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.leads4pass.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 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 2

A company hosts a highly available application using Azure Load Balancer.

A virtual machine (VM) on the backend pool stops responding to health probes. The health probes are configured to use HTTP.

You are troubleshooting the incoming traffic issue. You run a Netsh trace on port 80. No incoming packets are detected on the VM. Outgoing packets are detected.

What is the cause of the issue?

A. A network security group is preventing incoming traffic to the port.

B. A proxy is configured.

C. Session persistence is configured.

D. An application on the VM is blocking the port.

Correct Answer: A

QUESTION 3

A company uses Azure AD Connect. The company plans to implement self-service password reset (SSPR).

An administrator receives an error that password writeback cloud not be enabled during the Azure AD Connect configuration. The administrator observes the following event log error:

Error getting auth token

You need to resolve the issue.

Solution: Disable password writeback and then enable password writeback.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: B

The solution of disabling and re-enabling password writeback may not meet the goal of resolving the issue. According to 1, there are other steps that you should try before disabling and re-enabling password writeback, such as:

1.

Confirm network connectivity

2.

Restart the Azure AD Connect Sync service

3.

Install the latest Azure AD Connect release

4.

Troubleshoot password writeback

If none of these steps work, then you can try to disable and re-enable password writeback as a last resort.

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: Configure a route table with route propagation disabled.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: B

The proposed solution of configuring a route table with route propagation disabled will not meet the goal of making the new subnet unreachable from the on- premises network.

Route tables in Azure are used to control traffic flow within a virtual network and between virtual networks. By default, each subnet in an Azure virtual network is associated with a system-generated route table, which contains a default route

that enables traffic to flow to and from all the subnets within the virtual network. Disabling route propagation in a custom route table would prevent any new routes from being propagated to the associated subnets. However, it would not

prevent traffic from the on-premises network from reaching the new subnet since traffic between the virtual network and the on-premises network would still use the default route in the system- generated route table.

To meet the goal of making the new subnet unreachable from the on-premises network, you would need to create a new route table with a route that sends traffic destined for the new subnet to a null interface. This would cause the traffic to

be dropped and the subnet to be effectively unreachable from the on-premises network.

Reference:

Microsoft documentation on how to create a custom route table and associate it with a subnet:

https://docs.microsoft.com/en-us/azure/virtual-network/manage-route-table#create-a-custom-route-table.

Microsoft documentation on how to configure a route to a null interface:

https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-create-route-table-portal#to-route-to-a-null-interface.

QUESTION 5

HOTSPOT

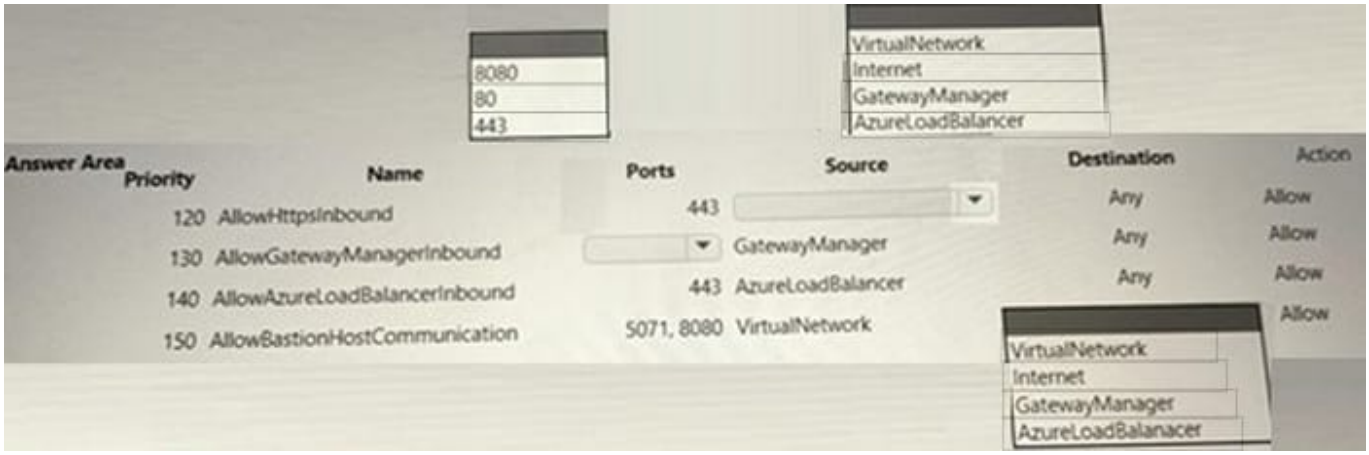
A company is deploying Azure Bastion to provide secure clientless access to its Azure VMs. The company configures a network security group named NSG1.

