AZ-720 Q&As

Troubleshooting Microsoft Azure Connectivity

Pass Microsoft AZ-720 Exam with 100% Guarantee

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

https://www.pass4itsure.com/az-720.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

A company has two subnet in a virtual network named VNe1m the subnet are named SubnetA and SubnetB. The company uses a site-to-site (S2) VPN in SubnetB to connect its on-premises environment to Azure. You deploy an Azure SQL Database named SQL1. You configure a service endpoint in SubnetA for Microsft.SqL

A. Configure a DNS record for the private IP address of SQL1.

B. Configure a network security group (NSG) to allow port 1433 on SubnetA

C. Configure a service endpoint on SubnetB.

D. Deploy a private endpoint for SQL1.

E. Deploy an Azure ExpressRoute circuit for VNet1.

Correct Answer: D

To allow the on-premises environment to access the Azure SQL Database named SQL1 over a site-to-site (S2S) VPN in SubnetB, you should deploy a private endpoint for SQL1. A private endpoint is a network interface that connects you

privately and securely to a service powered by Azure Private Link. Private Link allows you to access Azure PaaS services (for example, Azure Storage and SQL Database) and Azure-hosted customer/partner services over a private endpoint

in your virtual network. So the correct answer is D. Deploy a private endpoint for SQL1.

You can find more information about private endpoints in the official Microsoft documentation.

QUESTION 2

A company deploys Azure Bastion to connect to their virtual machine (VM) infrastructure. An engineer attempts to connect to a Windows VM by using Remote Desktop Protocol (RDP). The connection fails.

You need to troubleshoot the issue.

Which two actions should you perform?

A. Monitor traffic with the following PowerShell cmdlet Test- AzNetworkWatcherConnectivity.

B. Configure Azure Bastion with static assignment.

C. Apply a network security group on the same subnet as Azure Bastion.

D. Run the Network Watcher Connection troubleshoot service.

E. Monitor traffic with the following PowerShell cmdlet New-AzNetworkWatcherFlowLog.

Correct Answer: AD

The two actions that should be performed to troubleshoot the issue of a failed RDP connection to a Windows VM through Azure Bastion are A) Monitor traffic with the PowerShell cmdlet \\'Test-AzNetworkWatcherConnectivity\\' and D) Run the

Network Watcher Connection troubleshoot service.

A) Monitor traffic with the PowerShell cmdlet \\'Test-AzNetworkWatcherConnectivity\\': This cmdlet can be used to verify connectivity between two endpoints in Azure. By monitoring traffic, you can identify the root cause of issues with the VM\\'s

connectivity through Azure Bastion.

D) Run the Network Watcher Connection troubleshoot service: This service can help identify the root cause of connectivity issues with Azure resources. It analyses network traffic to identify common misconfiguration issues and provides

guidance on how to resolve them.

Reference:

https://docs.microsoft.com/en-us/azure/bastion/bastion-troubleshoot

https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-connectivity-powershell

QUESTION 3

A company has an ExpressRoute gateway between their on-premises site and Azure. The ExpressRoute gateway is on a virtual network named VNet1. The company enables FastPath on the gateway. You associate a network security group

(NSG) with all of the subnets.

Users report issues connecting to VM1 from the on-premises environment. VM1 is on a virtual network named VNet2. Virtual network peering is enabled between VNet1 and VNet2.

You create a flow log named FlowLog1 and enable it on the NSG associated with the gateway subnet.

You discover that FlowLog1 is not reporting outbound flow traffic.

You need to resolve the issue with FlowLog1.

What should you do?

A. Create the storage account for FlowLog1 as a premium block blob.

B. Create the storage account for FlowLog1 as a premium page blob.

C. Enable FlowLog1 in a network security group associated with the subnet of VM1.

D. Configure the FlowTimeoutInMinutes property on VNet1 to a non-null value.

Correct Answer: C

when FastPath is enabled on an ExpressRoute gateway, network traffic between your on-premises network and your virtual network bypasses the gateway and goes directly to virtual machines in the virtual network. Therefore, if you want to capture outbound flow traffic from VM1, you need to enable flow logging on an NSG associated with the subnet of VM1.

QUESTION 4

A company connects their on-premises network by using Azure VPN Gateway. The on- premises environment includes three VPN devices that separately tunnel to the gateway by using Border Gateway Protocol (BGP).

A new subnet should be unreachable from the on-premises network.

You need to implement a solution.

Solution: Disable peering on the virtual network.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: A

QUESTION 5

A company connects their on-premises network by using Azure VPN Gateway. The on- premises environment includes three VPN devices that separately tunnel to the gateway by using Border Gateway Protocol (BGP).

A new subnet should be unreachable from the on-premises network.

You need to implement a solution.

Solution: Configure subnet delegation.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: B

The proposed solution, which is to configure subnet delegation, does not meet the goal of making the new subnet unreachable from the on-premises network. Subnet delegation is a mechanism to delegate management of a subnet to another

resource such as a Network Virtual Appliance or a Service Endpoint. It does not provide any means to restrict or isolate a subnet from the rest of the network.

To meet the goal, you can use Network Security Groups (NSGs) to restrict traffic to and from the new subnet. NSGs allow you to define inbound and outbound security rules that specify the type of traffic that is allowed or denied based on

different criteria such as source or destination IP address, protocol, port number, etc. By creating a custom NSG and defining rules that deny traffic to and from the new subnet, you can effectively make that subnet unreachable from the on-

premises network.

Therefore, the correct answer is option B, "No".

Reference:

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

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