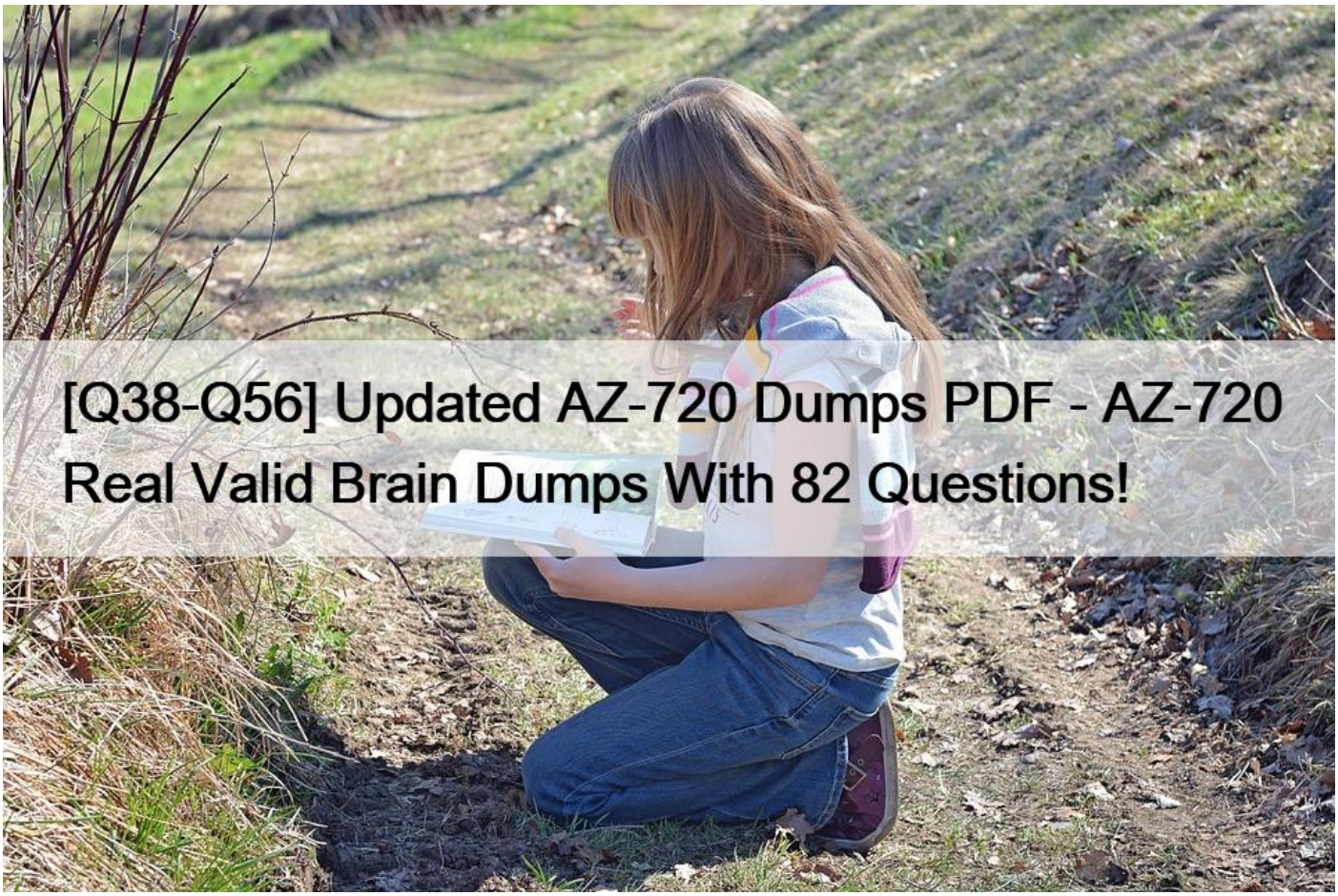
# [Q38-Q56 Updated AZ-720 Dumps PDF - AZ-720 Real Valid Brain Dumps With 82 Questions!

