtual Machines

View Case Study

How many availability sets would you create for deployment of the web and database virtual machines onto Azure?

- A. 1
- B. 2 
- C. 4
- D. 10

---

**Explanation:**

Answer – B

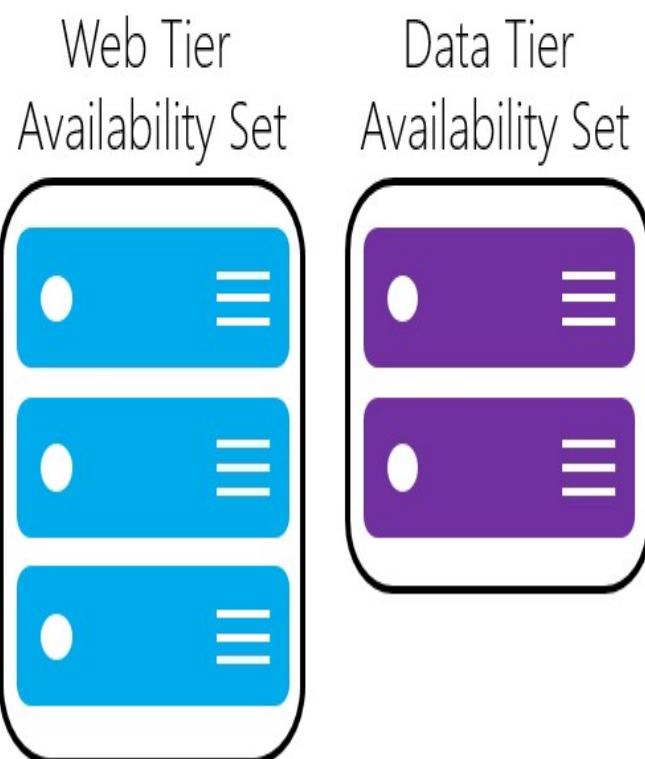
You should ideally create availability sets based on the number of tiers you have for your application.

This is also given in the Microsoft documentation

## Configure each application tier into separate availability sets

If your virtual machines are all nearly identical and serve the same purpose for your application, we recommend that you configure an availability set for each tier of your application. If you place two different tiers in the same availability set, all virtual machines in the same application tier can be rebooted at once. By configuring at least two virtual machines in an availability set for each tier, you guarantee that at least one virtual machine in each tier is available.

For example, you could put all the virtual machines in the front end of your application running IIS, Apache, Nginx in a single availability set. Make sure that only front-end virtual machines are placed in the same availability set. Similarly, make sure that only data-tier virtual machines are placed in their own availability set, like your replicated SQL Server virtual machines, or your MySQL virtual machines.



Since this is clearly mentioned in the documentation, all other options are invalid.

For more information on availability sets, one can go to the below URL

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

Ask our Experts

Rate this Question?

View Queries

open ▾

**Question 25****Unattempted****Domain :Configure and Manage Virtual Networks****View Case Study**

When adding custom domain names, which of the following record needs to be added to your custom domain registrar?

- A. A record
- B. NS record
- C. TXT record
- D. PTR record

---

**Explanation:**

Answer – C

When you add a custom domain name in Azure AD, below is an example of what you would need to add to your domain registrar to complete the registration of the custom domain.

whizlabs.com  
Custom domain name

 Delete

To use whizlabs.com with your Azure AD, create a new TXT record with your domain name registrar using the info below.

RECORD TYPE TXT MX

ALIAS OR HOST NAME  

DESTINATION OR POINTS TO ADDRESS  

TTL  

[Share these settings via email](#)

Verify domain  
Verification will not succeed until you have configured your domain with your registrar as described above.  
Verify

Since this is clearly shown, all other options are invalid

For more information on custom domain names in Azure, one can go to the below URL

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-custom-domain>

[Ask our Experts](#)

Rate this Question?  

[View Queries](#)

open ▾

**Question 26**

**Unattempted**

Domain :Configure and Manage Virtual Networks

[View Case Study](#)

Which of the following rule would you apply to the Network Security Group for the Network interface attached to the Web server?

- A. An inbound rule allowing traffic on port 80
- B. An inbound rule allowing traffic on port 443 ✓
- C. An outbound rule allowing traffic on port 80
- D. An outbound rule allowing traffic on port 443

### Explanation:

Answer – B

Since the users will connect via HTTPS, that means that port 443 should be open. And we need to add an Inbound security rule. An example is shown below

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	Port_443	443	TCP	Any	10.1.0.4/32	<span style="color: green;">✓</span> Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	<span style="color: green;">✓</span> Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	<span style="color: green;">✓</span> Allow
65500	DenyAllInBound	Any	Any	Any	Any	<span style="color: red;">✗</span> Deny

Option A is incorrect since this is the port for HTTP traffic

Options C and D are incorrect since you need to modify the Inbound security rule

For more information on security groups, one can go to the below URL

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

Ask our Experts

Rate this Question? 😊 😢

View Queries

open ▾

Question 27

Unattempted

Domain :Deploying and Managing Virtual Machines

## View Case Study

You need to ensure that Internet Information Services is automatically installed on the web tier Virtual Machines. You also need to ensure that Internet Information Services is always available on these machines. Which of the following can help achieve this requirement?

- A. Use the Azure DSC extension ✓
- B. Use the Network Watcher agent
- C. Create an availability set
- D. Create a scale set

### Explanation:

Answer – A

This is also given as an example in the Microsoft documentation

### Get started with cmdlets

The Azure DSC extension can use DSC configuration documents to directly configure Azure VMs during deployment. This step doesn't register the node to Automation. The node is *not* centrally managed.

The following example shows a simple example of a configuration. Save the configuration locally as `iisInstall.ps1`.

```
PowerShell Copy

configuration IISInstall
{
    node "localhost"
    {
        WindowsFeature IIS
        {
            Ensure = "Present"
            Name = "Web-Server"
        }
    }
}
```

Option B is invalid since this is used as a network performance monitoring, diagnostic, and analytics service

Option C is invalid since this is used to create a high availability solution

Option D is invalid since this is used to scale your solution

For more information on Overview of DSC for Azure Virtual Machines, one can go to the below URL

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

Ask our Experts

Rate this Question?  

**View Queries**

open ▾

**Question 28**

**Unattempted**

**Domain :Implementing and Managing Storage**

Your company wants to deploy a blogging solution on Azure. Below are the key deployment requirements

Ability to connect to Azure BLOB storage as the origin

Ensure that users across the world get the same performance when they access the blogging site

You provide a solution of using the Azure File Sync service. Does this solution meet the requirement?

A. Yes

B. No 

#### **Explanation:**

Answer – B

The Azure File Sync service is used as a file distribution service. The ideal solution to use here is the Content Delivery service

For more information on the File Sync Service, one can go to the below URL

<https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-planning>

Ask our Experts

Rate this Question?  

**View Queries**

open ▾

**Question 29**

**Unattempted**

**Domain :Implementing and Managing Storage**

Your company wants to deploy a blogging solution on Azure. Below are the key deployment requirements

Ability to connect to Azure BLOB storage as the origin

Ensure that users across the world get the same performance when they access the blogging site

You provide a solution of using the Content Delivery Network. Does this solution meet the requirement?

A. Yes 

B. No

**Explanation:**

Answer – A

Yes, this is the correct solution. The Microsoft documentation mentions the following

Azure Content Delivery Network (CDN) offers developers a global solution for rapidly delivering high-bandwidth content to users by caching their content at strategically placed physical nodes across the world. Azure CDN can also accelerate dynamic content, which cannot be cached, by leveraging various network optimizations using CDN POPs. For example, route optimization to bypass Border Gateway Protocol (BGP).

The benefits of using Azure CDN to deliver web site assets include:

Better performance and improved user experience for end users, especially when using applications in which multiple round-trips are required to load content.

Large scaling to better handle instantaneous high loads, such as the start of a product launch event.

Distribution of user requests and serving of content directly from edge servers so that less traffic is sent to the origin server.

For more information on the Content Delivery Network service, one can go to the below URL

<https://docs.microsoft.com/en-us/azure/cdn/cdn-overview>

**Ask our Experts**

**Rate this Question?**  

**View Queries**

**open ▼**

**Question 30****Unattempted****Domain :Implementing and Managing Storage**

Your company wants to deploy a blogging solution on Azure. Below are the key deployment requirements

Ability to connect to Azure BLOB storage as the origin

Ensure that users across the world get the same performance when they access the blogging site

You provide a solution of using the cloud tiering service. Does this solution meet the requirement?

