

AZ-104

Real Exam Questions & Answers

Latest Exam Questions
All Topics Covered-2022
Added New Que's

Microsoft
CERTIFIED

AZURE
ADMINISTRATOR

ASSOCIATE



Subscribe

Question 241

CertyIQ

DRAG DROP

You have an Azure subscription that contains two virtual networks named VNet1 and VNet2. Virtual machines connect to the virtual networks.

The virtual networks have the address spaces and the subnets configured as shown in the following table.

Virtual network	Address space	Subnet	Peering
VNet1	10.1.0.0/16	10.1.0.0/24 10.1.1.0/26	VNet2
VNet2	10.2.0.0/16	10.2.0.0/24	VNet1

You need to add the address space of 10.33.0.0/16 to VNet1. The solution must ensure that the hosts on VNet1 and VNet2 can communicate.

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

Select and Place:

Actions

Answer Area

Remove VNet1.

Add the 10.33.0.0/16 address space to VNet1.

Create a new virtual network named VNet1.

On the peering connection in VNet2, allow gateway transit.

Recreate peering between VNet1 and VNet2.

On the peering connection in VNet1, allow gateway transit.

Remove peering between VNet1 and VNet2.



Correct Answer:

Actions

Answer Area

Remove VNet1.

Add the 10.33.0.0/16 address space to VNet1.

Create a new virtual network named VNet1.

On the peering connection in VNet2, allow gateway transit.

Recreate peering between VNet1 and VNet2.

On the peering connection in VNet1, allow gateway transit.

Remove peering between VNet1 and VNet2.

Remove peering between VNet1 and VNet2.

Add the 10.33.0.0/16 address space to VNet1.

Recreate peering between VNet1 and VNet2.



Explanation:

Step 1: Remove peering between Vnet1 and VNet2.

You can't add address ranges to, or delete address ranges from a virtual network's address space once a virtual network is peered with another virtual network. To add or remove address ranges, delete the peering, add or remove the address ranges, then re-create the peering.

Step 2: Add the 10.44.0.0/16 address space to VNet1.

Step 3: Recreate peering between VNet1 and VNet2

Reference:

Question 242

CertyIQ

You have an Azure web app named webapp1.

You have a virtual network named VNET1 and an Azure virtual machine named VM1 that hosts a MySQL database. VM1 connects to VNET1.

You need to ensure that webapp1 can access the data hosted on VM1.

What should you do?

A. Deploy an internal load balancer

B. Peer VNET1 to another virtual network

C. Connect webapp1 to VNET1

D. Deploy an Azure Application Gateway

Explanation:

Correct Answer: D

Question 243

CertyIQ

You create an Azure VM named VM1 that runs Windows Server 2019.

VM1 is configured as shown in the exhibit. (Click the Exhibit tab.)

VM1
Virtual machine

Security

Extensions

Continuous delivery (Preview)

Availability set

Configuration

Identity

Properties

Locks

Export template

Operations

Auto-shutdown

Backup

Disaster recovery

Update management

Inventory

Change tracking

Configuration management ...

Policies

Run command

Monitoring

Insights (preview)

Alerts

Metrics

Diagnostics settings

Connect

Start

Restart

Stop

Capture

Delete

Refresh

Resource group (change) : [RG1](#)
Status : Stopped (deallocated)
Location : West Europe
Subscription (change) : [Azure Pass – Sponsorship](#)
Subscription ID : 90f9d59c-629e-4346-b577-8b7e1ef1316a

Computer name : (start VM to view)
Operating system : Windows
Size : Standard DS2 v2 (2 vcpus, 7 GiB memory)
Ephemeral OS disk : N/A
Public IP address : [VM1-ip](#)
Private IP address : 10.0.0.4
Virtual network/subnet : [VNET1/default](#)
DNS name : [Configure](#)

Tags (change) : [Click here to add tags](#)

Show data for last:

1 hour

6 hours

12 hours

1 day

7 days

30 days

CPU (average)

Network (total)

You need to enable Desired State Configuration for VM1.
What should you do first?

- A. Connect to VM1.
- B. Start VM1.
- C. Capture a snapshot of VM1.
- D. Configure a DNS name for VM1.

Explanation:

Correct Answer: B

Status is Stopped (Deallocated).

The DSC extension for Windows requires that the target virtual machine is able to communicate with Azure.

The VM needs to be started.

Reference:

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

Question 244

CertyIQ

You have five Azure virtual machines that run Windows Server 2016. The virtual machines are configured as web servers.

You have an Azure load balancer named LB1 that provides load balancing services for the virtual machines.

You need to ensure that visitors are serviced by the same web server for each request.

What should you configure?

A. Floating IP (direct server return) to Disabled

B. Session persistence to None

C. Floating IP (direct server return) to Enabled

D. Session persistence to Client IP

Explanation:

Correct Answer: D

With Sticky Sessions when a client starts a session on one of your web servers, session stays on that specific server. To configure An Azure Load-Balancer For Sticky Sessions set Session persistence to Client IP or to Client IP and protocol.

On the following image you can see sticky session configuration:

Note:

Client IP and protocol specifies that successive requests from the same client IP address and protocol combination will be handled by the same virtual machine.

Client IP specifies that successive requests from the same client IP address will be handled by the same virtual machine.

Reference:

<https://cloudopszone.com/configure-azure-load-balancer-for-sticky-sessions/>

Question 245

CertyIQ

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

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

You have an Azure subscription that contains the following resources:

A virtual network that has a subnet named Subnet1

Two network security groups (NSGs) named NSG-VM1 and NSG-Subnet1

A virtual machine named VM1 that has the required Windows Server configurations to allow Remote Desktop connections

NSG-Subnet1 has the default inbound security rules only.

NSG-VM1 has the default inbound security rules and the following custom inbound security rule:

Priority: 100

Source: Any

Source port range: *

Destination: *

Destination port range: 3389

Protocol: UDP

Action: Allow

VM1 has a public IP address and is connected to Subnet1. NSG-VM1 is associated to the network interface of VM1. NSG-Subnet1 is associated to Subnet1.

You need to be able to establish Remote Desktop connections from the internet to VM1.

Solution: You add an inbound security rule to NSG-Subnet1 that allows connections from the Any source to the *destination for port range 3389 and uses the TCP protocol. You remove NSG-VM1 from the network interface of VM1.

Does this meet the goal?

A. Yes

B. No

Explanation:

Correct Answer: B

The default port for RDP is TCP port 3389. A rule to permit RDP traffic must be created automatically when you create your VM.

Note on NSG-Subnet1: Azure routes network traffic between all subnets in a virtual network, by default.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-rdp-connection>

Question 246

CertyIQ

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

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

You have an Azure subscription that contains the following resources:

A virtual network that has a subnet named Subnet1

Two network security groups (NSGs) named NSG-VM1 and NSG-Subnet1

A virtual machine named VM1 that has the required Windows Server configurations to allow Remote Desktop connections

NSG-Subnet1 has the default inbound security rules only.

NSG-VM1 has the default inbound security rules and the following custom inbound security rule:

Priority: 100

Source: Any

Source port range: *

Destination: *

Destination port range: 3389

Protocol: UDP

Action: Allow

VM1 has a public IP address and is connected to Subnet1. NSG-VM1 is associated to the network interface of VM1. NSG-Subnet1 is associated to Subnet1.

You need to be able to establish Remote Desktop connections from the internet to VM1.

Solution: You add an inbound security rule to NSG-Subnet1 that allows connections from the internet source to the VirtualNetwork destination for port range 3389 and uses the UDP protocol.

Does this meet the goal?

A. Yes

B. No

Explanation:

Correct Answer: B

The default port for RDP is TCP port 3389. A rule to permit RDP traffic must be created automatically when you create your VM.