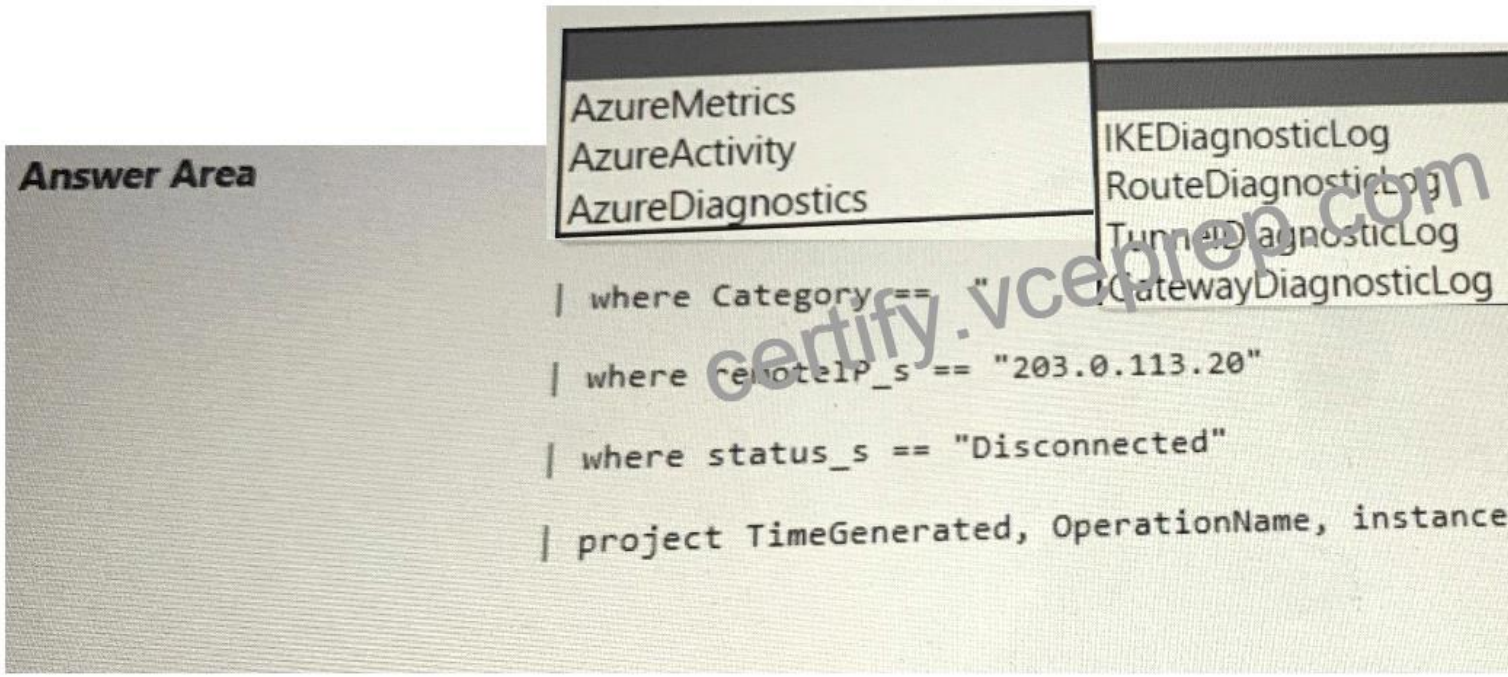


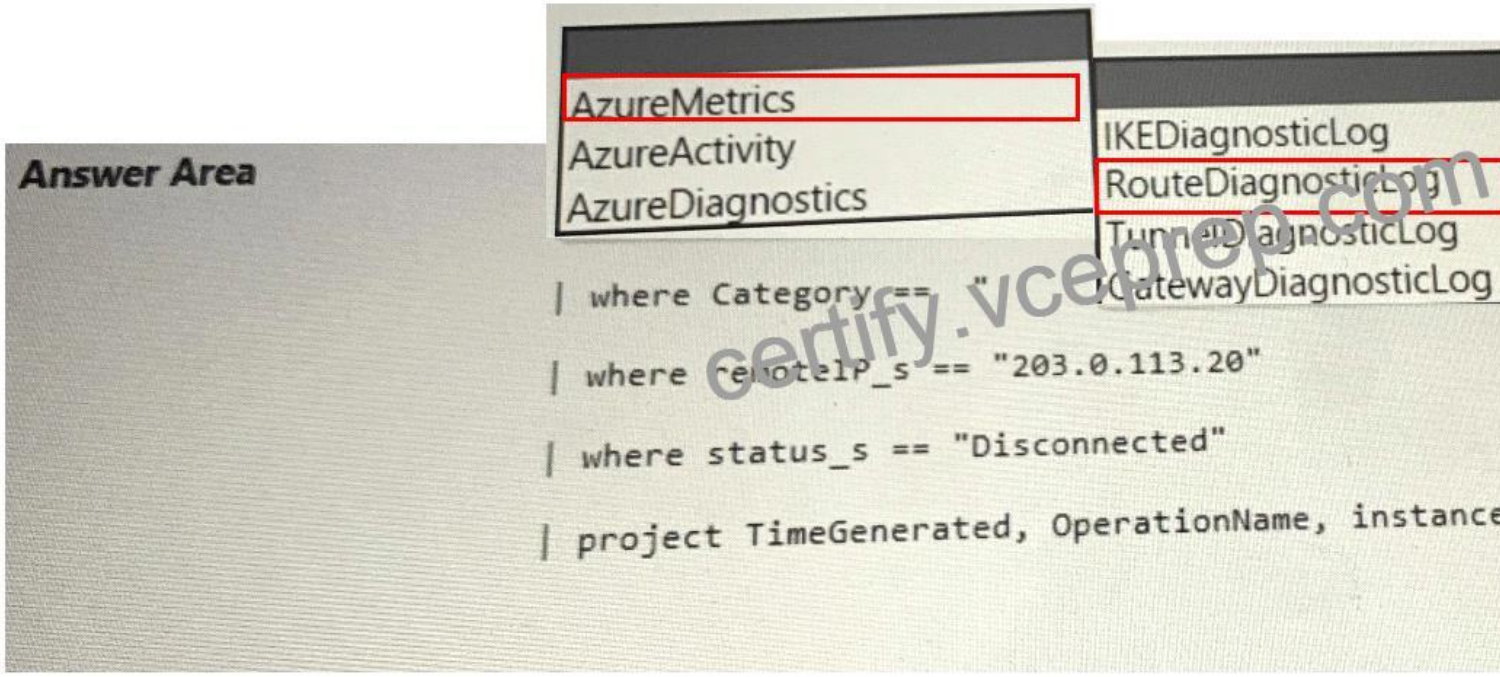

**Updated AZ-720 Dumps PDF - AZ-720 Real Valid Brain Dumps With 82 Questions! 100% Free AZ-720 Exam Dumps Use Real Microsoft Certified: Azure Support Engineer for Connectivity Specialty Dumps NO.38** A company uses an Azure VPN gateway with an IP address of 203.0.113.20.