During deployment, the following error displays: Network security group NSG1 does not have necessary rules for Azure Bastion Subnet AzureBastionSubnet.

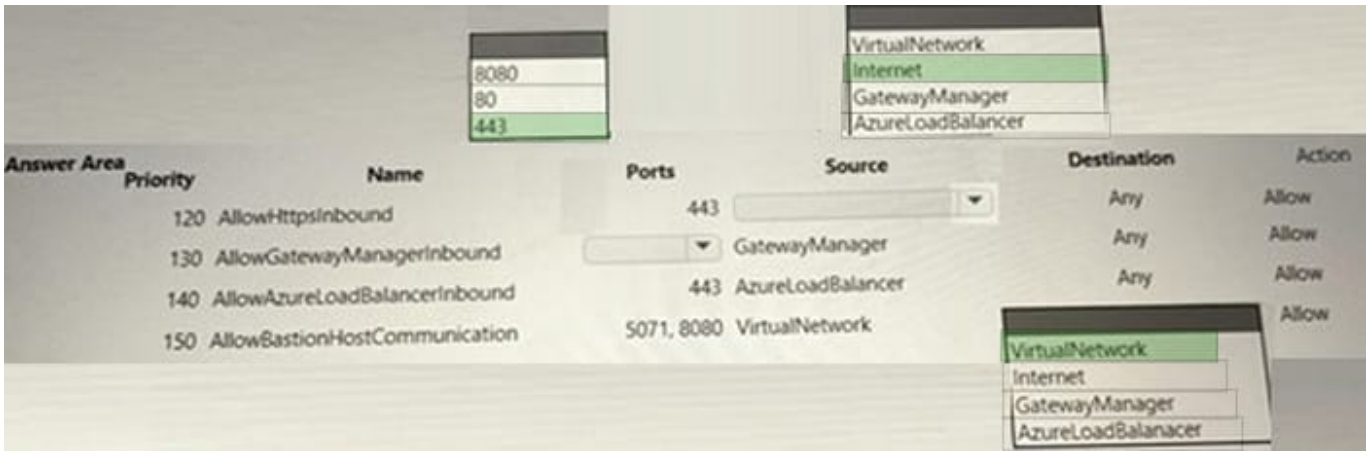
You need to fix the inbound rules for NSG1.

How should you complete the configuration?

Hot Area:



Correct Answer:



QUESTION 6

A company migrates an on-premises Windows virtual machine (VM) to Azure. An administrator enables backups for the VM by using the Azure portal.

The company reports that the Azure VM backup job is failing.

You need to troubleshoot the issue.

Solution: Create a new manual backup in Backup center.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: B

It is unlikely that creating a new manual backup in Backup center would resolve the issue of an Azure VM backup job failing after enabling backups for the VM through the Azure portal. To troubleshoot the issue, the administrator should

first

check the Azure VM backup job logs and identify the specific error message or code provided. This can help identify the underlying issue and the appropriate solution. Therefore, the solution mentioned in the question is incorrect and the

answer is B. No.

Reference:

Troubleshoot Azure VM backup failures (Microsoft documentation)

QUESTION 7

A company deploys a new file sharing application on four Standard_D2_v3 virtual machines (VMs) behind an Azure Load Balancer. The company implements Azure Firewall.

Users report that the application is slow during peak usage periods. An engineer reports that the peak usage for each VM is approximately 1 Gbps.

You need to implement a solution that support a minimum of 10 Gbps.

What should you do to increase the throughput?