Note on NSG-Subnet1: Azure routes network traffic between all subnets in a virtual network, by default.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-rdp-connection>

Question 247

CertyIQ

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

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

You have an Azure subscription that contains the following resources:

A virtual network that has a subnet named Subnet1

Two network security groups (NSGs) named NSG-VM1 and NSG-Subnet1

A virtual machine named VM1 that has the required Windows Server configurations to allow Remote Desktop connections

NSG-Subnet1 has the default inbound security rules only.

NSG-VM1 has the default inbound security rules and the following custom inbound security rule:

Priority: 100

Source: Any

Source port range: *

Destination: *

Destination port range: 3389

Protocol: UDP

Action: Allow

VM1 has a public IP address and is connected to Subnet1. NSG-VM1 is associated to the network interface of VM1. NSG-Subnet1 is associated to Subnet1.

You need to be able to establish Remote Desktop connections from the internet to VM1.

Solution: You add an inbound security rule to **NSG-Subnet1 and NSG-VM1** that allows connections from the

internet source to the VirtualNetwork destination for port range 3389 and uses the TCP protocol.
Does this meet the goal?

A. Yes

B. No

Explanation:

Correct Answer: A

The default port for RDP is TCP port 3389. A rule to permit RDP traffic must be created automatically when you create your VM.

Note on NSG-Subnet1: Azure routes network traffic between all subnets in a virtual network, by default.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-rdp-connection>

Question 248

CertyIQ

You have a virtual network named VNet1 that has the configuration shown in the following exhibit.

```
Name : VNet1
ResourceGroupName : Production
Location : westus
Id : /subscriptions/14d26092-8e42-4ea7-b770-9dcef70fb1ea/resourceGroups/Production/providers/Microsoft.Network/virtualNetworks/VNet1
Etag : W/"76f7edd6-d022-455b-aeae-376059318e5d"
ResourceGuid : 562696cc-b2ba-4cc5-9619-0a735d6c34c7
ProvisioningState : Succeeded
Tags :
AddressSpace : {
  "AddressPrefixes": [
    "10.2.0.0/16"
  ]
}
DhcpOptions : {}
Subnets : [
  {
    "Name": "default",
    "Etag": "W/\ "76f7edd6-d022-455b-aeae-376059318e5d\\"",
    "Id": "/subscriptions/14d26092-8e42-4ea7-b770-9dcef70fb1ea/resourceGroups/Production/providers/Microsoft.Network/virtualNetworks/VNet1/subnets/default",
    "AddressPrefix": "10.2.0.0/24",
    "IpConfigurations": [],
    "ResourceNavigationLinks": [],
    "ServiceEndpoints": [],
    "ProvisioningState": "Succeeded"
  }
]
VirtualNetworkPeerings : []
EnableDDoSProtection : false
EnableVmProtection : false
```

Use the drop-down menus to select the answer choice that completes each statement based on the

2022 Latest AZ-104/DP-900/SC-900/AZ-900 Exam Real Que's and other exam series on [CertyIQ](#) (YouTube Channel)

information presented in the graphic.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

Before a virtual machine on VNet1 can receive an IP address from 192.168.1.0/24, you must first

	▼
add a network interface	
add a subnet	
add an address space	
delete a subnet	
delete an address space	

Before a virtual machine on VNet1 can receive an IP address from 10.2.1.0/24, you must first

	▼
add a network interface	
add a subnet	
add an address space	
delete a subnet	
delete an address space	

Correct Answer:

Answer Area

Before a virtual machine on VNet1 can receive an IP address from 192.168.1.0/24, you must first

	▼
add a network interface	
add a subnet	
add an address space	
delete a subnet	
delete an address space	

Before a virtual machine on VNet1 can receive an IP address from 10.2.1.0/24, you must first

	▼
add a network interface	
add a subnet	
add an address space	
delete a subnet	
delete an address space	

Explanation:

Box 1: add an address space

Your IaaS virtual machines (VMs) and PaaS role instances in a virtual network automatically receive a private IP address from a range that you specify, based on the address space of the subnet they are connected to. We need to add the 192.168.1.0/24 address space.

Box 2: add a network interface

The 10.2.1.0/24 network exists. We need to add a network interface.

Reference:

<https://docs.microsoft.com/en-us/office365/enterprise/designing-networking-for-microsoft-azure-iaas>

Question 249

CertyIQ

You have an Azure subscription that contains a virtual network named VNET1. VNET1 contains the subnets shown in the following table.

Name	Connected virtual machines
Subnet1	VM1, VM2
Subnet2	VM3, VM4
Subnet3	VM5, VM6

Each virtual machine uses a static IP address.

You need to create network security groups (NSGs) to meet following requirements:

Allow web requests from the internet to VM3, VM4, VM5, and VM6.

Allow all connections between VM1 and VM2.

Allow Remote Desktop connections to VM1.

Prevent all other network traffic to VNET1.

What is the minimum number of NSGs you should create?

A. 1

B. 3

C. 4

D. 12

Explanation:

Correct Answer: C

Each network security group also contains default security rules.

Note: A network security group (NSG) contains a list of security rules that allow or deny network traffic to resources connected to Azure Virtual Networks (VNet). NSGs can be associated to subnets, individual VMs (classic), or individual network interfaces (NIC) attached to VMs (Resource Manager).

Reference:

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

Question 250

CertyIQ

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

Name	Location
RG1	West US
RG2	East US

RG1 contains the resources shown in the following table.

Name	Type	Location
storage1	Storage account	West US
VNet1	Virtual network	West US
NIC1	Network interface	West US
Disk1	Disk	West US
VM1	Virtual machine	West US

VM1 is running and connects to NIC1 and Disk1. NIC1 connects to VNET1.

RG2 contains a public IP address named IP2 that is in the East US location. IP2 is not assigned to a virtual machine.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
You can move storage1 to RG2.	<input type="radio"/>	<input type="radio"/>
You can move NIC1 to RG2.	<input type="radio"/>	<input type="radio"/>
If you move IP2 to RG1, the location of IP2 will change.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
You can move storage1 to RG2.	<input checked="" type="radio"/>	<input type="radio"/>
You can move NIC1 to RG2.	<input type="radio"/>	<input checked="" type="radio"/>
If you move IP2 to RG1, the location of IP2 will change.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Box 1: Yes

You can move storage

Box 2: No

You can't move to a new resource group a NIC that is attached to a virtual machine.

Box 3: No

Azure Public IPs are region specific and can't be moved from one region to another.

Reference:

Question 251

CertyIQ

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

Name	Type	Resource group
VNET1	Virtual network	RG1
VM1	Virtual machine	RG1

The Not allowed resource types Azure policy is assigned to RG1 and uses the following parameters:

Microsoft.Network/virtualNetworks

Microsoft.Compute/virtualMachines

In RG1, you need to create a new virtual machine named VM2, and then connect VM2 to VNET1.

What should you do first?

A. Remove Microsoft.Compute/virtualMachines from the policy.

B. Create an Azure Resource Manager template

C. Add a subnet to VNET1.

D. Remove Microsoft.Network/virtualNetworks from the policy.

Explanation:

Correct Answer: A

The Not allowed resource types Azure policy prohibits the deployment of specified resource types. You specify an array of the resource types to block.

Virtual Networks and Virtual Machines are prohibited.

Reference:

<https://docs.microsoft.com/en-us/azure/governance/policy/samples/not-allowed-resource-types>

Question 252

CertyIQ

Your company has an Azure subscription named Subscription1.

The company also has two on-premises servers named Server1 and Server2 that run Windows Server 2016.

Server1 is configured as a DNS server that has a primary DNS zone named adatum.com. Adatum.com contains 1,000 DNS records.