Users report that the VPN connection frequently drops.

You need to determine when each connection failure occurred.

How should you complete the Azure Monitor query?




**NO.39** 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.

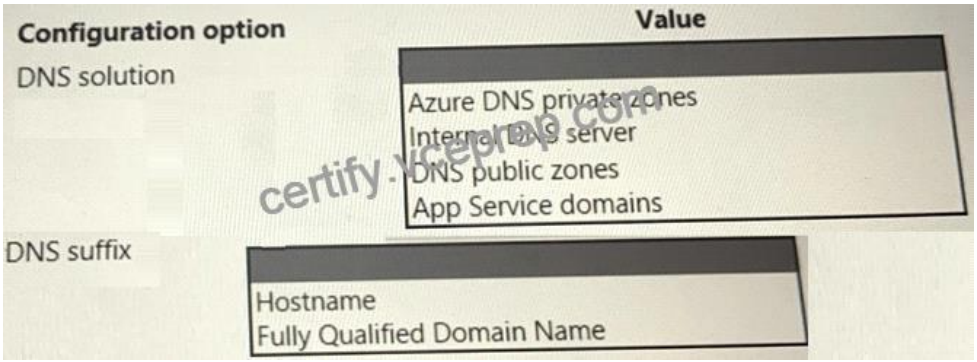
Does the solution meet the goal?
* Yes
* No