A. Yes

B. No 

**Explanation:**

Answer – B

The cloud tiering feature is used to ensure volumes have a percentage of free space when you use the Azure File Sync service. The ideal solution to use here is the Content Delivery service

For more information on cloud tiering, one can go to the below URL

<https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-cloud-tiering>

[Ask our Experts](#)[Rate this Question? !\[\]\(0543580a0d5cc16093caeca5ef5b67ae\_img.jpg\) !\[\]\(14704be5c6a7621ab060922cd42889db\_img.jpg\)](#)[View Queries](#)[open ▾](#)**Question 31****Unattempted****Domain :Managing Azure Subscriptions and Resources**

Your company has an Azure account and an Azure subscription. They have created a Virtual Network named whizlabs-net. The following users have been setup

User	Role
whizlabs-usr1	Owner
whizlabs-usr2	Security admin

whizlabs-usr3

Network Contributor

Which of the following users would be able to add a subnet to the Virtual Network?

- A. whizlabs-usr1 only
- B. whizlabs-usr2 only
- C. whizlabs-usr3 only
- D. whizlabs-usr1 and whizlabs-usr2 only
- E. whizlabs-usr1 and whizlabs-usr3 only 
- F. whizlabs-usr2 and whizlabs-usr3 only
- G. whizlabs-usr1, whizlabs-usr2 and whizlabs-usr3

#### Explanation:

Answer – E

If you look at the Network Contributor Role, they have access to manage Virtual Networks. And then by default the Owner will have all privileges over Azure resources.

## Network Contributor

Description	Lets you manage networks, but not access to them.
Id	4d97b98b-1d4f-4787-a291-c67834d212e7

For more information on the built-in roles, please go to the below URL

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

[Ask our Experts](#)[Rate this Question? !\[\]\(0c0a7169d07bb83b4413369246d7d571\_img.jpg\) !\[\]\(8af23bfdacdba3ba0d208cef6cbc5bde\_img.jpg\)](#)[View Queries](#)[open ▾](#)**Question 32****Unattempted**

**Domain :Managing Azure Subscriptions and Resources**

Your company has an Azure account and an Azure subscription. They have created a Virtual Network named whizlabs-net. The following users have been setup

User	Role
whizlabs-usr1	Owner
whizlabs-usr2	Security admin
whizlabs-usr3	Network Contributor

Which of the following users would be able to add the Reader role access for a user to the Virtual Network?

- A. whizlabs-usr1 only
- B. whizlabs-usr2 only
- C. whizlabs-usr3 only
- D. whizlabs-usr1 and whizlabs-usr2 only
- E. whizlabs-usr1 and whizlabs-usr3 only
- F. whizlabs-usr2 and whizlabs-usr3 only
- G. whizlabs-usr1, whizlabs-usr2 and whizlabs-usr3

**Explanation:**

Answer – A

The Network Contributor does not have access to assign roles. And if you look at the Security admin role , it only has the privilege to work with Security Center.

## Security Admin

Description	In Security Center only: Can view security policies, view security states, edit security policies, view alerts and recommendations, dismiss alerts and recommendations
-------------	--

For more information on the built-in roles, please go to the below URL

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

Ask our Experts

Rate this Question?  

View Queries

open ▾

**Question 33**

**Unattempted**

Domain :Managing Azure Subscriptions and Resources

You work as an Azure Administrator for a company. You have to ensure that a role can be in place that would have the following requirements

View all the resources in the Azure subscription

Issue support requests to Microsoft.

Use the principle of least privilege.

You have to complete the below JSON role definition

```
[  
 {  
   "assignable Scopes": [  
     "/"  
   ],  
   "description": "Lets you create and manage Support requests",  
   "id": "/subscriptions/20c6eec9-2d80-4700-b0f6-  
4fde579a8783/providers/Microsoft.Authorization/roleDefinitions/cfd33db0-3dd1-45e3-aa9d-  
cdbdf3b6f24e",  
   "name": "cf33db0-3dd1-45e3-aa9d-cdbdf3b6f24e",  
   "permissions": [  
     {  
       "actions": [  
         Slot1  
       ,  
       "Microsoft.Resources/subscriptions/resource Groups/read",  
       Slot2  
     ],  
       "dataActions": [],  
       "notActions": [],  
       "notDataActions": []  
     }  
   ],  
   "roleName": "Support Request Contributor",  
   "roleType": "BuiltInRole",  
   "type": "Microsoft.Authorization/roleDefinitions"  
 }  
 ]
```

Which of the following would go into Slot1?

- A. **"Microsoft.Authorization/\*/\*"**
- B. **"Microsoft.Authorization/\*/read"** 
- C. **" Microsoft.Authorization/read/\*"**
- D. **o**

---

#### Explanation:

Answer - B

If you look at the Microsoft documentation for the role definition, you can see that the correct action is "Microsoft.Authorization/\*/read"

## Support Request Contributor

Description Lets you create and manage Support requests

Id cfd33db0-3dd1-45e3-aa9d-cdbdf3b6f24e

Actions

Microsoft.Authorization/\*/read Read authorization

Microsoft.Resources/subscriptions/resourceGroups/read Gets or lists resource groups.

Microsoft.Support/\* Create and manage support tickets

For more information on the built-in roles, please go to the below URL

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

Ask our Experts

Rate this Question?  

[View Queries](#)

open ▾

### Question 34

Unattempted

Domain :Managing Azure Subscriptions and Resources

You work as an Azure Administrator for a company. You have to ensure that a role can be in place that would have the following requirements

View all the resources in the Azure subscription

Issue support requests to Microsoft.

Use the principle of least privilege.

You have to complete the below JSON role definition

```
[  
 {  
   "assignable Scopes": [  
     "/"  
   ],  
   "description": "Lets you create and manage Support requests",  
   "id": "/subscriptions/20c6eec9-2d80-4700-b0f6-  
4fde579a8783/providers/Microsoft.Authorization/roleDefinitions/cfd33db0-3dd1-45e3-aa9d-  
cdbdf3b6f24e",  
   "name": "cf33db0-3dd1-45e3-aa9d-cdbdf3b6f24e",  
   "permissions": [  
     {  
       "actions": [  
         Slot1  
       ,  
       "Microsoft.Resources/subscriptions/resource Groups/read",  
       Slot2  
     ],  
       "dataActions": [],  
       "notActions": [],  
       "notDataActions": []  
     }  
   ],  
   "roleName": "Support Request Contributor",  
   "roleType": "BuiltInRole",  
   "type": "Microsoft.Authorization/roleDefinitions"  
 }  
 ]
```

Which of the following would go into Slot2?

- A.    `"*/"`
- B.    `"*/Microsoft.Support"`
- C.    `"Microsoft.Support/*"` 
- D.    `o`

---

#### Explanation:

Answer – C

If you look at the Microsoft documentation for the role definition, you can see that the correct action is "Microsoft.Support/\*"

## Support Request Contributor

Description Lets you create and manage Support requests

Id cfd33db0-3dd1-45e3-aa9d-cdbdf3b6f24e

### Actions

Microsoft.Authorization/\*/read Read authorization

Microsoft.Resources/subscriptions/resourceGroups/read Gets or lists resource groups.

Microsoft.Support/\* Create and manage support tickets

For more information on the built-in roles, please go to the below URL

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

Ask our Experts

Rate this Question?  

[View Queries](#)

open ▾

**Question 35**

**Unattempted**

Domain :Configure and Manage Virtual Networks

You are an IT Administrator for a company. You have been requested to set up a public load balancer in Azure.

\$whizlabspublicip = Slot1 -ResourceGroupName whizlabs-rg -Name

'LoadbalancerIP' -Location westeurope -AllocationMethod Static -Sku Standard

\$whizlabsfrontendIP = Slot2 -Name 'FrontEndPool' -PublicIpAddress  
\$whizlabspublicip

Which of the following commands would go into Slot1?