You manage Server1 and Subscription1 from Server2. Server2 has the following tools installed:

The DNS Manager console

Azure PowerShell

Azure CLI 2.0

You need to move the adatum.com zone to an Azure DNS zone in Subscription1. The solution must minimize administrative effort.

What should you use?

A. Azure CLI

B. Azure PowerShell

C. the Azure portal

D. the DNS Manager console

Explanation:

Step 1: Installing the DNS migration script

Open an elevated PowerShell window (Administrative mode) and run following command

```
install-script PrivateDnsMigrationScript
```

Step 2: Running the script

Execute following command to run the script

```
PrivateDnsMigrationScript.ps1
```

Reference:

<https://docs.microsoft.com/en-us/azure/dns/private-dns-migration-guide>

Question 253

CertyIQ

You have a public load balancer that balances ports 80 and 443 across three virtual machines. You need to direct all the Remote Desktop Protocol (RDP) connections to VM3 only. What should you configure?

A. an inbound NAT rule

B. a new public load balancer for VM3

C. a frontend IP configuration

D. a load balancing rule

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/load-balancer/tutorial-load-balancer-port-forwarding-portal>

<https://pixelrobots.co.uk/2017/08/azure-load-balancer-for-rds/>

Question 254

CertyIQ

You have an Azure subscription named Subscription1 that contains the virtual networks in the following table. Subscription1 contains the virtual machines in the following table.

Name	Subnet	Availability set
VM1	Subnet11	AS1
VM2	Subnet11	AS1
VM3	Subnet11	<i>Not applicable</i>
VM4	Subnet11	<i>Not applicable</i>
VM5	Subnet12	<i>Not applicable</i>
VM6	Subnet12	<i>Not applicable</i>

In Subscription1, you create a load balancer that has the following configurations:

Name: LB1

SKU: Basic

Type: Internal

Subnet: Subnet12

Virtual network: VNET1

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
LB1 can balance the traffic between VM1 and VM2.	<input type="radio"/>	<input type="radio"/>
LB1 can balance the traffic between VM3 and VM4.	<input type="radio"/>	<input type="radio"/>
LB1 can balance the traffic between VM5 and VM6.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
LB1 can balance the traffic between VM1 and VM2.	<input checked="" type="radio"/>	<input type="radio"/>
LB1 can balance the traffic between VM3 and VM4.	<input type="radio"/>	<input checked="" type="radio"/>
LB1 can balance the traffic between VM5 and VM6.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Reference:

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

Question 255

HOTSPOT

You have an Azure virtual machine that runs Windows Server 2019 and has the following configurations:

Name: VM1

Location: West US

Connected to: VNET1

Private IP address: 10.1.0.4

Public IP addresses: 52.186.85.63

DNS suffix in Windows Server: Adatum.com

You create the Azure DNS zones shown in the following table.

Name	Type	Location
Adatum.pri	Private	West Europe
Contoso.pri	Private	Central US
Adatum.com	Public	West Europe
Contoso.com	Public	North Europe

You need to identify which DNS zones you can link to VNET1 and the DNS zones to which VM1 can automatically register.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

DNS zones that you can link to VNET1:

▼

Adatum.com only

Adatum.pri and adatum.com only

The private zones only

The public zones only

DNS zones to which VM1 can automatically register:

▼

Adatum.com only

Adatum.pri and adatum.com only

The private zones only

The public zones only

Correct Answer:

Answer Area

DNS zones that you can link to VNET1:

▼

Adatum.com only

Adatum.pri and adatum.com only

The private zones only

The public zones only

DNS zones to which VM1 can automatically register:

▼

Adatum.com only

Adatum.pri and adatum.com only

The private zones only

The public zones only

Explanation:

Reference:

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

Question 256

CertyIQ

DRAG DROP

You have an on-premises network that you plan to connect to Azure by using a site-to-site VPN.

In Azure, you have an Azure virtual network named VNet1 that uses an address space of 10.0.0.0/16. VNet1 contains a subnet named Subnet1 that uses an address space of 10.0.0.0/24.

You need to create a site-to-site VPN to Azure.

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

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

Select and Place:

Actions

Answer Area

Create a local gateway.

Create a VPN gateway.

Create a gateway subnet.

Create a custom DNS server.

Create a VPN connection.

Create an Azure Content Delivery Network (CDN) profile.



Correct Answer:

Actions

Answer Area

Create a local gateway.

Create a VPN gateway.

Create a gateway subnet.

Create a custom DNS server.

Create a VPN connection.

Create an Azure Content Delivery Network (CDN) profile.

Create a gateway subnet.

Create a VPN gateway.

Create a local gateway.

Create a VPN connection.



Question 257

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

Name	Type	Details
VNet1	Virtual network	<i>Not applicable</i>
Subnet1	Subnet	Hosted on VNet1
VM1	Virtual machine	On Subnet1
VM2	Virtual machine	On Subnet1

VM1 and VM2 are deployed from the same template and host line-of-business applications. You configure the network security group (NSG) shown in the exhibit. (Click the Exhibit tab.)

→ Move Delete Refresh

Resource group (change) : RG1lod9053488
 Location : East US
 Subscription (change) : Microsoft AZ
 Subscription ID : ac344a74-f85a-4b2e-8057-642088faaf20

Custom security rules : 1 inbound, 1 outbound
 Associated with : 0 subnets, 0 network interfaces

Tags (change) : [Click here to add tags](#)

Inbound security rules

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	Port_80	80	TCP	Internet	Any	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Allow AzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Outbound security rules

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	DenyWebSites	80	TCP	Any	Internet	Deny
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

You need to prevent users of VM1 and VM2 from accessing websites on the Internet over TCP port 80. What should you do?

- A. Disassociate the NSG from a network interface
- B. Change the Port_80 inbound security rule.
- C. Associate the NSG to Subnet1.
- D. Change the DenyWebSites outbound security rule.

Explanation:

Correct Answer: C

You can associate or dissociate a network security group from a network interface or subnet.

The NSG has the appropriate rule to block users from accessing the Internet. We just need to associate it with

Subnet1.

Reference:

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

Question 258

CertyIQ

You have two subscriptions named Subscription1 and Subscription2. Each subscription is associated to a different Azure AD tenant.

Subscription1 contains a virtual network named VNet1. VNet1 contains an Azure virtual machine named VM1 and has an IP address space of 10.0.0.0/16.

Subscription2 contains a virtual network named VNet2. VNet2 contains an Azure virtual machine named VM2 and has an IP address space of 10.10.0.0/24.

You need to connect VNet1 to VNet2.

What should you do first?

A. Move VM1 to Subscription2.

B. Move VNet1 to Subscription2.

C. Modify the IP address space of VNet2.

D. Provision virtual network gateways.

Explanation:

The virtual networks can be in the same or different regions, and from the same or different subscriptions.

When connecting VNets from different subscriptions, the subscriptions do not need to be associated with the same Active Directory tenant.

Configuring a VNet-to-VNet connection is a good way to easily connect VNets. Connecting a virtual network to another virtual network using the VNet-to-VNet connection type (VNet2VNet) is similar to creating a Site-to-Site IPsec connection to an on-premises location. Both connectivity types use a VPN gateway to provide a secure tunnel using IPsec/IKE, and both function the same way when communicating.

The local network gateway for each VNet treats the other VNet as a local site. This lets you specify additional address space for the local network gateway in order to route traffic.

Reference:


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

Question 259

CertyIQ

You plan to create an Azure virtual machine named VM1 that will be configured as shown in the following Exhibit

Create a virtual machine

 Changing Basic options may reset selections you have made. Review all options prior to creating the virtual machine.

Basics Disks Networking Management Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image.

Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization.