A. Request an increase in networking quotas.

B. Increase the size of the VM instance.

C. Disable the Azure Firewall and implement network security groups in its place.

D. Move two of the servers behind a separate load balancer and configure round robin routing in Traffic Manager.

Correct Answer: B

According to the given scenario, the application deployed on four Standard_D2_v3 virtual machines behind an Azure Load Balancer is experiencing slow performance during peak usage periods It is reported that the peak usage for each VM is approximately 1 Gbps, and the goal is to increase the throughput to a minimum of 10 Gbps. To achieve this goal, the best option is to increase the size of the VM instance. The Standard_D2_v3 virtual machine size has a maximum network bandwidth of 1 Gbps, so increasing the size of the VM instance to a higher tier, such as Standard_D8_v3 or higher, will provide more network bandwidth and improve the application\\'s performance. Option A, requesting an increase in networking quotas, may not be sufficient to achieve the required network bandwidth.

Option C, disabling the Azure Firewall and implementing network security groups, may not have a significant impact on the network bandwidth. Option D, moving two of the servers behind a separate load balancer and configuring round-robin

routing in Traffic Manager, may improve availability and performance but will not increase the network bandwidth.

Source:

[1] https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes-general

[2] https://docs.microsoft.com/en-us/azure/virtual-network/designing-hub-spoke-topologies#optimize-data-transfer-between-hub-and-spoke-vnets

QUESTION 8

HOTSPOT

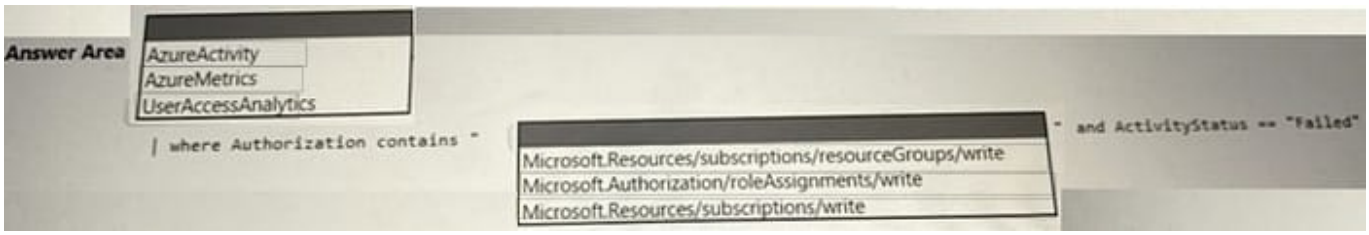
A company uses Azure Active Directory (Azure AD) with Azure role-based access control (RBAC) for access to resources.

Some users report that they are unable to grant RBAC roles to other users.

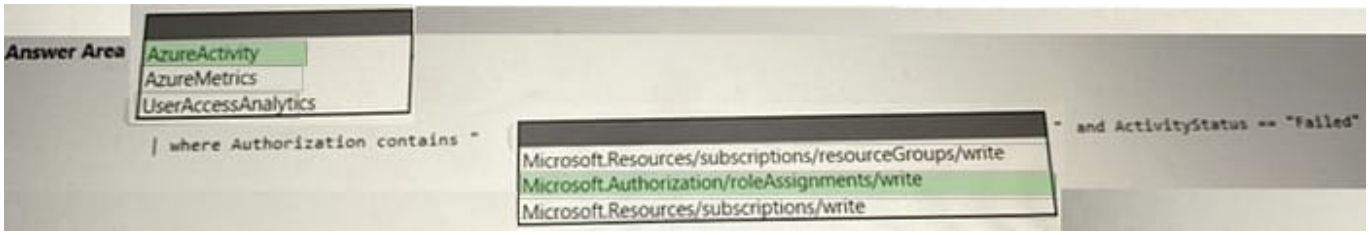
You need to troubleshoot the issue.

How should you complete the Azure Monitor query?

Hot Area:



Correct Answer:



QUESTION 9

A company configures an Azure site-to-site VPN between an on-premises network and an Azure virtual network.

The company reports that after completing the configuration, the VPN connection cannot be established.

You need to troubleshoot the connection issue.

What should you do first?

A. Identify the shared key by running this PowerShell cmdlet: Get-AzVirtualNetworkGatewayConnectionSharedKey.

B. Identify the shared key by running this PowerShell cmdlet: Get-AzVirtualNetworkGatewayConnectionVpnDeviceConfigScript.

