

AZ-700^{Q&As}

Designing and Implementing Microsoft Azure Networking Solutions

Pass Microsoft AZ-700 Exam with 100% Guarantee

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

<https://www.leads4pass.com/az-700.html>

100% Passing Guarantee
100% Money Back Assurance

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

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

You need to ensure that hosts on VNET1 and VNET2 can communicate. The solution must minimize latency between the virtual networks.

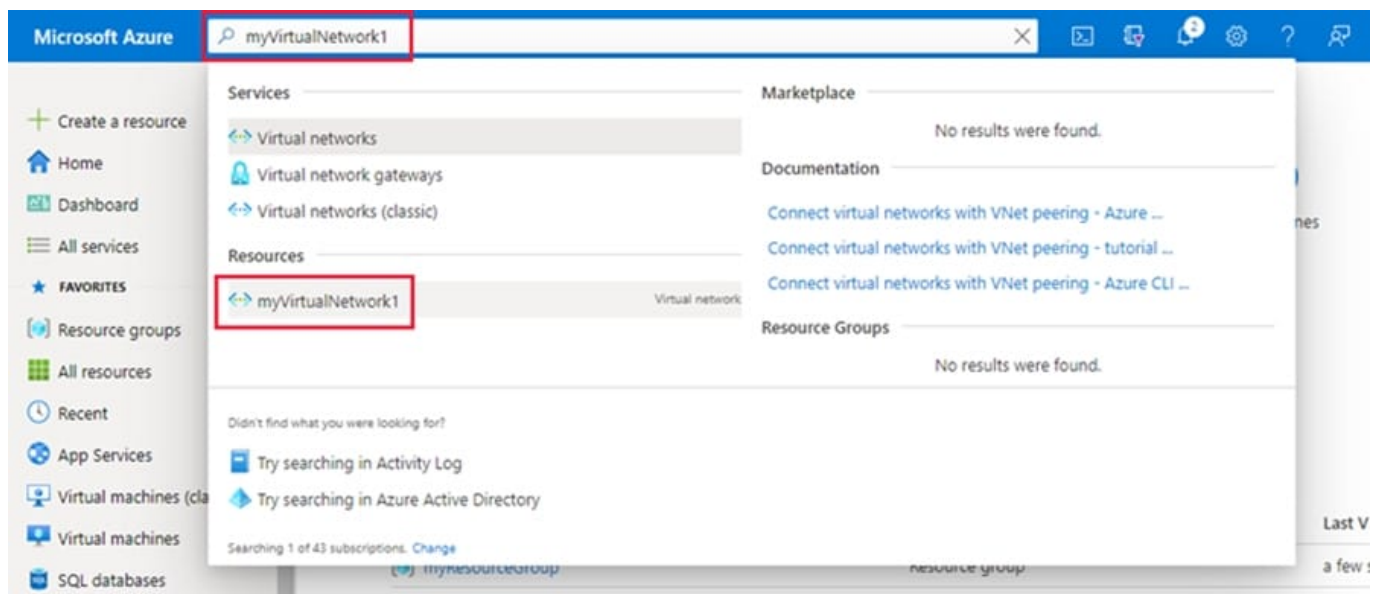
To complete this task, sign in to the Azure portal.

- A. See explanation below.
- B. Placeholder
- C. Placeholder
- D. Placeholder

Correct Answer: A

Peer virtual networks

Step 1: In the search box at the top of the Azure portal, look for VNet1. When VNET1 appears in the search results, select it.



Step 2: Under Settings, select Peerings, and then select + Add, as shown in the following picture:

Home > myVirtualNetwork1

myVirtualNetwork1 | Peerings

Search (Ctrl+/) << **Add** Refresh

Filter by name...

Name ↑↓	Peering status ↑↓	Peer ↑↓	Gateway transit ↑↓
Add a peering to get started			

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

Settings

- Address space
- Connected devices
- Subnets
- DDoS protection
- Firewall
- Security
- DNS servers
- Peerings**
- Service endpoints

Step 3: Enter or select the following information, accept the defaults for the remaining settings, and then select Add.

*

..

*

Virtual network

Select VNET2 for the name of the remote virtual network. The remote virtual network can be in the same region of VNET1 or in a different region.

Home > myVirtualNetwork1 >

Add peering

myVirtualNetwork1

i For peering to work, two peering links must be created. By selecting remote virtual network, Azure will create both peering links.

This virtual network

Peering link name *

myVirtualNetwork1-myVirtualNetwork2 ✓

Traffic to remote virtual network ⓘ

- Allow (default)
- Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ

- Allow (default)
- Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server ⓘ

- Use this virtual network's gateway or Route Server
- Use the remote virtual network's gateway or Route Server
- None (default)

Remote virtual network

Peering link name *

myVirtualNetwork2-myVirtualNetwork1 ✓

Virtual network deployment model ⓘ

- Resource manager
- Classic

I know my resource ID ⓘ

Subscription * ⓘ

Azure Subscription ✓

Virtual network *

myVirtualNetwork2 ✓

Traffic to remote virtual network ⓘ

- Allow (default)
- Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ

- Allow (default)
- Block traffic that originates from outside this virtual network