Looking for classic VMs? [Create VM from Azure Marketplace](#)

PROJECT DETAILS

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

* Subscription ⓘ	MyDev-Test Subscription ▼
* Resource group ⓘ	RG1 ▼
	Create new

INSTANCE DETAILS

* Virtual machine name ⓘ	VM1
* Region ⓘ	(US) West US 2 ▼
Availability options ⓘ	No infrastructure redundancy required ▼
* Image ⓘ	Windows Server 2016 Datacenter ▼
	Browse all public and private images
Azure Spot instance ⓘ	<input type="radio"/> Yes <input checked="" type="radio"/> No
* Size ⓘ	Standard DS1 v2 1 vcpu, 3.5 GiB memory (ZAR 632.47/month) Change size

The planned disk configurations for VM1 are shown in the following exhibit.

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

Disk options

* OS disk type ⓘ

Standard HDD

The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.

Enable Ultra Disk compatibility (Preview) ⓘ ☐ Yes ☒ No

Ultra Disks are only available when using Managed Disks.

Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

ⓘ Adding unmanaged data disks is currently not supported at the time of VM creation. You can add them after the VM is created.

^ Advanced

Use managed disks ⓘ

☒ No ☐ Yes

* Storage account ⓘ

(new) rg1 disks799

[Create new](#)

You need to ensure that VM1 can be created in an Availability Zone.

Which two settings should you modify? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Use managed disks

B. OS disk type

C. Availability options

D. Size

E. Image

Explanation:

Correct Answer: AC

A: Your VMs should use managed disks if you want to move them to an Availability Zone by using Site Recovery.

C: When you create a VM for an Availability Zone, Under Settings > High availability, select one of the numbered zones from the Availability zone dropdown.

Settings

High availability

Availability zone ⓘ

2

Storage

Use managed disks ⓘ

No Yes

Network

* Virtual network ⓘ >

(new) myResourceGroup9-vnet

* Subnet ⓘ >

default (172.16.4.0/24)

* Public IP address ⓘ >

(new) myVM-ip

* Network security group (firewall) ⓘ >

(new) myVM-nsg

Reference:

<https://docs.microsoft.com/en-us/azure/site-recovery/move-azure-vms-avset-azone>

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

Question 260

CertyIQ

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

Name	Type	Resource group	Location
RG1	Resource group	<i>Not applicable</i>	Central US
RG2	Resource group	<i>Not applicable</i>	West US
RG3	Resource group	<i>Not applicable</i>	East US
VMSS1	Virtual machine scale set	RG1	West US

VMSS1 is set to VM (virtual machines) orchestration mode.

You need to deploy a new Azure virtual machine named VM1, and then add VM1 to VMSS1.

Which resource group and location should you use to deploy VM1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Resource group:

	▼
RG1 only	
RG2 only	
RG1 or RG2 only	
RG1, RG2, or RG3	

Location:

	▼
West US only	
Central US only	
Central US or West US only	
East US, Central US, or West US	

Correct Answer:

Answer Area

Resource group:

	▼
RG1 only	
RG2 only	
RG1 or RG2 only	
RG1, RG2, or RG3	

Location:

	▼
West US only	
Central US only	
Central US or West US only	
East US, Central US, or West US	

Explanation:

Box 1: RG1, RG2, or RG3

The resource group stores metadata about the resources. When you specify a location for the resource group, you're specifying where that metadata is stored.

Box 2: West US only

Note: Virtual machine scale sets will support 2 distinct orchestration modes:

ScaleSetVM – Virtual machine instances added to the scale set are based on the scale set configuration model. The virtual machine instance lifecycle - creation, update, deletion - is managed by the scale set.

VM (virtual machines) – Virtual machines created outside of the scale set can be explicitly added to the scaleset.

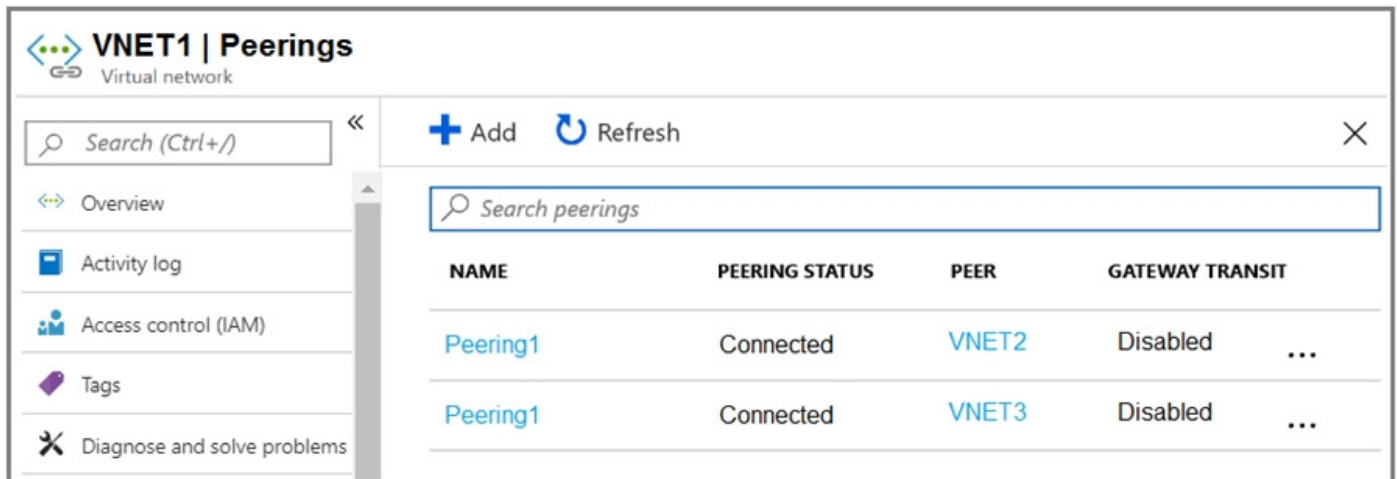
Reference:

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

Question 261

HOTSPOT

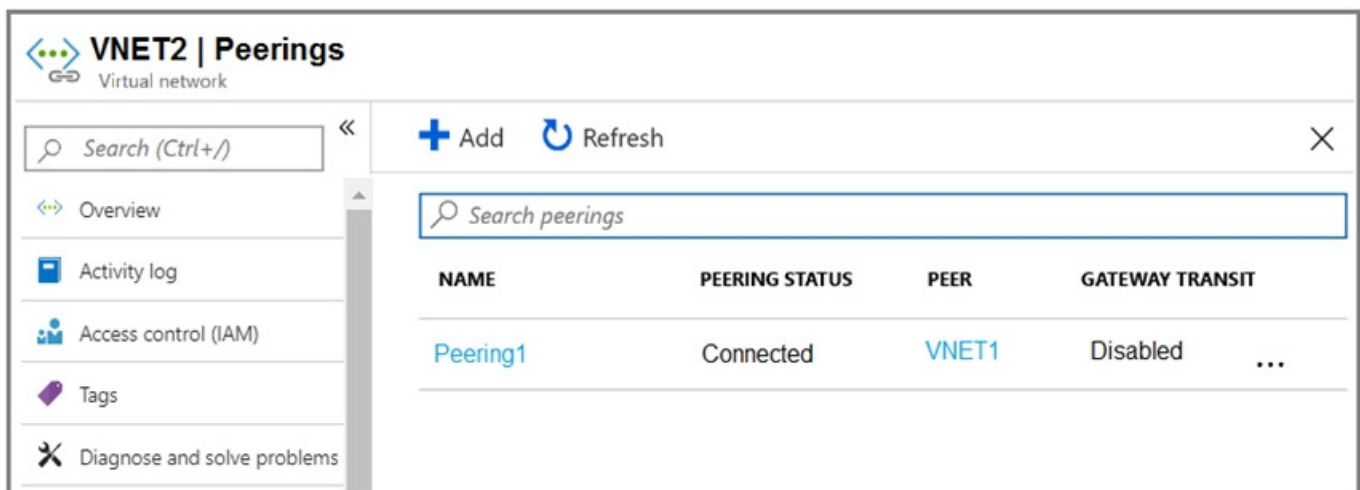
You have an Azure subscription that contains three virtual networks named VNET1, VNET2, and VNET3. Peering for VNET1 is configured as shown in the following exhibit.