C. Verify the AzureRoot.cer file exists.

D. Verify the AzureClient.pfx file exists.

Correct Answer: A

To troubleshoot the connection issue, you should do first identify the shared key by running this PowerShell cmdlet: Get-AzVirtualNetworkGatewayConnectionSharedKey. According to 1, this cmdlet returns the shared key that is used for

authentication between an Azure virtual network gateway and a local network gateway. You can use this cmdlet to verify that the shared key matches on both sides of the VPN connection.

Therefore, you should choose A. Identify the shared key by running this PowerShell cmdlet:

Get-AzVirtualNetworkGatewayConnectionSharedKey.

QUESTION 10

A company uses Azure virtual machines (VMs) in multiple regions. The VMs have the following configuration:

Server name	Resource group	Availability set	Virtual network	Region
VM1	RG1	AVSet1	VNet1	East US
VM2	RG1	AVSet1	VNet1	East US
VM3	RG3	N/A	VNet2	East US 2

The backend pool of an internal Azure Load Balancer (ILB) named ILB1 contains VM1 and VM2. The ILB uses the Basic SKU and is in a resource group RG2.

Virtual network peering has been configured between VNet1 and VNet2.

Users report that they are unable to connect to resources on VM1 and VM2 by using ILB1 from VM3.

You need to resolve the connectivity issues.

What should you do?

A. Redeploy VM1 and VM2 into availability zones.

B. Move ILB1 to RG1.

C. Redeploy the ILB using the Standard SKU.

D. Move VM1 and VM2 into RG3.

Correct Answer: C

To resolve the connectivity issues, you need to redeploy the ILB using the Standard SKU. According to 1, Basic Load Balancer does not support Global VNet Peering, which is required for cross-region communication between VMs in different VNets. Standard Load Balancer supports Global VNet Peering and can load balance traffic across regions and availability zones.

QUESTION 11

HOTSPOT

A company named Contoso connects its on-premises resources to Azure by using ExpressRoute.

An administrator reports that the circuit is in a failed state.

You need to resolve the issue.

How should you complete the PowerShell commands?

Hot Area:

Correct Answer:

QUESTION 12

A company uses Azure AD Connect. The company plans to implement self-service password reset (SSPR).

An administrator receives an error that password writeback cloud not be enabled during the Azure AD Connect configuration. The administrator observes the following event log error:

Error getting auth token

You need to resolve the issue.

Solution: Use a global administrator account with a password that is less than 256 characters to configure Azure AD Connect.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: B

No, restarting the Azure AD Connect service would not resolve the issue described in the scenario. The error message "Error getting auth token" indicates there is a problem with authentication

, which is preventing password writeback from being enabled during the Azure AD Connect configuration.

To resolve this issue, you should first confirm that the Azure AD Connect server can authenticate to the Azure AD tenant by using a valid set of credentials. If authentication is successful, then you can investigate other possible causes such

as network connectivity issues, misconfigured firewall rules, expired certificates, etc.

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

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/tshoot-connect-authentication

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/tshoot-connect-password-writeback#troubleshooting-steps

---

QUESTION 13

A company has an Azure Active Directory (Azure AD) tenant. The company provisions an Azure Active Directory Domain Services (Azure AD DS) instance.

Users report that they are unable to sign into Azure AD DS after being provisioned from Azure AD. You verify the user accounts exist in Azure AD DS.

You need to resolve the issue.

What should you do?

A. Delete the Azure application named AzureActiveDirectoryDomainControllerServices and then enable Azure AD DS again.

B. Deploy Azure AD Connect.

C. Delete the Azure application named Azure AD Domain Services Sync and then enable Azure AD DS again.

D. Instruct the users to change their password in Azure AD.

Correct Answer: D

Azure AD doesn\\'t generate or store password hashes in the format that\\'s required for NTLM or Kerberos authentication until you enable Azure AD DS for your tenant. Therefore, Azure AD can\\'t automatically generate these NTLM or Kerberos password hashes based on users\\' existing credentials. For cloud-only environments with no on-premises synchronization, you need to instruct users to change their password in Azure AD after enabling Azure AD DS. This will generate the required password hashes and sync them to Azure AD DS within 20 minutes.