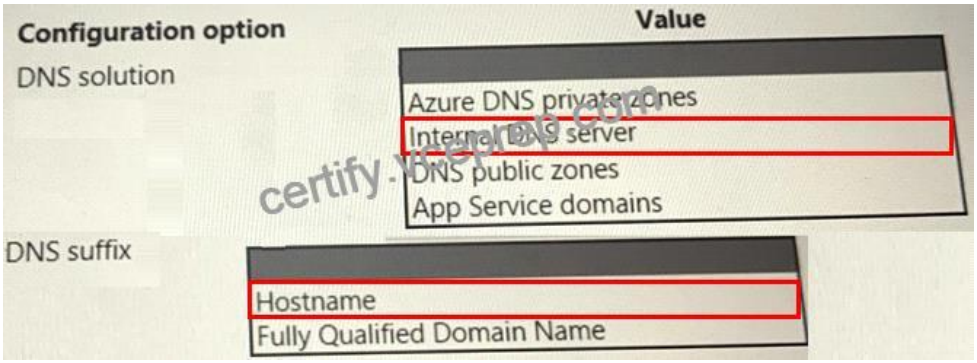
**NO.40** A company has an Azure environment that uses one virtual network.

The company restructures the environment to use two different virtual networks. Virtual machines in one network cannot communicate with virtual machines in the other virtual network.

You need to re-establish a connection between virtual machines in the two networks.

How should you configure the networks?



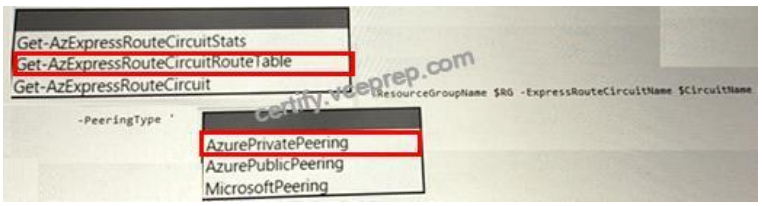




**NO.41** A company connects an on-premises network to an Azure virtual network by using ExpressRoute.

The ExpressRoute connection is experiencing higher than normal latency.

You need to confirm the traffic flow.

How should you complete the PowerShell command?




**NO.42** 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?



**NO.43** A company plans to use an Azure PaaS service by using Azure Private Link service. The azure Private Link service and an endpoint have been configured.

The company reports that the endpoint is unable to connect to the service.

You need to resolve the connectivity issue.

What should you do?
* Disable the endpoint network policies.
* Validate the VPN device.
* Approve the connection state.
* Disable the service network policies.

**NO.44** A company has an Azure tenant. The company deploys an Azure Firewall named FW1 using the Standard

SKU. You configure FW1 using classic firewall rules.

The company creates an application rule collection with the following settings:

Priority: 100

Action: Deny

Rule type: FQDN

Source type: IP address

Source: *

Protocol: http:80,https:443

Target FQDN: *.cloud.contoso.com

An engineer observes that traffic to console.cloud.conotoso.com is still allowed by FW1.

You need to determine why the traffic is allowed.

What should you review?
* Network rules
* Web categories
* Infrastructure rules
* Application rules

**NO.45** A company uses an Azure VPN gateway to connect to their on-premises environment.

The company’s on-premises VPN gateway is used by several services. One service is experiencing

connectivity issues.

You need to minimize downtime for all services and resolve the connectivity issue.