- A. **New-AzureRmPublicIpAddress** ✓
- B. **New-AzureRmLoadBalancerFrontendIpConfig**
- C. **Set-AzureRmPublicIpAddress**
- D. **Set-AzureRmLoadBalancerFrontendIpConfig**

---

#### Explanation:

Answer - A

An example of this is given in the Microsoft documentation

## Create a public IP Standard

Create a Public IP Standard using the following command:

PowerShell

 Copy

```
$publicIp = New-AzureRmPublicIpAddress -ResourceGroupName myResourceGroup -Name 'myPublicIP' `  
-Location westeurope -AllocationMethod Static -Sku Standard
```

## Create a front-end IP configuration for the website

Create a frontend IP configuration using the following command:

PowerShell

 Copy

```
$feip = New-AzureRmLoadBalancerFrontendIpConfig -Name 'myFrontEndPool' -PublicIpAddress $publicIp
```

Since this is clearly given in the documentation, all other options are incorrect

For more information on creating a load balancer via Powershell, please go to the below URL

<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-get-started-internet-az-powershell>

[Ask our Experts](#)

Rate this Question?  

[View Queries](#)

[open ▾](#)

**Question 36**

**Unattempted**

Domain :Configure and Manage Virtual Networks

You are an IT Administrator for a company. You have been requested to setup a public load balancer n Azure.

\$whizlabspublicip = Slot1 -ResourceGroupName whizlabs-rg -Name

'LoadbalancerIP' -Location westeurope -AllocationMethod Static -Sku Standard

\$whizlabsfrontendIP = Slot2 -Name 'FrontEndPool' -PublicIpAddress  
\$whizlabspublicip

Which of the following commands would go into Slot2?

- A. **New-AzureRmPublicIpAddress**
- B. **New-AzureRmLoadBalancerFrontendIpConfig** ✓
- C. **Set-AzureRmPublicIpAddress**
- D. **Set-AzureRmLoadBalancerFrontendIpConfig**

---

#### Explanation:

Answer - B

An example of this is given in the Microsoft documentation

## Create a public IP Standard

Create a Public IP Standard using the following command:

PowerShell

 Copy

```
$publicIp = New-AzureRmPublicIpAddress -ResourceGroupName myResourceGroup -Name 'myPublicIP' `  
-Location westeurope -AllocationMethod Static -Sku Standard
```

## Create a front-end IP configuration for the website

Create a frontend IP configuration using the following command:

PowerShell

 Copy

```
$feip = New-AzureRmLoadBalancerFrontendIpConfig -Name 'myFrontEndPool' -PublicIpAddress $publicIp
```

Since this is clearly given in the documentation, all other options are incorrect

For more information on creating a load balancer via powershell, please go to the below URL

<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-get-started-internet-az-powershell>

[Ask our Experts](#)

Rate this Question?  

[View Queries](#)

open ▾

**Question 37**

**Unattempted**

Domain :Manage Identities

A company has an Azure account and currently has an Azure premium P2 based subscription. As an IT administrator, you have to configure a conditional access policy as shown below

\* Name

whizlabs-policy



## Assignments

---

Users and groups ⓘ  
0 users and groups selected



Cloud apps ⓘ  
0 cloud apps selected



Conditions ⓘ  
0 conditions selected



## Access controls

---

Grant ⓘ  
0 controls selected



Session ⓘ  
0 controls selected



## Enable policy

On

Off

---

Create

You have to ensure the following key requirement

Users from select locations would need to authenticate using MFA.

In which of the following sections would you configure the locations for the policy?

- A. Users and Groups
- B. Conditions
- C. Grants
- D. Session

---

### Explanation:

Answer – B

If you see the Conditions section, you will have the ability to define the locations set for the policy

New	Conditions	Locations
<p><b>Info</b></p> <p>* Name whizlabs-policy</p> <hr/> <p><b>Assignments</b></p> <p>Users and groups ⓘ 0 users and groups selected</p> <p>Cloud apps ⓘ 0 cloud apps selected</p> <p>Conditions ⓘ 0 conditions selected</p> <hr/> <p><b>Access controls</b></p> <p>Grant ⓘ 0 controls selected</p> <p>Session ⓘ 0 controls selected</p> <hr/> <p><b>Enable policy</b></p> <p>On    Off</p> <hr/>	<p><b>Info</b></p> <hr/> <p>Sign-in risk ⓘ Not configured</p> <hr/> <p>Device platforms ⓘ Not configured</p> <hr/> <p>Locations ⓘ Not configured</p> <hr/> <p>Client apps (preview) ⓘ Not configured</p> <hr/> <p>Device state (preview) ⓘ Not configured</p> <hr/>	<p>Control user access based on their physical location. <a href="#">Learn more</a></p> <p>Configure ⓘ</p> <p>Yes    No</p> <p>Include    Exclude</p> <hr/> <p><input type="radio"/> Any location</p> <p><input type="radio"/> All trusted locations</p> <p><input type="radio"/> Selected locations</p> <hr/> <p>Select None</p> <hr/>
<p>Create</p>	<p>Done</p>	<p>Done</p>

Since this is clearly shown in the implementation, all other options are incorrect

For more information on conditional access policies, please go to the below URL

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

Ask our Experts

Rate this Question?  

View Queries

open ▾

Question 38

Unattempted

Domain :Manage Identities

A company has an Azure account and current has an Azure premium P2 based subscription. As an IT administrator, you have to configure a conditional access policy as shown below

\* Name

whizlabs-policy



### Assignments

Users and groups 



0 users and groups selected

Cloud apps 



0 cloud apps selected

Conditions 



0 conditions selected

### Access controls

Grant 



0 controls selected

Session 



0 controls selected

### Enable policy

On

Off

Create

You have to ensure the following key requirement

Users from select locations would need to authenticate using MFA.

In which of the following sections would you configure the MFA requirement for the policy?

- A. Users and Groups
- B. Conditions
- C. Grant
- D. Session

---

**Explanation:**

Answer – C

If you see the Grant section, you will have the ability to define the MFA requirement

## New

**Info**

\* Name  
whizlabs-policy

### Assignments

Users and groups ⓘ >  
0 users and groups selected

Cloud apps ⓘ >  
0 cloud apps selected

Conditions ⓘ >  
0 conditions selected

### Access controls

Grant ⓘ >  
0 controls selected

Session ⓘ >  
0 controls selected

### Enable policy

On Off

Create

## Grant

Select the controls to be enforced.

Block access  
 Grant access

Require multi-factor authentication ⓘ

Require device to be marked as compliant ⓘ

Require Hybrid Azure AD joined device ⓘ

Require approved client app ⓘ  
See list of approved client apps

For multiple controls

Require all the selected controls  
 Require one of the selected controls

Select

Since this is clearly shown in the implementation, all other options are incorrect

For more information on conditional access policies, please go to the below URL

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

[Ask our Experts](#)Rate this Question?  [View Queries](#)

open ▾

**Question 39****Unattempted****Domain :Configure and Manage Virtual Networks**

A company currently has an Azure subscription. They have deployed a Virtual Network to the subscription. The details of the Network are given below

Name	Type	Address range	Part of Network
whizlabs-net	Virtual Network	10.1.0.0/16	NA
SubnetA	Subnet	10.1.0.0/24	whizlabs-net
GatewaySubnet	Subnet	10.1.255.0/27	whizlabs-net

You have to setup a Site-to-Site VPN connection with your on-premise network. The VPN device has an IP address of 12.10.79.10. Your on-premise network has an IP address range of 10.101.1.0/24.

You now have to configure the local network gateway as shown below

## Create local network gate...

□ X

\* Name

 ✓

\* IP address i

Address space i

 ...

Configure BGP settings

\* Subscription

 ▼

\* Resource group i

 ▼

[Create new](#)

\* Location

 ▼

Which of the following would you enter as the IP address for the Local Network gateway?

- A. **10.1.0.0**
- B. **10.101.1.0**
- C. **10.1.255.0**
- D. **12.10.79.10** ✓

### Explanation:

Answer – D

The IP address needs to be that of the IP address allocated to the VPN device.

This is also mentioned in the Microsoft documentation

3. On the [Create local network gateway page](#), specify the values for your local network gateway.

- **Name:** Specify a name for your local network gateway object.
- **IP address:** This is the public IP address of the VPN device that you want Azure to connect to. Specify a valid public IP address. If you don't have the IP address right now, you can use the values shown in the example, but you'll need to go back and replace your placeholder IP address with the public IP address of your VPN device. Otherwise, Azure will not be able to connect.

For more information on creating site to site VPN connections, please go ahead and visit the below URL

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal>

[Ask our Experts](#)

Rate this Question?  