QUESTION 14

HOTSPOT

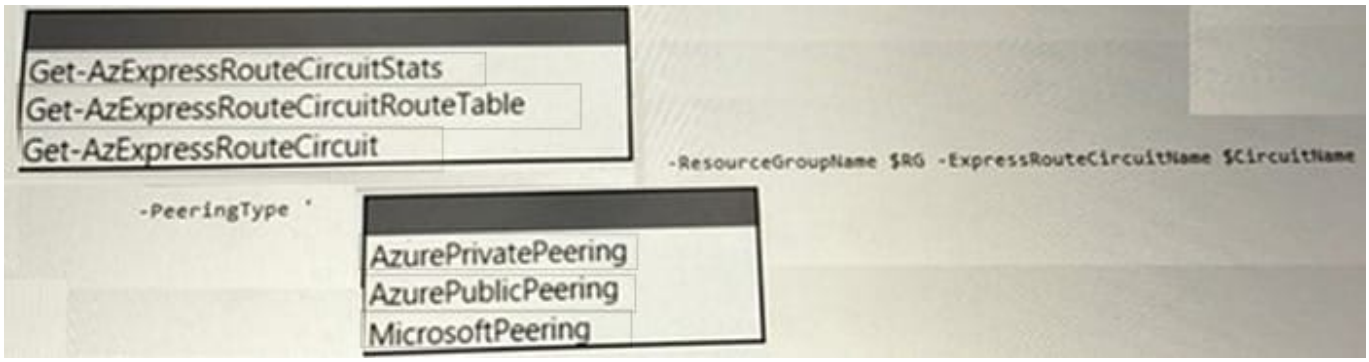
A company connects an on-premises network to an Azure virtual network by using ExpressRoute.

The ExpressRoute connection is experiencing higher than normal latency.

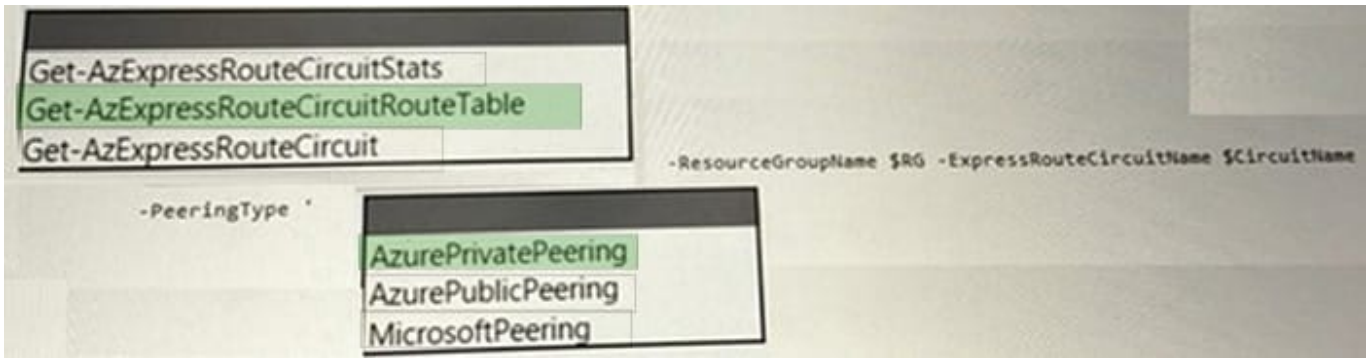
You need to confirm the traffic flow.

How should you complete the PowerShell command?

Hot Area:



Correct Answer:



QUESTION 15

A company has an Azure point-to-site virtual private network (VPN) that uses certificate- based authentication.

A user reports that the following error message when they try to connect to the VPN by using a VPN client on a Windows 11 machine:

1.

A certificate could not be found

2.

You need to resolve the issue. Which three actions should you perform?

A. Configure an Azure Active Directory (Azure AD) tenant.

B. Install a root certificate on the user\\'s device.

C. Generate a root certificate.

D. Install a client certificate on the VPN gateway.

E. Enable Azure AD authentication on the gateway

F. Generate a client certificate.

G. Install a client certificate on the user\\'s device.

Correct Answer: BFG

AZ-720 Study Guide AZ-720 Exam Questions AZ-720 Braindumps