Which three actions should you perform?
* Configure the hashing algorithm to be different on both gateways.
* Rest the VPN gateway.
* Configure the pre-shared key to be the same on the Azure VPN gateway and the on-premises VPN

gateways.
* Rest the VPN connection.
* Configure the hashing algorithm to be the same on both gateways.
* Configure the pre-shared key to be different on the Azure VPN gateway and the on-premises VPN gateways.

**NO.46** A company implements Azure Firewall and deploys an Azure Firewall policy.

The policy incudes multiple application and network rules for the company’s infrastructure. After deployment,

an application is not accessible from on-premises computers.

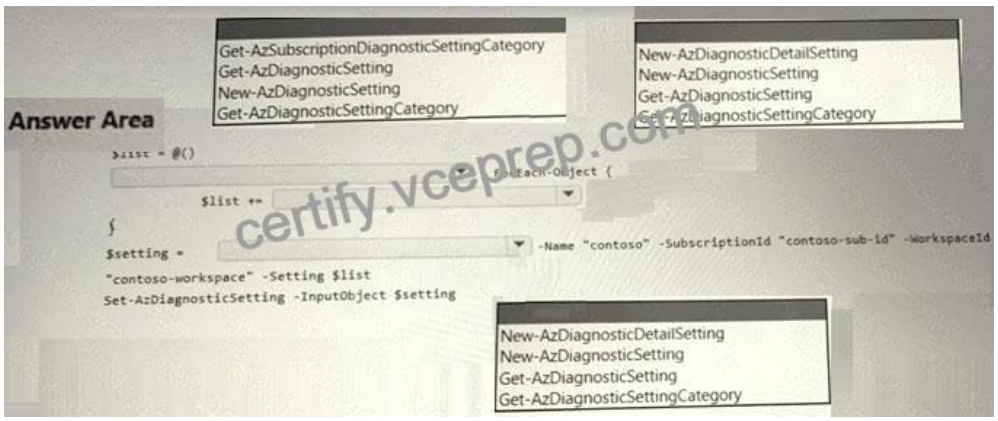
You need to enable diagnostic logging for the following settings:

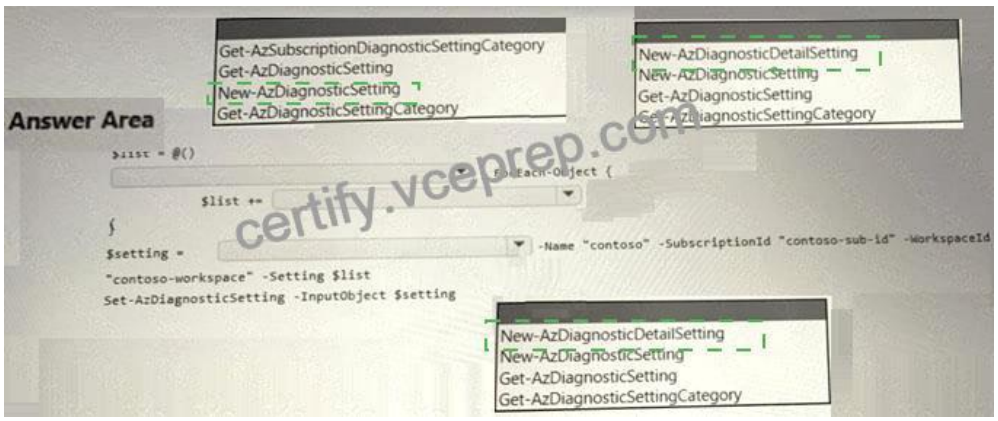
* AzureFirewallApplicationRule

* AzureFirewallNetworkRule

* AzureFirewallDnsProxy

How should you complete the PowerShell cmdlet?




**NO.47** A company enables just-in-time (JIT) virtual machine (VM) access in Azure.

An administrator observes a list of VMs on the Unsupported tab of the JIT VM access page in the Microsoft

Defender for Cloud portal.

You need to determine why some VMs are not supported for JIT VM access.