[View Queries](#)

[open ▾](#)

**Question 40**

**Unattempted**

Domain :Configure and Manage Virtual Networks

A company currently has an Azure subscription. They have deployed a Virtual Network to the subscription. The details of the Network are given below

Name	Type	Address range	Part of Network
whizlabs-net	Virtual Network	10.1.0.0/16	NA
SubnetA	Subnet	10.1.0.0/24	whizlabs-net
GatewaySubnet	Subnet	10.1.255.0/27	whizlabs-net

You have to setup a Site-to-Site VPN connection with your on-premise network. The VPN device has an IP address of 12.10.79.10. Your on-premise network has an IP address range of 10.101.1.0/24.

You now have to configure the local network gateway as shown below

## Create local network gate...

X

\* Name

 ✓

\* IP address i

Address space i

 ...

Configure BGP settings

\* Subscription

 ▼

\* Resource group i

 ▼

[Create new](#)

\* Location

 ▼

Which of the following would you enter as the address range for the Local Network gateway?

- A. **10.1.0.0/24**
- B. **10.1.255.0/27**
- C. **10.101.1.0/24** ✓
- D. **10.1.0.0/16**

### Explanation:

Answer – C

The address space needs to be that of the Address range of the local network in your on-premise environment.

This is also mentioned in the Microsoft documentation

3. On the [Create local network gateway page](#), specify the values for your local network gateway.

- **Name:** Specify a name for your local network gateway object.
- **IP address:** This is the public IP address of the VPN device that you want Azure to connect to. Specify a valid public IP address. If you don't have the IP address right now, you can use the values shown in the example, but you'll need to go back and replace your placeholder IP address with the public IP address of your VPN device. Otherwise, Azure will not be able to connect.
- **Address Space** refers to the address ranges for the network that this local network represents. You can add multiple address space ranges. Make sure that the ranges you specify here do not overlap with ranges of other networks that you want to connect to. Azure will route the address range that you specify to the on-premises VPN device IP address. *Use your own values here if you want to connect to your on-premises site, not the values shown in the example.*

For more information on creating site to site VPN connections, please go ahead and visit the below URL

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal>

[Ask our Experts](#)

Rate this Question?  

[View Queries](#)

[open ▾](#)

**Question 41**

**Unattempted**

Domain :Configure and Manage Virtual Networks

Which of the following needs to be setup in Azure for the Site-to-Site VPN connection?

- A. An additional address space for the Virtual Network
- B. A service endpoint
- C. A gateway subnet 
- D. A gateway Virtual Machine

**Explanation:**

Answer – C

This is also given in the Microsoft documentation

### 3. Create the gateway subnet

The virtual network gateway uses specific subnet called the gateway subnet. The gateway subnet is part of the virtual network IP address range that you specify when configuring your virtual network. It contains the IP addresses that the virtual network gateway resources and services use. The subnet must be named 'GatewaySubnet' in order for Azure to deploy the gateway resources. You can't specify a different subnet to deploy the gateway resources to. If you don't have a subnet named 'GatewaySubnet', when you create your VPN gateway, it will fail.

Since this is clearly mentioned in the Microsoft documentation, all other options are incorrect

For more information on creating a Site-to-Site VPN connection, please go ahead and visit the below URL

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal>

---

Ask our Experts

Rate this Question?  

---

**View Queries**

open ▾

---

**Question 42**

**Unattempted**

**Domain :Configure and Manage Virtual Networks**

You have the Azure virtual networks shown in the following table.

Name	Address space	Subnet	Resource Group-Region
VNet1	10.11.0.0/16	10.11.0.0/17	West US
VNet2	10.11.0.0/17	10.11.0.0/25	West US
VNet3	10.10.0.0/22	10.10.1.0/24	East US
VNet4	192.168.16.0/22	192.168.16.0/24	North Europe

To which virtual networks can you establish a peering connection from VNet1?

- A. VNet2 and VNet3 only
- B. VNet2 only
- C. VNet3 and VNet4 only
- D. VNet2, VNet3, and VNet4

---

**Explanation:**

Answer – C

Vnet2 has an overlapping CIDR block, so Virtual Network peering cannot be established to this Virtual Network from VNet1

For more information on Virtual Network peering, please visit the below URL

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

[Home](#) > [Virtual networks](#) > Create virtual network

## Create virtual network

[Basics](#) [IP Addresses](#) [Security](#) [Tags](#) [Review + create](#)

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

**IPv4 address space**  

The address space '10.11.0.0/17' overlaps with '10.11.0.0/16' in virtual network 'myVirtualNetwork1'.

[Ask our Experts](#)[Rate this Question?](#)  [View Queries](#)[open](#) ▾**Question 43****Unattempted****Domain :Configure and Manage Virtual Networks**

Your company has an Azure account and a subscription. The subscription contains the virtual networks in the following table

Name	Address Space	Subnet name	Subnet address range
VNet1	10.1.0.0/16	Subnet1	10.1.1.0/24
VNet2	10.10.0.0/16	Subnet2	10.10.1.0/24
VNet3	172.16.0.0/16	Subnet3	172.16.1.0/24

The subscription also contains the virtual machines in the following table

Name	Network	Subnet	IP address
VM1	VNet1	Subnet1	10.1.1.4
VM2	VNet2	Subnet2	10.10.1.4
VM3	VNet3	Subnet3	172.16.1.4

The firewalls on all the virtual machines are configured to allow all ICMP traffic

You add the peerings in the following table.

Virtual Network	Peering Network
VNet1	VNet3
VNet2	VNet3
VNet3	VNet1

For each of the following statements, select Yes if the statement is true

VM1 can ping VM3

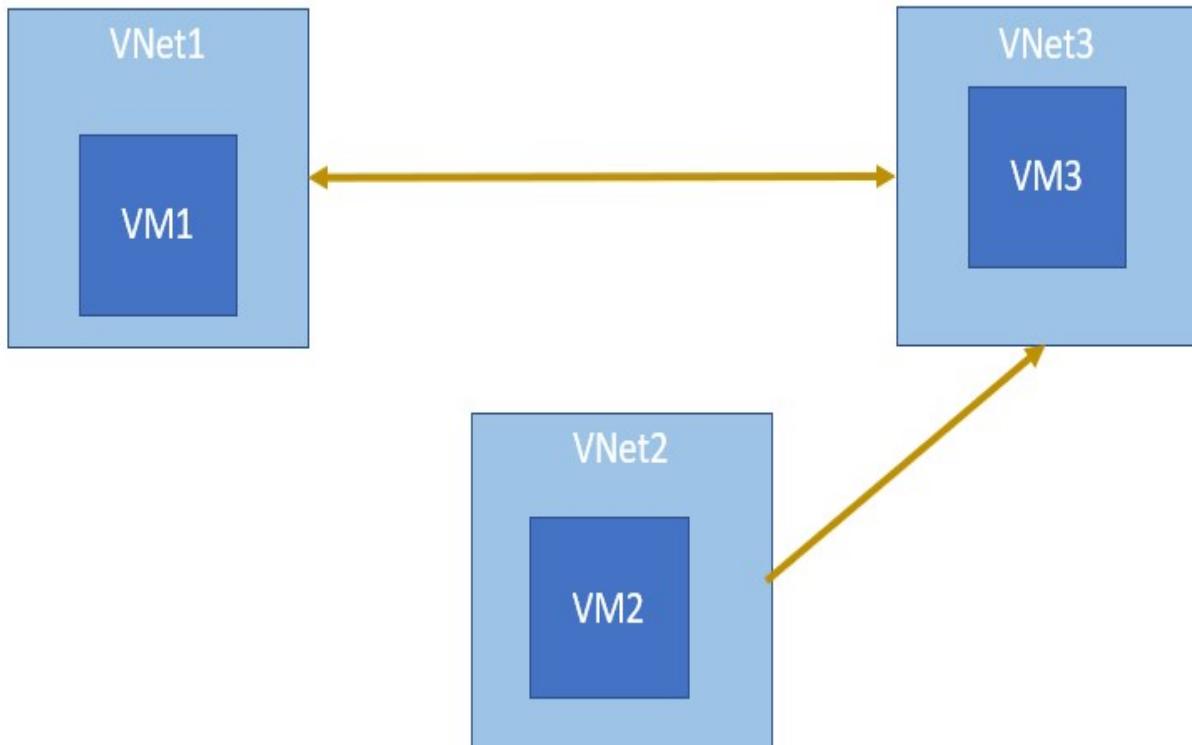
A. Yes

B. No

#### Explanation:

Answer – A

So, if you look at the overall picture for the VNET peerings , below is the diagram that we have



Now since there are peerings in both directions for VNET1 and VNET3 , the VM's can ping each

other.