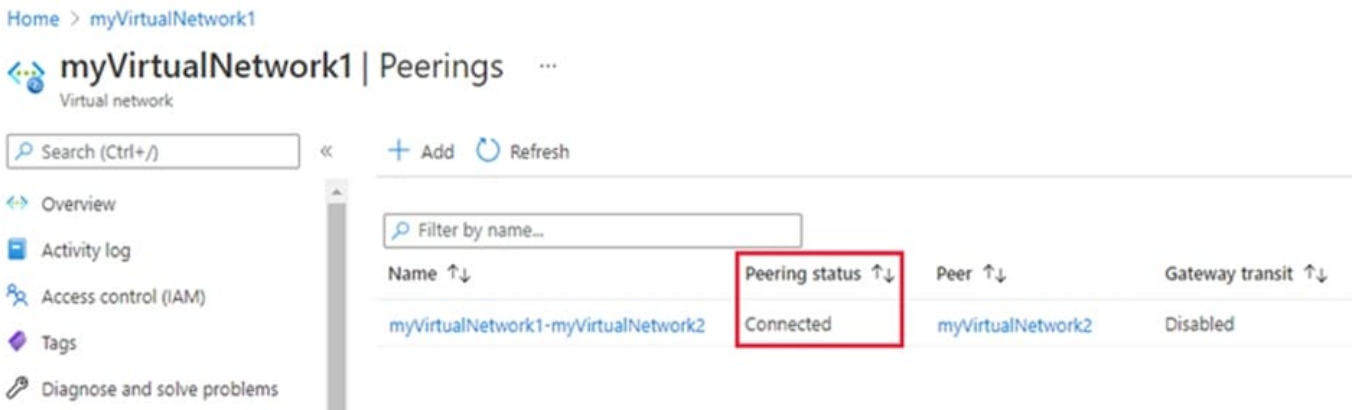
Virtual network gateway or Route Server ⓘ

- Use this virtual network's gateway or Route Server
- Use the remote virtual network's gateway or Route Server
- None (default)

Add

Step 4: Click Add

In the Peering page, the Peering status is Connected, as shown in the following picture:



Reference: <https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-connect-virtual-networks-portal>

QUESTION 2

HOTSPOT

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:



Correct Answer:



QUESTION 3

You need to ensure that all hosts deployed to subnet3-2 connect to the internet by using the same static public IP address. The solution must minimize administrative effort when adding hosts to the subnet.

To complete this task, sign in to the Azure portal.

- A. See explanation below.
- B. Placeholder
- C. Placeholder
- D. Placeholder

Correct Answer: A

NAT gateway provides outbound internet connectivity for one or more subnets of a virtual network. Once NAT gateway is associated to a subnet, NAT provides source network address translation (SNAT) for that subnet. NAT gateway

specifies which static IP addresses virtual machines use when creating outbound flows.

Plan:

Stage 1: Create a NAT gateway

Stage 2: Edit subnet subnet3-2 and link it to the NAT gateway

Stage 1: Create a NAT gateway

Step 1: Sign in to the Azure portal.

Step 2: In the search box at the top of the portal, enter NAT gateway. Select NAT gateways in the search results.

Step 3: Select + Create.

Step 4: In Create network address translation (NAT) gateway, enter or select this information in the Basics tab:

* NAT gateway name: Enter myNATgateway

Step 5: Select the Outbound IP tab, or select the Next: Outbound IP button at the bottom of the page.

Step 6: In the Outbound IP tab, enter or select the following information:

Public IP addresses - Select Create a new public IP address.

In Name, enter myPublicIP.

Select OK.

Step 7: Select the Review + create tab, or select the blue Review + create button at the bottom of the page.

Step 8: Select Create.

Stage 2: Edit subnet subnet3-2 and link it to the NAT gateway

Change subnet settings

Step 1: Go to the Azure portal to view your virtual networks. Search for and select Virtual networks.

Step 2: Select the name of the virtual network containing the subnet you want to change.

Step 3: From Settings, select Subnets.

Step 4: In the list of subnets, select the subnet you want to change settings for. Here choose subnet3-2 connect.

Step 5: In the subnet page, change the NAT Gateway to myNATgateway (the one we created in Stage 1).

Step 6: Select Save.

Reference:

<https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource> <https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/quickstart-create-nat-gateway-portal>

QUESTION 4

Your company has an Azure virtual network named Vnet1 that uses an IP address space of 192.168.0.0/20.

Vnet1 contains a subnet named Subnet1 that uses an IP address space of 192.168.0.0/24. You create an IPv6 address range to Vnet1 by using a CIDR suffix of /48. You need to enable the virtual machines on Subnet1 to communicate with each other by using IPv6 addresses assigned by the company.

The solution must minimize the number of additional IPv4 addresses.

What should you do for each virtual machine?

- A. Create an additional IP configuration
- B. Create an additional NIC
- C. Create a public IPv6 address

Correct Answer: A

You need to configure the VM NICs with an IPv6 address. <https://docs.microsoft.com/en-us/azure/load-balancer/ipv6-add-to-existing-vnet-cli>

QUESTION 5

You have an Azure subscription that contains two virtual networks named VritualNetwork1 and VritualNetwork2.

You have a Windows 10 device that connects to VritualNetwork1 by using a Point-to-Site (P2S) IKEv2 VPN. You have implemented virtual network peering between VritualNetwork1 and VritualNetwork2.

VritualNetwork1 allows gateway transit. VritualNetwork2 can use the remote gateway. You discover that you cannot communicate with VritualNetwork2 from the Windows 10 device. You need to ensure that you can communicate with

VritualNetwork2 from the Windows 10 device.

To achieve the requirement, you download and reinstall the VPN client configuration.

Did you achieve the requirement?

A. Yes

B. No

Correct Answer: A

The VPN client must be downloaded again if any changes are made to VNet peering or the network topology.

If you make a change to the topology of your network and have Windows VPN clients, the VPN client package for Windows clients must be downloaded and installed again in order for the changes to be applied to the client.

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

[Latest AZ-700 Dumps](#)

[AZ-700 VCE Dumps](#)

[AZ-700 Practice Test](#)