What should you conclude?
* The administrator does not have the SecurityReader role.
* The administrator is using the Microsoft Defender for Cloud free tier.
* The client firewall does not allow port 22 on the VMs.
* A network security group is not associated with the VMs.

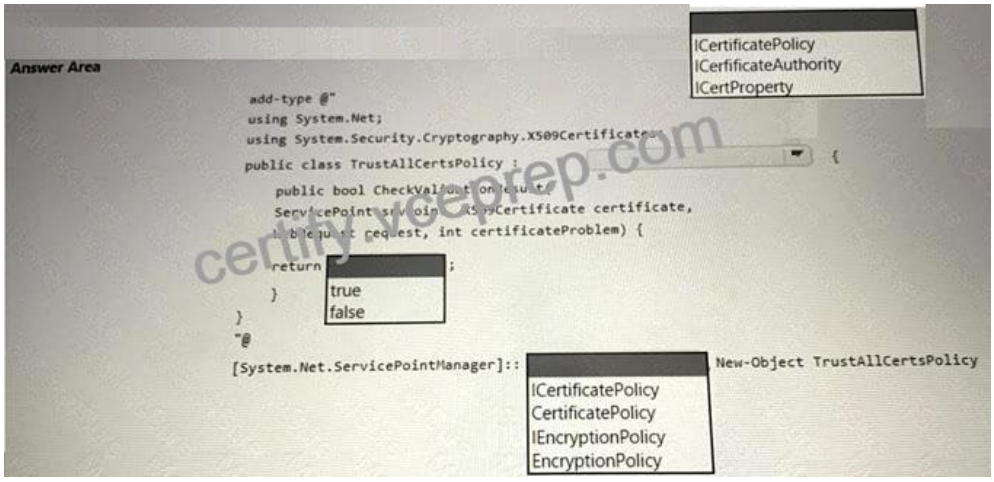
**NO.48** A company deploys Azure Traffic Manager load balancing for an Azure App Service solution.

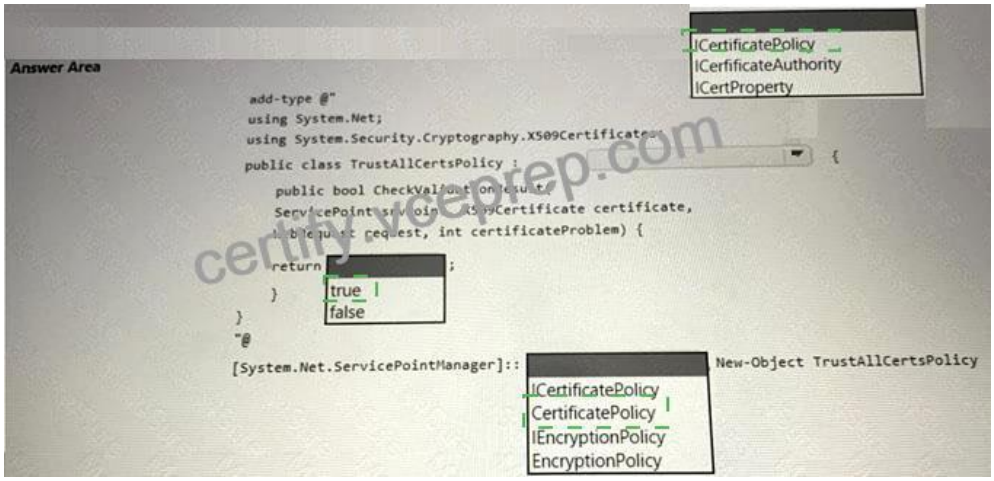
Load balancing performance is showing a degraded status after deployment, and new HTTPS probes are

failing to reach the Traffic Manager endpoints.

You need to troubleshoot the probe failure.

How should you complete the PowerShell script?