For more information on VNET peering, please visit the below URL

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

Ask our Experts

Rate this Question?  

**View Queries**

open ▾

#### Question 44

Unattempted

Domain :Configure and Manage Virtual Networks

Your company has an Azure account and a subscription. The subscription contains the virtual networks in the following table

Name	Address Space	Subnet name	Subnet address range
VNet1	10.1.0.0/16	Subnet1	10.1.1.0/24
VNet2	10.10.0.0/16	Subnet2	10.10.1.0/24
VNet3	172.16.0.0/16	Subnet3	172.16.1.0/24

The subscription also contains the virtual machines in the following table

Name	Network	Subnet	IP address
VM1	VNet1	Subnet1	10.1.1.4
VM2	VNet2	Subnet2	10.10.1.4
VM3	VNet3	Subnet3	172.16.1.4

The firewalls on all the virtual machines are configured to allow all ICMP traffic

You add the peerings in the following table.

Virtual Network	Peering Network
VNet1	VNet3
VNet2	VNet3

VNet3

VNet1

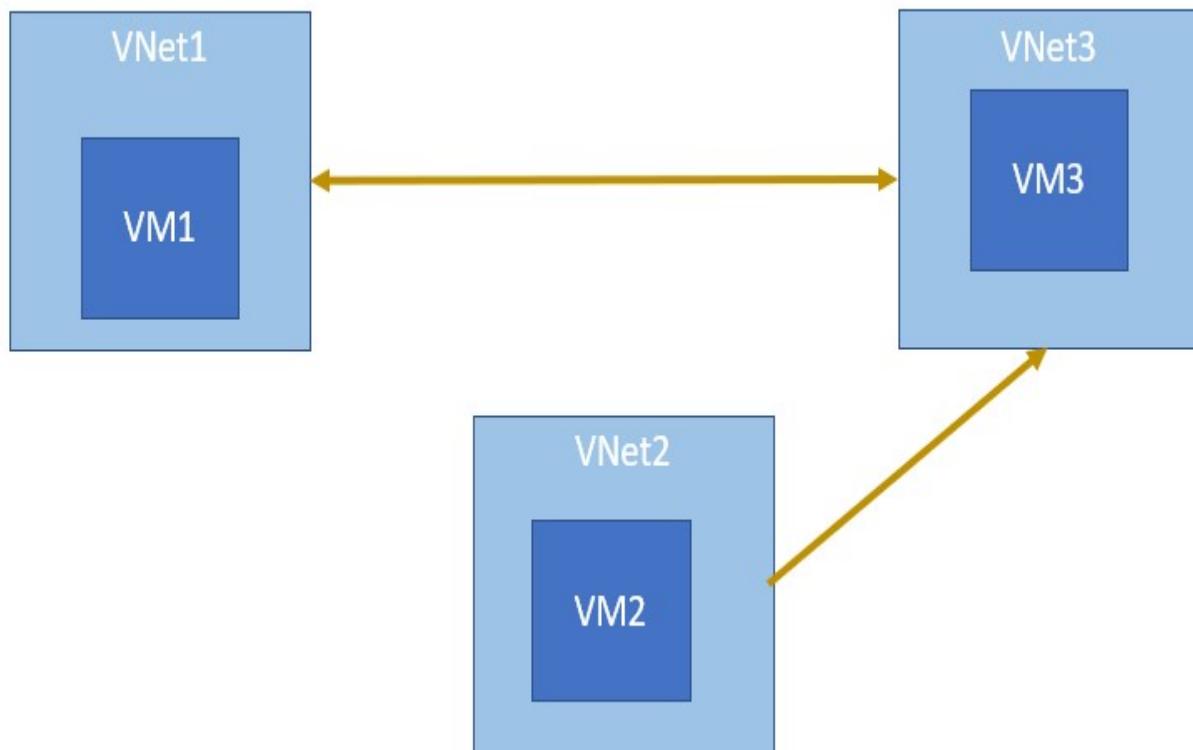
VM2 can ping VM3

A. Yes

B. No **Explanation:**

Answer – B

So, if you look at the overall picture for the VNET peerings , below is the diagram that we have



In order for peering to work, you have to create peerings in both directions , so this will not work.

For more information on VNET peering, please visit the below URL

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

[Ask our Experts](#)Rate this Question?  [View Queries](#)

open ▾

**Question 45****Unattempted****Domain :Configure and Manage Virtual Networks**

Your company has an Azure account and a subscription. The subscription contains the virtual networks in the following table

Name	Address Space	Subnet name	Subnet address range
VNet1	10.1.0.0/16	Subnet1	10.1.1.0/24
VNet2	10.10.0.0/16	Subnet2	10.10.1.0/24
VNet3	172.16.0.0/16	Subnet3	172.16.1.0/24

The subscription also contains the virtual machines in the following table

Name	Network	Subnet	IP address
VM1	VNet1	Subnet1	10.1.1.4
VM2	VNet2	Subnet2	10.10.1.4
VM3	VNet3	Subnet3	172.16.1.4

The firewalls on all the virtual machines are configured to allow all ICMP traffic

You add the peerings in the following table.

Virtual Network	Peering Network
VNet1	VNet3
VNet2	VNet3
VNet3	VNet1

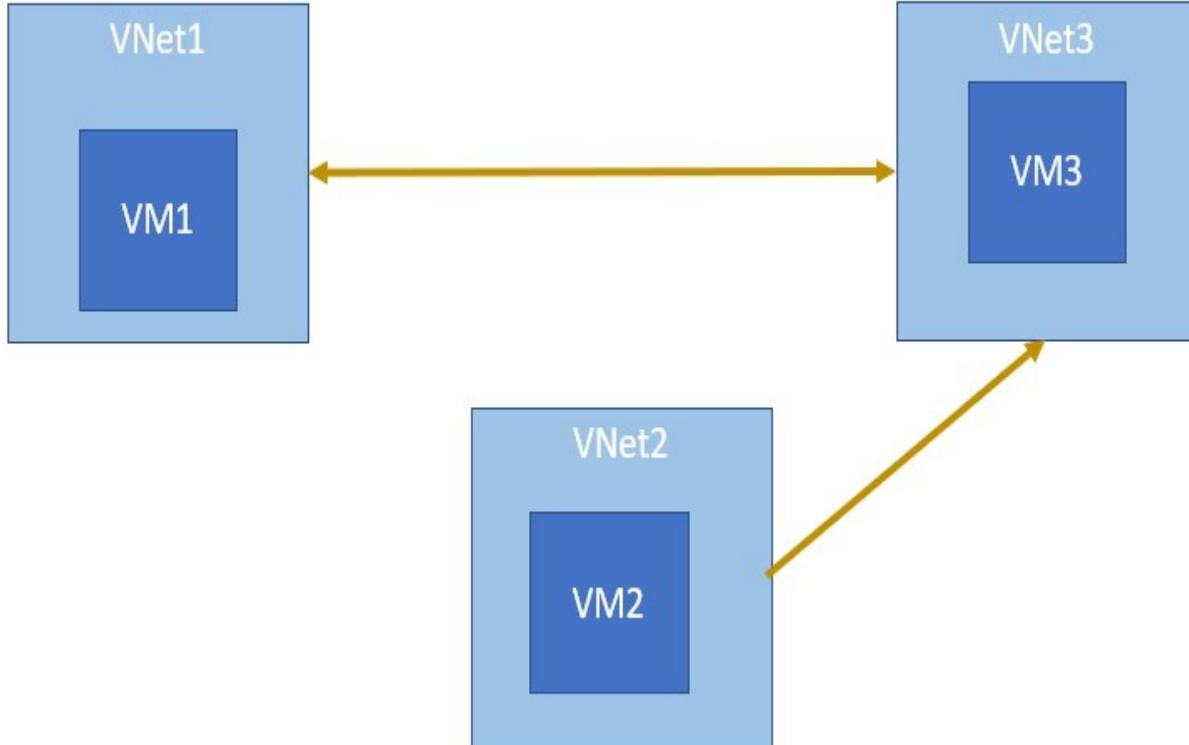
VM2 can ping VM1

- A. Yes
- B. No 

**Explanation:**

Answer – B

So, if you look at the overall picture for the VNET peerings , below is the diagram that we have



VNET1 and VNET2 don't have any peering connection , so this will not work.