The screenshot shows the 'VNET1 | Peerings' page in the Azure portal. The left sidebar contains navigation links: Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. The main area has a search bar and a table of peerings. The table has columns: NAME, PEERING STATUS, PEER, and GATEWAY TRANSIT. There are two entries, both named 'Peering1', both with a status of 'Connected'. The first entry's peer is 'VNET2' and the second is 'VNET3'. Both have 'Disabled' gateway transit.

NAME	PEERING STATUS	PEER	GATEWAY TRANSIT
Peering1	Connected	VNET2	Disabled ...
Peering1	Connected	VNET3	Disabled ...

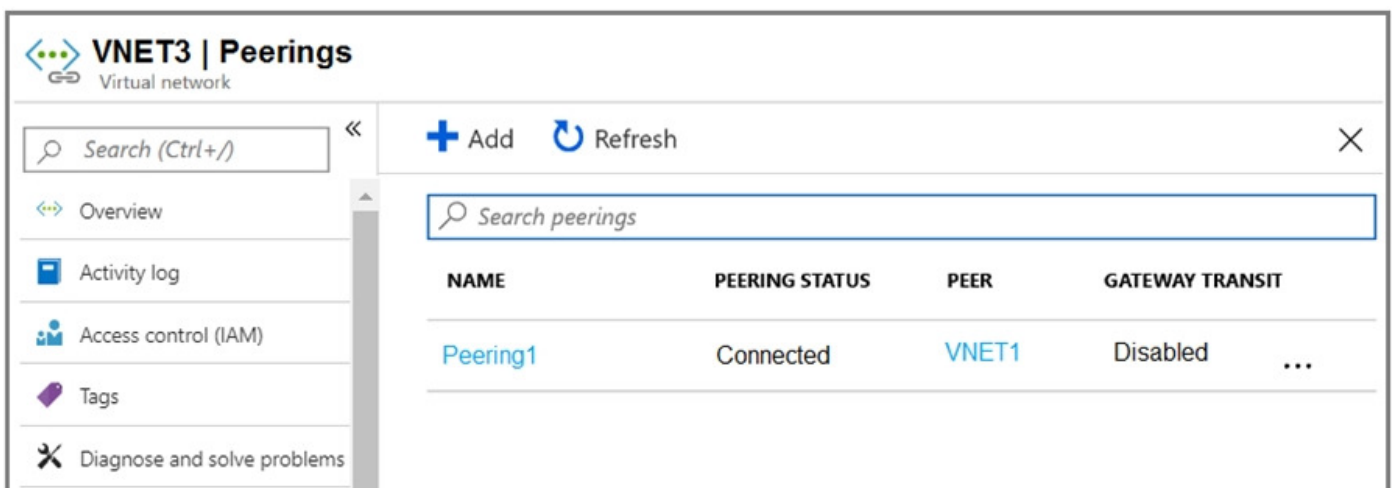
Peering for VNET2 is configured as shown in the following exhibit.



The screenshot shows the 'VNET2 | Peerings' page in the Azure portal. The left sidebar contains navigation links: Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. The main area has a search bar and a table of peerings. The table has columns: NAME, PEERING STATUS, PEER, and GATEWAY TRANSIT. There is one entry named 'Peering1' with a status of 'Connected'. The peer is 'VNET1' and the gateway transit is 'Disabled'.

NAME	PEERING STATUS	PEER	GATEWAY TRANSIT
Peering1	Connected	VNET1	Disabled ...

Peering for VNET3 is configured as shown in the following exhibit.



The screenshot shows the 'VNET3 | Peerings' page in the Azure portal. The left sidebar contains navigation links: Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. The main area has a search bar and a table of peerings. The table has columns: NAME, PEERING STATUS, PEER, and GATEWAY TRANSIT. There is one entry named 'Peering1' with a status of 'Connected'. The peer is 'VNET1' and the gateway transit is 'Disabled'.

NAME	PEERING STATUS	PEER	GATEWAY TRANSIT
Peering1	Connected	VNET1	Disabled ...

How can packets be routed between the virtual networks? To answer, select the appropriate options in the 2022 Latest AZ-104/DP-900/SC-900/AZ-900 Exam Real Que's and other exam series on [CertyIQ](#) (YouTube Channel)

answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Packets from VNET1 can be routed to:

<input type="checkbox"/>	▼
VNET2 only	
VNET3 only	
VNET2 and VNET3	

Packets from VNET2 can be routed to:

<input type="checkbox"/>	▼
VNET1 only	
VNET3 only	
VNET1 and VNET3	

Correct Answer:

Answer Area

Packets from VNET1 can be routed to:

<input type="checkbox"/>	▼
VNET2 only	
VNET3 only	
VNET2 and VNET3	

Packets from VNET2 can be routed to:

<input type="checkbox"/>	▼
VNET1 only	
VNET3 only	
VNET1 and VNET3	

Explanation:

Box 1. VNET2 and VNET3

Box 2: VNET1

Gateway transit is disabled.

Reference:

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

Question 262

CertyIQ

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

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

You have a computer named Computer1 that has a point-to-site VPN connection to an Azure virtual network named VNet1. The point-to-site connection uses a self-signed certificate.

From Azure, you download and install the VPN client configuration package on a computer named Computer2.

You need to ensure that you can establish a point-to-site VPN connection to VNet1 from Computer2.

Solution: You modify the Azure Active Directory (Azure AD) authentication policies.

Does this meet the goal?

A. Yes

B. No

Explanation:

Correct Answer: B

Instead export the client certificate from Computer1 and install the certificate on Computer2.

Note:

Each client computer that connects to a VNet using Point-to-Site must have a client certificate installed. You generate a client certificate from the self-signed root certificate, and then export and install the client certificate.

If the client certificate is not installed, authentication fails.

Reference:

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

Question 263

CertyIQ

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

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

You have a computer named Computer1 that has a point-to-site VPN connection to an Azure virtual network named VNet1. The point-to-site connection uses a self-signed certificate.

From Azure, you download and install the VPN client configuration package on a computer named Computer2.

You need to ensure that you can establish a point-to-site VPN connection to VNet1 from Computer2.

Solution: You join Computer2 to Azure Active Directory (Azure AD)

Does this meet the goal?

A. Yes

B. No

Explanation:

A client computer that connects to a VNet using Point-to-Site must have a client certificate installed.

Reference:

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

Question 264

CertyIQ

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

2022 Latest AZ-104/DP-900/SC-900/AZ-900 Exam Real Que's and other exam series on [CertyIQ](#) (YouTube Channel)

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

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

You have an Azure subscription that contains 10 virtual networks. The virtual networks are hosted in separate resource groups.

Another administrator plans to create several network security groups (NSGs) in the subscription.

A1EF0DA36AF2AEB0893389B060FE620E

You need to ensure that when an NSG is created, it automatically blocks TCP port 8080 between the virtual networks.

Solution: You create a resource lock, and then you assign the lock to the subscription.

Does this meet the goal?

A. Yes

B. No


Question 265

CertyIQ

You have an Azure subscription named Subscription1. Subscription1 contains a virtual machine named VM1.

You have a computer named Computer1 that runs Windows 10. Computer1 is connected to the Internet.