For more information on VNET peering, please visit the below URL

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

---

Ask our Experts

Rate this Question?

---

**View Queries**

open ▾

**Question 46**

**Unattempted**

Domain :Managing Azure Subscriptions and Resources

A company has setup their Azure account. They have also setup different Azure AD groups and assigned the appropriate roles to the groups. There is a requirement to ensure that the Security department gets notified if any of the following actions are taken

If anybody creates a new role assignment

If anybody deletes an existing role assignment

Which of the following can help accomplish this requirement?

- A. Diagnostic logs for the resource groups.
- B. Azure Advisor
- C. Activity logs in Azure Monitor 
- D. Azure Security Center

---

**Explanation:**

Answer – C

You can view the relevant activities in Azure Monitor. You can also create alerts based on Activity Log. The Microsoft documentation mentions the following

# View activity logs for RBAC changes to Azure resources

02/02/2019 • 3 minutes to read • Contributors 

Sometimes you need information about role-based access control (RBAC) changes to Azure resources, such as for auditing or troubleshooting purposes. Any time someone makes changes to role assignments or role definitions within your subscriptions, the changes get logged in [Azure Activity Log](#). You can view the activity logs to see all the RBAC changes for the past 90 days.

## Operations that are logged

Here are the RBAC-related operations that are logged in Activity Log:

- Create role assignment
- Delete role assignment
- Create or update custom role definition
- Delete custom role definition

The other services mentioned in the other options will not provide the facility to view the relevant RBAC changes.

For more information on Activity logs for RBAC changes, one can go to the following link

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

---

Ask our Experts

Rate this Question?  

---

**View Queries**

open ▾

---

**Question 47**

**Unattempted**

Domain :Implementing and Managing Storage

A company has the following storage accounts in place as part of their Azure subscription

Name	Storage Account Type

<b>whizlabstore1</b>	General Purpose V1
<b>whizlabstore2</b>	General Purpose V2
<b>whizlabstore3</b>	Blob Storage

Which of the following storage account/accounts could be used to store objects as part of the Archive tier?

- A. whizlabstore1 only
- B. whizlabstore2 only
- C. whizlabstore3 only
- D. whizlabstore1 and whizlabstore2 only
- E. whizlabstore1 and whizlabstore3 only
- F. whizlabstore2 and whizlabstore3 only 
- G. All storage accounts

#### Explanation:

Answer - F

As per the Microsoft documentation given below only the General Purpose V2 and Blob storage account types support the Archive access tier.

Storage account type	Supported services	Supported performance tiers	Supported access tiers	Replication options	Deployment model <sup>1</sup>	Encryption <sup>2</sup>
General-purpose V2	Blob, File, Queue, Table, and Disk	Standard, Premium <sup>5</sup>	Hot, Cool, Archive <sup>3</sup>	LRS, ZRS <sup>4</sup> , GRS, RA-GRS	Resource Manager	Encrypted
General-purpose V1	Blob, File, Queue, Table, and Disk	Standard, Premium <sup>5</sup>	N/A	LRS, GRS, RA-GRS	Resource Manager, Classic	Encrypted
Block blob storage	Blob (block blobs and append blobs only)	Premium	N/A	LRS	Resource Manager	Encrypted
FileStorage (preview)	Files only	Premium	N/A	LRS	Resource Manager	Encrypted
Blob storage	Blob (block blobs and append blobs only)	Standard	Hot, Cool, Archive <sup>3</sup>	LRS, GRS, RA-GRS	Resource Manager	Encrypted

As a result, all other options are incorrect

For more information on storage accounts, one can go to the following link

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

Ask our Experts

Rate this Question?  

**View Queries**

open ▾

**Question 48**

**Unattempted**

Domain :Implementing and Managing Storage

A company has a storage account named whizlabstore1 defined as part of their Azure subscription. It needs to be ensured that only IP addresses within the range of 15.16.7.0/24 have access to the storage account. Which of the following powershell command could be used for this purpose?

- A. **Add-AzStorageAccountNetworkRule** 
- B. **Set-AzStorageAccountNetwork**

**C. Update-AzStorage****D. Set-AzRmStorageAccountNetwork****Explanation:**

Answer - A

An example of this is given in the Microsoft documentation. The Add-AzStorageAccountNetworkRule is used to add an IP address or an IP address range to have access to the storage account.

**PowerShell**

1. Install the [Azure PowerShell](#) and [sign in](#).

2. List IP network rules.

```
PowerShell Copy  
  
(Get-AzStorageAccountNetworkRuleSet -ResourceGroupName "myresourcegroup" -AccountName "mystorageaccount").IP
```

3. Add a network rule for an individual IP address.

```
PowerShell Copy  
  
Add-AzStorageAccountNetworkRule -ResourceGroupName "myresourcegroup" -AccountName "mystorageaccount" -IPAddr
```

4. Add a network rule for an IP address range.

```
PowerShell Copy  
  
Add-AzStorageAccountNetworkRule -ResourceGroupName "myresourcegroup" -AccountName "mystorageaccount" -IPAddr
```

Since this is clearly given in the documentation, all other options are incorrect

For more information on network security for the storage account, one can go to the following

link

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

Ask our Experts

Rate this Question?  

**View Queries**

open 

**Question 49**

**Unattempted**

Domain :Deploying and Managing Virtual Machines

A team needs to deploy a set of Windows virtual machines to Azure. Below are the key requirements when it comes to the storage needs for the data disks attached to the virtual machines

Should have the ability to store at least 10TB of data

Have the ability to support a minimum IOPS of 10,000

Minimize storage cost

Which of the following would you choose as the disk type, if you were considering using managed disks for the virtual machines?

- A. Standard HDD
- B. Standard SSD
- C. Premium SSD 
- D. Primary SSD

---

**Explanation:**

Answer – C

Now even though Premium SSD is a costly option, you still need to use that disk type if you need to fulfil all the requirements. Premium SSD has the capability to support an IOPS up to 20,000. The Microsoft documentation mentions the aspects of the different types of disks

# Disk comparison

The following table provides a comparison of ultra solid-state-drives (SSD) (preview), premium SSD, standard SSD, and standard hard disk drives (HDD) for managed disks to help you decide what to use.

	<b>Ultra SSD (preview)</b>	<b>Premium SSD</b>	<b>Standard SSD</b>	<b>Standard HDD</b>
Disk type	SSD	SSD	SSD	HDD
Scenario	IO-intensive workloads such as SAP HANA, top tier databases (for example, SQL, Oracle), and other transaction-heavy workloads.	Production and performance sensitive workloads	Web servers, lightly used enterprise applications and dev/test	Backup, non-critical, infrequent access
Disk size	65,536 gibabyte (GiB) (Preview)	32,767 GiB	32,767 GiB	32,767 GiB
Max throughput	2,000 MiB/s (Preview)	900 MiB/s	750 MiB/s	500 MiB/s
Max IOPS	160,000 (Preview)	20,000	6,000	2,000

Since this is clearly given in the documentation, all other options are incorrect

For more information on disks types of Windows, one can go to the following link

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

[Ask our Experts](#)

Rate this Question?  

[View Queries](#)

open ▾

**Question 50**

**Unattempted**

Domain :Deploying and Managing Virtual Machines

A company has the following windows virtual machines deployed to their subscription in Azure

whizlabsvm1

whizlabsvm2

The Monitoring department needs to collect certain performance-based counters from the virtual machines. Which of the following could help accomplish this?

- A. Enable base collection of metrics
- B. Enable collection of boot diagnostics
- C. Enable collection of performance diagnostics
- D. Enable collection of guest OS diagnostics data 

#### Explanation:

Answer – D

If you enable collection of guest OS diagnostics data, you will have the ability to collect data on the performance counters on Windows based virtual machines. The Microsoft documentation mentions the following

- **Enable the collection of guest OS diagnostics data.** When you create a VM, you have the opportunity on the settings screen to enable guest OS diagnostics. When you do enable the collection of diagnostics data, the [IaaSDiagnostics extension for Linux](#) or the [IaaSDiagnostics extension for Windows](#) is added to the VM, which enables you to collect additional disk, CPU, and memory data.

Using the collected diagnostics data, you can configure autoscaling for your VMs. You can also configure logs to store the data and set up alerts to let you know when performance isn't quite right.

The other options are invalid, because they won't provide the ability to collect performance counters for Windows based virtual machines.

For more information on monitoring Windows machines, one can go to the following link

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

Ask our Experts

Rate this Question?  

**View Queries**

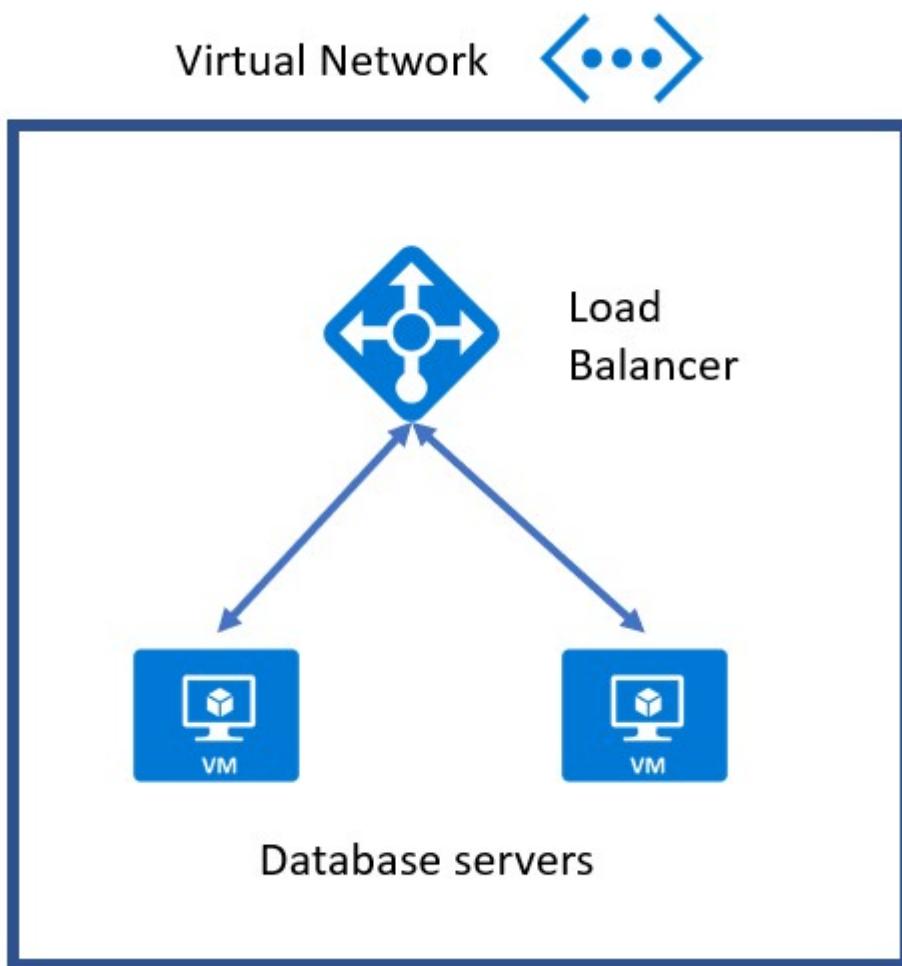
open ▾

**Question 51**

**Unattempted**

Domain :Configure and Manage Virtual Networks

A company needs to deploy the following architecture to Azure



The architecture would consist of a load balancer that should only accept requests via private IP addresses and should not flow via the internet. The Load balancer would direct requests to database servers hosted on Virtual machines.

Which of the following load balancer type should be implemented for this architecture?

- A. Public Load balancer
- B. Private Load balancer
- C. Internal Load balancer
- D. External Load balancer

#### Explanation:

Answer – B & C

An internal (or private) **load balancer** is used where **private** IPs are needed at the frontend only. Internal **load balancers** are used to **load** balance traffic inside a virtual network. A **load balancer** frontend can be accessed from an on-premises network in a hybrid scenario

Since we don't want requests to flow via the Internet, we should create an Internal load balancer. The Microsoft documentation mentions the following

## Internal Load Balancer

An internal Load Balancer directs traffic only to resources that are inside a virtual network or that use a VPN to access Azure infrastructure. In this respect, an internal Load Balancer differs from a public Load Balancer. Azure infrastructure restricts access to the load-balanced frontend IP addresses of a virtual network. Frontend IP addresses and virtual networks are never directly exposed to an internet endpoint. Internal line-of-business applications run in Azure and are accessed from within Azure or from on-premises resources.

An internal Load Balancer enables the following types of load balancing:

- **Within a virtual network:** Load balancing from VMs in the virtual network to a set of VMs that reside within the same virtual network.
- **For a cross-premises virtual network:** Load balancing from on-premises computers to a set of VMs that reside within the same virtual network.
- **For multi-tier applications:** Load balancing for internet-facing multi-tier applications where the backend tiers are not internet-facing. The backend tiers require traffic load-balancing from the internet-facing tier (see the next figure).
- **For line-of-business applications:** Load balancing for line-of-business applications that are hosted in Azure without additional load balancer hardware or software. This scenario includes on-premises servers that are in the set of computers whose traffic is load-balanced.

Option A is incorrect since this is created when requests need to flow via the Internet

Option D are incorrect terms when it comes to the load balancer.

For more information on the Azure Load balancer, one can go to the following link

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

---

Ask our Experts

Rate this Question?  

**View Queries**

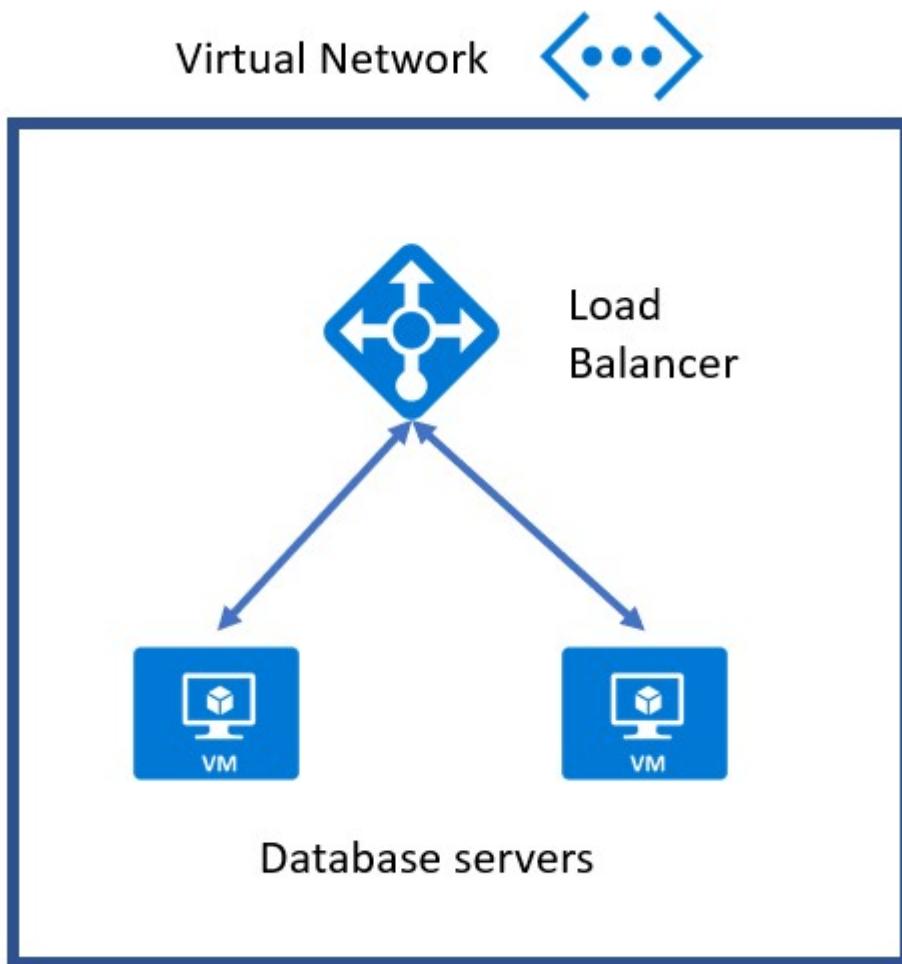
open ▾

**Question 52**

**Unattempted**

Domain :Configure and Manage Virtual Networks

A company needs to deploy the following architecture to Azure



The architecture would consist of a load balancer that should only accept requests via private IP addresses and should not flow via the internet. The Load balancer would direct requests to database servers hosted on Virtual machines.