You add a network interface named vm1173 to VM1 as shown in the exhibit. (Click the Exhibit tab.)

 **Network Interface: vm1173** **Effective security rules** Topology






Virtual network/subnet: **RG1-vnet/default** Public IP: **VM1-ip** Private IP: **10.0.0.5** Accelerated

networking: **Disabled**

Inbound port rules Outbound port rules Application security groups Load balancing

 Network security group **VM1-nsg** (attached to network interface: **vm1173**) **Add inbound port rule**

Impacts 0 subnets, 1 network interfaces

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINA...	ACTION
300	 RDP	3389	TCP	Any	Any	 Allow ...
65000	AllowVnetInBound	Any	Any	VirtualN...	VirtualN...	 Allow ...
65001	AllowAzureLoadB...	Any	Any	AzureLo...	Any	 Allow ...
65500	DenyAllInBound	Any	Any	Any	Any	 Deny ...

From Computer1, you attempt to connect to VM1 by using Remote Desktop, but the connection fails.

You need to establish a Remote Desktop connection to VM1.

What should you do first?

A. Change the priority of the RDP rule

B. Attach a network interface

C. Delete the DenyAllInBound rule

D. Start VM1

Explanation:

Correct Answer: D

Incorrect Answers:

A: Rules are processed in priority order, with lower numbers processed before higher numbers, because lower numbers have higher priority. Once traffic matches a rule, processing stops. RDP already has the lowest number and thus the highest priority.

B: The network interface has already been added to VM.

C: The Outbound rules are fine.

Reference:

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

Question 266



CertyIQ

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

Name	IP address	Connected to
VM1	10.1.0.4	VNET1/Subnet1
VM2	10.1.10.4	VNET1/Subnet2
VM3	172.16.0.4	VNET2/SubnetA
VM4	10.2.0.8	VNET3/SubnetB

A DNS service is installed on VM1.

You configure the DNS servers settings for each virtual network as shown in the following exhibit.

 Save  Discard

DNS servers ⓘ

☐ Default (Azure-provided)

☒ Custom

10.1.0.4 ...

...

You need to ensure that all the virtual machines can resolve DNS names by using the DNS service on VM1. What should you do?

- A. Configure a conditional forwarder on VM1
- B. Add service endpoints on VNET1
- C. Add service endpoints on VNET2 and VNET3
- D. Configure peering between VNET1, VNET2, and VNET3

Explanation:

Correct Answer: D

Virtual network peering enables you to seamlessly connect networks in Azure Virtual Network. The virtual networks appear as one for connectivity purposes. The traffic between virtual machines uses the Microsoft backbone infrastructure.

Incorrect Answers:

B, C: Virtual Network (VNet) service endpoint provides secure and direct connectivity to Azure services over an optimized route over the Azure backbone network. Endpoints allow you to secure your critical Azure service resources to only your virtual networks. Service Endpoints enables private IP addresses in the VNet to reach the endpoint of an Azure service without needing a public IP address on the VNet.

Reference:

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

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

Question 267

CertyIQ

HOTSPOT

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

Name	Connected to subnet
VM1	172.16.1.0/24
VM2	172.16.2.0/24

You add inbound security rules to a network security group (NSG) named NSG1 as shown in the following table.

Priority	Source	Destination	Protocol	Port	Action
100	172.16.1.0/24	172.16.2.0/24	TCP	Any	Allow
101	Any	172.16.2.0/24	TCP	Any	Deny

You run Azure Network Watcher as shown in the following exhibit.

Resource group *

RG1 ✓

Source type *

Virtual machine ▼

* Virtual machine

VM1 ▼

Destination

☒ Select a virtual machine ☐ Specify manually

Resource group *

RG1 ✓

Virtual machine * ?

VM2 ▼

Probe Settings

Protocol ?

☒ TCP ☐ ICMP

Destination port * ?

8080 ▼

Advanced settings

Check

Status

⚠ Unreachable

Agent extension version
1.4

Source virtual machine
VM1

Grid view Topology view

Hops

NAME	IP ADDRESS	STATUS	NEXT HOP IP ADDRESS	RTT FROM SOURCE (...)
VM1	172.16.1.4	✓	172.16.2.4	-
VM2	172.16.2.4	●	-	-

You run Network Watcher again as shown in the following exhibit.

Source type *

Virtual machine

* Virtual machine

VM1

Destination

☒ Select a virtual machine ☐ Specify manually

Resource group *

RG1

Virtual machine* ⓘ

VM2

Probe Settings

Protocol ⓘ

☐ TCP ☒ ICMP

Check

Status

✓ Reachable

Agent extension version

1.4

Source virtual machine

VM1

Grid view Topology view

Hops

NAME	IP ADDRESS	STATUS	NEXT HOP IP ADDRESS	RTT FROM SOURCE (...)
VM1	172.16.1.4	✓	172.16.2.4	0
VM2	172.16.2.4	✓	-	-

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

Answer Area

Statements	Yes	No
NSG1 limits VM1 traffic	<input type="radio"/>	<input type="radio"/>
NSG1 applies to VM2	<input type="radio"/>	<input type="radio"/>
VM1 and VM2 connect to the same virtual network	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
NSG1 limits VM1 traffic	<input type="radio"/>	<input checked="" type="radio"/>
NSG1 applies to VM2	<input checked="" type="radio"/>	<input type="radio"/>
VM1 and VM2 connect to the same virtual network	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Box 1: No

It limits traffic to VM2, but not VM1 traffic.

Box 2: Yes

Yes, the destination is VM2.

Box 3: No

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works>

Question 268

CertyIQ

You have the Azure virtual network named VNet1 that contains a subnet named Subnet1. Subnet1 contains three Azure virtual machines. Each virtual machine has a public IP address. The virtual machines host several applications that are accessible over port 443 to users on the Internet. Your on-premises network has a site-to-site VPN connection to VNet1. You discover that the virtual machines can be accessed by using the Remote Desktop Protocol (RDP) from the Internet and from the on-premises network. You need to prevent RDP access to the virtual machines from the Internet, unless the RDP connection is established from the on-premises network. The solution must ensure that all the applications can still be accessed by the Internet users. What should you do?

- A. Modify the address space of the local network gateway
- B. Create a deny rule in a network security group (NSG) that is linked to Subnet1
- C. Remove the public IP addresses from the virtual machines
- D. Modify the address space of Subnet1

Explanation:

You can use a site-to-site VPN to connect your on-premises network to an Azure virtual network. Users on your

on-premises network connects by using the RDP or SSH protocol over the site-to-site VPN connection. You don't have to allow direct RDP or SSH access over the internet.

Reference:

<https://docs.microsoft.com/en-us/azure/security/fundamentals/network-best-practices>

Question 269

CertyIQ

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

Name	Type
ASG1	Application security group
NSG1	Network security group (NSG)
Subnet1	Subnet
VNet1	Virtual network
NIC1	Network interface
VM1	Virtual machine

Subnet1 is associated to VNet1. NIC1 attaches VM1 to Subnet1.
You need to apply ASG1 to VM1.
What should you do?

A. Associate NIC1 to ASG1

B. Modify the properties of ASG1

C. Modify the properties of NSG1

Explanation:

Correct Answer: A

Application Security Group can be associated with NICs.

References:

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

Question 270

CertyIQ

You have an Azure subscription named Subscription1 that contains an Azure virtual network named VNet1. VNet1 connects to your on-premises network by using Azure ExpressRoute. You plan to prepare the environment for automatic failover in case of ExpressRoute failure. You need to connect VNet1 to the on-premises network by using a site-to-site VPN. The solution must minimize cost. Which three actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Create a connection

B. Create a local site VPN gateway

C. Create a VPN gateway that uses the VpnGw1 SKU

D. Create a gateway subnet

E. Create a VPN gateway that uses the Basic SKU

Explanation:

Correct Answer: ADE

Reference:

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

Question 271

CertyIQ

HOTSPOT

You have peering configured as shown in the following exhibit.