You need to ensure that all requests for the Remote Desktop protocol for the virtual machine are accepted on a custom port number of 3400. Which of the following is the right PowerShell command to execute for this requirement?

- A. `New-AzLoadBalancerInboundNatRuleConfig` ✓
- B. `New-AzLoadBalancerProbeConfig`
- C. `New-AzLoadBalancerRuleConfig`
- D. `New-AzLoadBalancer`

#### Explanation:

Answer – A

For the requirement, we have to create a NAT rule. An example of this is also given in the Microsoft documentation

# Create the configuration rules, probe, and load balancer

After the front-end IP pool and the back-end address pool are created, specify the rules for the load balancer resource.

## Step 1: Create the configuration rules

The example creates the following four rule objects:

- An inbound NAT rule for the Remote Desktop Protocol (RDP): Redirects all incoming traffic on port 3441 to port 3389.
- A second inbound NAT rule for RDP: Redirects all incoming traffic on port 3442 to port 3389.
- A health probe rule: Checks the health status of the HealthProbe.aspx path.
- A load balancer rule: Load-balances all incoming traffic on public port 80 to local port 80 in the back-end address pool.



```
Azure PowerShell
Copy Try It

$inboundNATRule1= New-AzLoadBalancerInboundNatRuleConfig -Name "RDP1" -FrontendIpConfiguration $frontendIP -Proto
$inboundNATRule2= New-AzLoadBalancerInboundNatRuleConfig -Name "RDP2" -FrontendIpConfiguration $frontendIP -Proto
$healthProbe = New-AzLoadBalancerProbeConfig -Name "HealthProbe" -RequestPath "HealthProbe.aspx" -Protocol http -
$lbrule = New-AzLoadBalancerRuleConfig -Name "HTTP" -FrontendIpConfiguration $frontendIP -BackendAddressPool $beA
```

Since this is clearly given in the Microsoft documentation, all other options are incorrect

For more information on configuring the Azure Load balancer via powershell, one can go to the following link

<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-get-started-ilb-arm-ps>

Ask our Experts

Rate this Question?  

View Queries

open ▾

Question 53

Unattempted

Domain :Manage Identities

Your company currently has an on-premise Active directory setup with a domain of whizlabs.com. The company has also set up an Azure AD tenant of whizlabs.onmicrosoft.com. They now want to use Azure AD to synchronize the users from the on-premise Active Directory to Azure AD.

You are requested to recommend a pre-requisite action from the following options which could be performed at Azure AD.

- A. Run the IdFix tool
- B. Ensure that the forest functional level is Windows 2003 or greater
- C. Ensure to add and verify the domain 
- D. Setup the Azure AD connect server

---

#### Explanation:

Answer – C

In order to ensure that users from the whizlabs.com domain are synchronized to Azure AD; you have to ensure first that the domain is set up in Azure. The Microsoft documentation mentions the following

## Before you install Azure AD Connect

Before you install Azure AD Connect, there are a few things that you need.

### Azure AD

- An Azure AD tenant. You get one with an [Azure free trial](#). You can use one of the following portals to manage Azure AD Connect:
  - The [Azure portal](#).
  - The [Office portal](#).
- [Add and verify the domain](#) you plan to use in Azure AD. For example, if you plan to use contoso.com for your users then make sure this domain has been verified and you are not only using the contoso.onmicrosoft.com default domain.
- An Azure AD tenant allows by default 50k objects. When you verify your domain, the limit is increased to 300k objects. If you need even more objects in Azure AD, then you need to open a support case to have the limit increased even further. If you need more than 500k objects, then you need a license, such as Office 365, Azure AD Basic, Azure AD Premium, or Enterprise Mobility and Security.

All other options are incorrect because these are all settings that need to be carried out on the on-premise server.

For more information on the pre-requisites for Azure AD connect, one can go to the following link

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-prerequisites>

---

Ask our Experts

Rate this Question?  

---

**View Queries**

open ▾

**Question 54**

**Unattempted**

Domain :Managing Azure Subscriptions and Resources

A company has just setup an Azure account and subscription. The Senior management want to keep a control on costs during the initial deployment of resources. Which of the following can be used to keep a tabs on overall costs incurred for hosting resources in Azure?

- A. Use the pricing calculator to calculate the costs beforehand.
- B. Create a budget and then an action group to notify when thresholds are breached. 
- C. Use the Azure Advisor to notify when costs are being breached.
- D. Use resource tags for all resources

---

**Explanation:**

Answer – B

You can create a budget in Azure cost management and also create an action group to notify when costs are being breached.

The Microsoft documentation mentions the following

# Tutorial: Create and manage Azure budgets

04/09/2019 • 5 minutes to read • Contributors 

Budgets in Cost Management help you plan for and drive organizational accountability. With budgets, you can account for the Azure services you consume or subscribe to during a specific period. They help you inform others about their spending to proactively manage costs, and to monitor how spending progresses over time. When the budget thresholds you've created are exceeded, only notifications are triggered. None of your resources are affected and your consumption isn't stopped. You can use budgets to compare and track spending as you analyze costs.

Monthly budgets are evaluated against spending every four hours. However, data and notifications for consumed resources are available within eight hours.

Budgets reset automatically at the end of a period (monthly, quarterly, or annually) for the same budget amount when you select an expiration date in the future. Because they reset with the same budget amount, you need to create separate budgets when budgeted currency amounts differ for future periods.

Option A is partially correct but is only viable before creating resources in Azure.

Option C is incorrect since this is ideal when you want to have recommendations in place in Azure

Option D is incorrect since this is ideal from a billing perspective and segregation on costs

For more information on a tutorial on creating budgets, one can go to the following link

<https://docs.microsoft.com/en-us/azure/cost-management/tutorial-acm-create-budgets>

[Ask our Experts](#)

Rate this Question?  

[View Queries](#)

open ▾

**Question 55**

**Incorrect**

Domain :Deploying and Managing Virtual Machines

A team has a set of Linux Virtual Machines defined in Azure. The size of one of the Virtual machines needs to be changed. You have to write an Azure CLI script for this. Which of the following should ideally be part of the first steps in the script?

- A. Deallocate the virtual machine first

- ✓ B. Restart the virtual machine first ✗
- C. Check the list of VM sizes on the hardware cluster ✓
- D. Detach the primary network interface

---

**Explanation:**

Answer – C

First you have to check the availability of the required VM size on the hardware cluster. The Microsoft documentation mentions the following

# Resize a Linux virtual machine using Azure CLI

02/10/2017 • 2 minutes to read • Contributors  all

After you provision a virtual machine (VM), you can scale the VM up or down by changing the [VM size](#). In some cases, you must deallocate the VM first. You need to deallocate the VM if the desired size is not available on the hardware cluster that is hosting the VM. This article details how to resize a Linux VM with the Azure CLI.

## Resize a VM

To resize a VM, you need the latest [Azure CLI](#) installed and logged in to an Azure account using [az login](#).



1. View the list of available VM sizes on the hardware cluster where the VM is hosted with `az vm list-vm-resize-options`. The following example lists VM sizes for the VM named `myVM` in the resource group `myResourceGroup` region:

```
Azure CLI Copy
az vm list-vm-resize-options --resource-group myResourceGroup --name myVM --output table
```

2. If the desired VM size is listed, resize the VM with [az vm resize](#). The following example resizes the VM named `myVM` to the `Standard_DS3_v2` size:

```
Azure CLI Copy
az vm resize --resource-group myResourceGroup --name myVM --size Standard_DS3_v2
```

Since this is clearly given in the Microsoft documentation, all other options are incorrect

For more information on a tutorial to resize a Linux VM, one can go to the following link

<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/change-vm-size>

Ask our Experts

Rate this Question?  

[View Queries](#)

open ▾

[Finish Review](#)

Certification	Company	Support	
Cloud Certification	Become Our Instructor	Contact Us	 <a href="#">Join us on Slack!</a>
Java Certification	Support	Help Topics	Join our open <b>Slack community</b> and get your queries answered instantly! Our experts are online to answer your questions!
PM Certification	Discussions		
Big Data Certification	Blog		<b>Follow us</b>
	Business		  

---

© Copyright 2021. Whizlabs Software Pvt. Ltd. All Right Reserved.