NAME	PEERING STATUS	PEER	GATEWAY TRANSIT
peering1	Disconnected	vNET1	Enabled ...
peering2	Disconnected	vNET2	Disabled ...

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Hosts on vNET6 can communicate with hosts on [answer choice].

	▼
vNET6 only	
vNET6 and vNET1 only	
vNET6, vNET1, and vNET2 only	
all the virtual networks in the subscription	

To change the status of the peering connection to vNET1 to **Connected**, you must first [answer choice].

	▼
add a service endpoint	
add a subnet	
delete peering1	
modify the address space	

Correct Answer:

Answer Area

Hosts on vNET6 can communicate with hosts on [answer choice].

	▼
vNET6 only	
vNET6 and vNET1 only	
vNET6, vNET1, and vNET2 only	
all the virtual networks in the subscription	

To change the status of the peering connection to vNET1 to **Connected**, you must first [answer choice].

	▼
add a service endpoint	
add a subnet	
delete peering1	
modify the address space	

Explanation:

Box 1: vNET6 only

Peering status to both VNet1 and Vnet2 are disconnected.

Box 2: delete peering1

Peering to Vnet1 is Enabled but disconnected. We need to update or re-create the remote peering to get it back to Initiated state.

Reference:

<https://blog.kloud.com.au/2018/10/19/address-space-maintenance-with-vnet-peering/>

Question 272

CertyIQ

HOTSPOT

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

Name	Type
VM1	Virtual machine
VM2	Virtual machine
LB1	Load balancer (Basic SKU)

You install the Web Server server role (IIS) on VM1 and VM2, and then add VM1 and VM2 to LB1. LB1 is configured as shown in the LB1 exhibit. (Click the LB1 tab.)

Essentials ^	
Resource group (change)	Backend pool
VMRG	Backend1 (2 virtual machines)
Location	Health probe
West Europe	Probe1(HTTP:80/Probe1.htm)
Subscription name (change)	Load balancing rule
Azure Pass	Rule1 (TCP/80)
Subscription ID	NAT rules
e65d2b22-fde8	-
SKU	Public IP address
Basic	104.40.178.194 (LB1)

Rule1 is configured as shown in the Rule1 exhibit. (Click the Rule1 tab.)

* Name
Rule1

* IP Version
☒ IPv4 ☐ IPv6

* Frontend IP address ⓘ
104.40.178.194 (LoadBalanceFrontEnd) ▼

Protocol
☒ TCP ☐ UDP

* Port
80

* Backend port ⓘ
80

Backend pool ⓘ
Backend1 (2 virtual machines) ▼

Health probe ⓘ
Probe1 (HTTP:80/Probe1.htm) ▼

Session persistence ⓘ
None ▼

Idle timeout (minutes) ⓘ
 4

Floating IP (direct server return) ⓘ
Disabled

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
VM1 is in the same availability set as VM2.	<input type="radio"/>	<input checked="" type="radio"/>
If Probe1.htm is present on VM1 and VM2, LB1 will balance TCP port 80 between VM1 and VM2.	<input type="radio"/>	<input type="radio"/>
If you delete Rule1, LB1 will balance all the requests between VM1 and VM2 for all the ports.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
VM1 is in the same availability set as VM2.	<input checked="" type="radio"/>	<input type="radio"/>
If Probe1.htm is present on VM1 and VM2, LB1 will balance TCP port 80 between VM1 and VM2.	<input checked="" type="radio"/>	<input type="radio"/>
If you delete Rule1, LB1 will balance all the requests between VM1 and VM2 for all the ports.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Box 1: Yes

A Basic Load Balancer supports virtual machines in a single availability set or virtual machine scale set.

Box 2: Yes

When using load-balancing rules with Azure Load Balancer, you need to specify health probes to allow Load Balancer to detect the backend endpoint status. The configuration of the health probe and probe responses determine which backend pool instances will receive new flows. You can use health probes to detect the failure of an application on a backend endpoint. You can also generate a custom response to a health probe and use the health probe for flow control to manage load or planned downtime. When a health probe fails, Load Balancer will stop sending new flows to the respective unhealthy instance. Outbound connectivity is not impacted, only inbound connectivity is impacted.

Box 3: No

Reference:

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

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

Question 273

CertyIQ

HOTSPOT

You have an Azure virtual machine named VM1 that connects to a virtual network named VNet1. VM1 has the following configurations:

Subnet: 10.0.0.0/24

Availability set: AVSet

Network security group (NSG): None

Private IP address: 10.0.0.4 (dynamic)

Public IP address: 40.90.219.6 (dynamic)

You deploy a standard, Internet-facing load balancer named slb1.

You need to configure slb1 to allow connectivity to VM1.

Which changes should you apply to VM1 as you configure slb1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Before you create a backend pool on slb1, you must:

- Create and assign an NSG to VM1
- Remove the public IP address from VM1
- Change the private IP address of VM1 to static

Before you can connect to VM1 from slb1, you must:

- Create and configure an NSG
- Remove the public IP address from VM1
- Change the private IP address of VM1 to static

Correct Answer:

Answer Area

Before you create a backend pool on slb1, you must:

- Create and assign an NSG to VM1
- Remove the public IP address from VM1
- Change the private IP address of VM1 to static

Before you can connect to VM1 from slb1, you must:

- Create and configure an NSG
- Remove the public IP address from VM1
- Change the private IP address of VM1 to static

Explanation:

Change the private IP address of VM1 to static

Box 1: Remove the public IP address from VM1

Note: A public load balancer can provide outbound connections for virtual machines (VMs) inside your virtual network. These connections are accomplished by translating their private IP addresses to public IP addresses. Public Load Balancers are used to load balance internet traffic to your VMs.

Box 2: Create and configure an NSG

NSGs are used to explicitly permit allowed traffic. If you do not have an NSG on a subnet or NIC of your virtual machine resource, traffic is not allowed to reach this resource.

Reference:

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

Question 274

CertyIQ

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

Name	Type	Location
VNET1	Virtual network	East US
IP1	Public IP address	West Europe
RT1	Route table	North Europe

You need to create a network interface named NIC1.
In which location can you create NIC1?

A. East US and North Europe only

B. East US only

C. East US, West Europe, and North Europe

D. East US and West Europe only

Explanation:

Correct Answer: B

Before creating a network interface, you must have an existing virtual network in the same location and subscription you create a network interface in.

Reference:

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

Question 275

CertyIQ

You have Azure virtual machines that run Windows Server 2019 and are configured as shown in the following table.

Name	Virtual network name	DNS suffix configured in Windows Server
VM1	VNET1	Contoso.com
VM2	VNET2	Contoso.com

You create a public Azure DNS zone named adatum.com and a private Azure DNS zone named contoso.com. For contoso.com, you create a virtual network link named link1 as shown in the exhibit. (Click the **Exhibit** tab.)

The screenshot shows the configuration page for a virtual network link named 'link1' in the Azure portal. The page has a title bar with 'link1' and 'contoso.com'. Below the title bar are tabs for 'Save', 'Discard', 'Delete', 'Access Control (IAM)', and 'Tags'. The main content area shows the following details:

- Link name:** link1
- Link state:** Completed
- Provisioning state:** Succeeded
- Virtual network details:**
 - Virtual network id:** /subscriptions/8372f433-2dcd-4361-b5ef-5b188fed87d0/resourceGroups/RG2/provi...
- Virtual network:** VNET1
- Configuration:**
 - ☐ Enable auto registration ⓘ

You discover that VM1 can resolve names in contoso.com but cannot resolve names in adatum.com. VM1 can resolve other hosts on the Internet.

You need to ensure that VM1 can resolve host names in adatum.com.

What should you do?

- A. Update the DNS suffix on VM1 to be adatum.com
- B. Configure the name servers for adatum.com at the domain registrar
- C. Create an SRV record in the contoso.com zone
- D. Modify the Access control (IAM) settings for link1

Explanation:

Correct Answer: A

If you use Azure Provided DNS then appropriate DNS suffix will be automatically applied to your virtual machines. For all other options you must either use Fully Qualified Domain Names (FQDN) or manually apply appropriate DNS suffix to your virtual machines.

Reference:

Question 276

CertyIQ

HOTSPOT

You plan to use Azure Network Watcher to perform the following tasks:

Task1: Identify a security rule that prevents a network packet from reaching an Azure virtual machine.

Task2: Validate outbound connectivity from an Azure virtual machine to an external host.

Which feature should you use for each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Task1:	<div><div></div><div>IP flow verify</div><div>Next hop</div><div>Packet capture</div><div>Security group view</div><div>Traffic Analytics</div></div>
Task2:	<div><div></div><div>Connection troubleshoot</div><div>IP flow verify</div><div>Next hop</div><div>NSG flow logs</div><div>Traffic Analytics</div></div>

Correct Answer:

Answer Area

Task1:	<div><div></div><div>IP flow verify</div><div>Next hop</div><div>Packet capture</div><div>Security group view</div><div>Traffic Analytics</div></div>
Task2:	<div><div></div><div>Connection troubleshoot</div><div>IP flow verify</div><div>Next hop</div><div>NSG flow logs</div><div>Traffic Analytics</div></div>

Explanation:

Box 1: IP flow verify

At some point, a VM may become unable to communicate with other resources, because of a security rule.

The IP flow verify capability enables you to specify a source and destination IPv4 address, port, protocol (TCP or UDP), and traffic direction (inbound or outbound). IP flow verify then tests the communication and informs you if the connection succeeds or fails. If the connection fails, IP flow verify tells you which.

Box 2: Connection troubleshoot

Diagnose outbound connections from a VM: The connection troubleshoot capability enables you to test a connection between a VM and another VM, an FQDN, a URI, or an IPv4 address. The test returns similar information returned when using the connection monitor capability, but tests the connection at a point in time, rather than monitoring it over time, as connection monitor does. Learn more about how to troubleshoot connections using connection-troubleshoot.

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview>

Question 277

CertyIQ

HOTSPOT

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

Name	Operating system	Subnet	Virtual network
VM1	Windows Server 2019	Subnet1	VNET1
VM2	Windows Server 2019	Subnet2	VNET1
VM3	Red Hat Enterprise Linux 7.7	Subnet3	VNET1

You configure the network interfaces of the virtual machines to use the settings shown in the following table.

Name	DNS server
VM1	<i>None</i>
VM2	192.168.10.15
VM3	192.168.10.15

From the settings of VNET1 you configure the DNS servers shown in the following exhibit.

DNS servers ⓘ

☐ Default (Azure-provided)

☒ Custom

193.77.134.10 ...

Add DNS ser ...

The virtual machines can successfully connect to the DNS server that has an IP address of 192.168.10.15 and the DNS server that has an IP address of 193.77.134.10.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
VM1 connects to 193.77.134.10 for DNS queries.	<input type="radio"/>	<input type="radio"/>
VM2 connects to 193.77.134.10 for DNS queries.	<input type="radio"/>	<input type="radio"/>
VM3 connects to 192.168.10.15 for DNS queries.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
VM1 connects to 193.77.134.10 for DNS queries.	<input checked="" type="radio"/>	<input type="radio"/>
VM2 connects to 193.77.134.10 for DNS queries.	<input type="radio"/>	<input checked="" type="radio"/>
VM3 connects to 192.168.10.15 for DNS queries.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Box 1: Yes

You can specify DNS server IP addresses in the VNet settings. The setting is applied as the default DNS server(s) for all VMs in the VNet.

Box 2: No

You can set DNS servers per VM or cloud service to override the default network settings.

Box 3: Yes

You can set DNS servers per VM or cloud service to override the default network settings.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-faq#name-resolution-dns>

Question 278

CertyIQ

HOTSPOT

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

Name	Lock name	Lock type
RG1	None	None
RG2	Lock	Delete

RG1 contains the resources shown in the following table.

Name	Type	Lock name	Lock type
storage2	Storage account	Lock1	Delete
VNET2	Virtual network	Lock2	Read-only
IP2	Public IP address	None	None

You need to identify which resources you can move from RG1 to RG2, and which resources you can move from RG2 to RG1.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Resources that you can move from RG1 to RG2:

▼

None

IP1 only

IP1 and storage1 only

IP1 and VNET1 only

IP1, VNET2, and storage1

Resources that you can move from RG2 to RG1:

▼

None

IP2 only

IP2 and storage2 only

IP2 and VNET2 only

IP2, VNET2, and storage2

Correct Answer:

Answer Area

Resources that you can move from RG1 to RG2:

▼

None

IP1 only

IP1 and storage1 only

IP1 and VNET1 only

IP1, VNET2, and storage1

Resources that you can move from RG2 to RG1:

▼

None

IP2 only

IP2 and storage2 only

IP2 and VNET2 only

IP2, VNET2, and storage2

Explanation:

Box 1: IP1, Storage1

IP addresses and storage accounts can be moved.

Virtual networks cannot be moved.

There is no lock on RG1.

Box 2: None

There is a delete lock on RG2.

Note: When you apply a lock at a parent scope, all resources within that scope inherit the same lock. Even resources you add later inherit the lock from the parent. The most restrictive lock in the inheritance takes precedence.

CanNotDelete means authorized users can still read and modify a resource, but they can't delete the resource.

ReadOnly means authorized users can read a resource, but they can't delete or update the resource. Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources>

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/move-support-resources>

Question 279

CertyIQ

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

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

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

You deploy a load balancer that has the following configurations:

Name: LB1

Type: Internal

SKU: Standard

Virtual network: VNET1

You need to ensure that you can add VM1 and VM2 to the backend pool of LB1.

Solution: You create a Basic SKU public IP address, associate the address to the network interface of VM1, and then start VM1.

Does this meet the goal?

A. Yes

B. No

Explanation:

A Backend Pool configured by IP address has the following limitations:

Standard load balancer only

Reference:

<https://docs.microsoft.com/en-us/azure/load-balancer/backend-pool-management>

Question 280

CertyIQ

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

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

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

You deploy a load balancer that has the following configurations:

Name: LB1

Type: Internal

SKU: Standard

Virtual network: VNET1

You need to ensure that you can add VM1 and VM2 to the backend pool of LB1.

Solution: You create a Standard SKU public IP address, associate the address to the network interface of VM1, and then stop VM2.

Does this meet the goal?

A. Yes

B. No

Explanation:

A Backend Pool configured by IP address has the following limitations:

Standard load balancer only

Reference:

<https://docs.microsoft.com/en-us/azure/load-balancer/backend-pool-management>

End of Part 7



Please find the videos of this **AZ-900/AI-900/AZ-305/AZ-104 /DP-900/ SC-900** and other Microsoft exam series on

CertyIQ Official YouTube channel (FREE PDFs): -

Please **Subscribe** to CertyIQ YouTube Channel to get notified for latest exam dumps by clicking on the below image, it will redirect to the **CertyIQ** YouTube page.



Connect with us @ [LinkedIn](#) [Telegram](#)

Contact us for other dumps: -

contact.certyiqofficial@gmail.com

For any other enquiry, please drop us a mail at

enquiry.certyiqofficial@gmail.com