**NO.49** 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?
* Identify the shared key by running this PowerShell cmdlet:

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

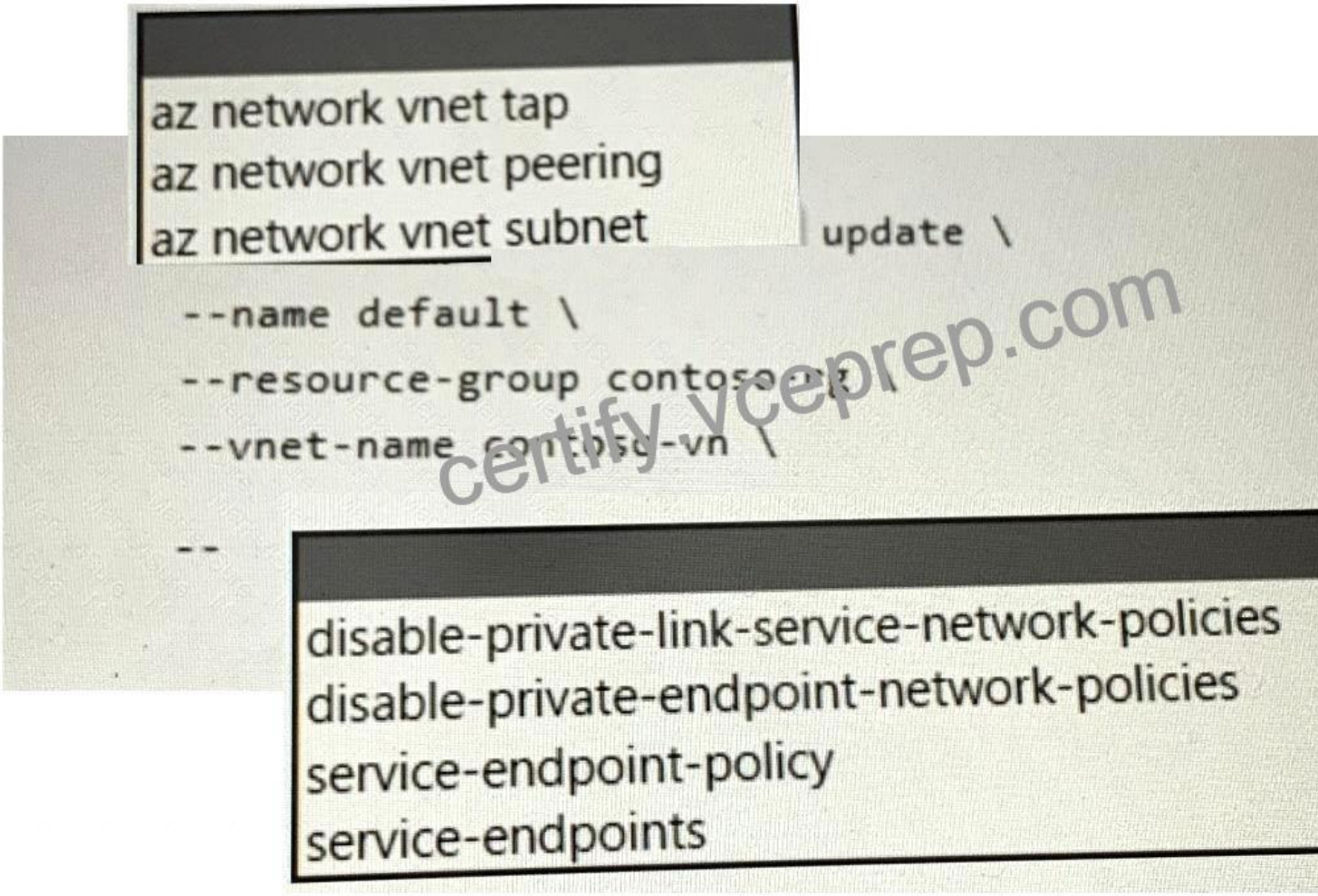
Get-AzVirtualNetworkGatewayConnectionVpnDeviceConfigScript.
* Verify the AzureRoot.cer file exists.
* Verify the AzureClient.pfx file exists.

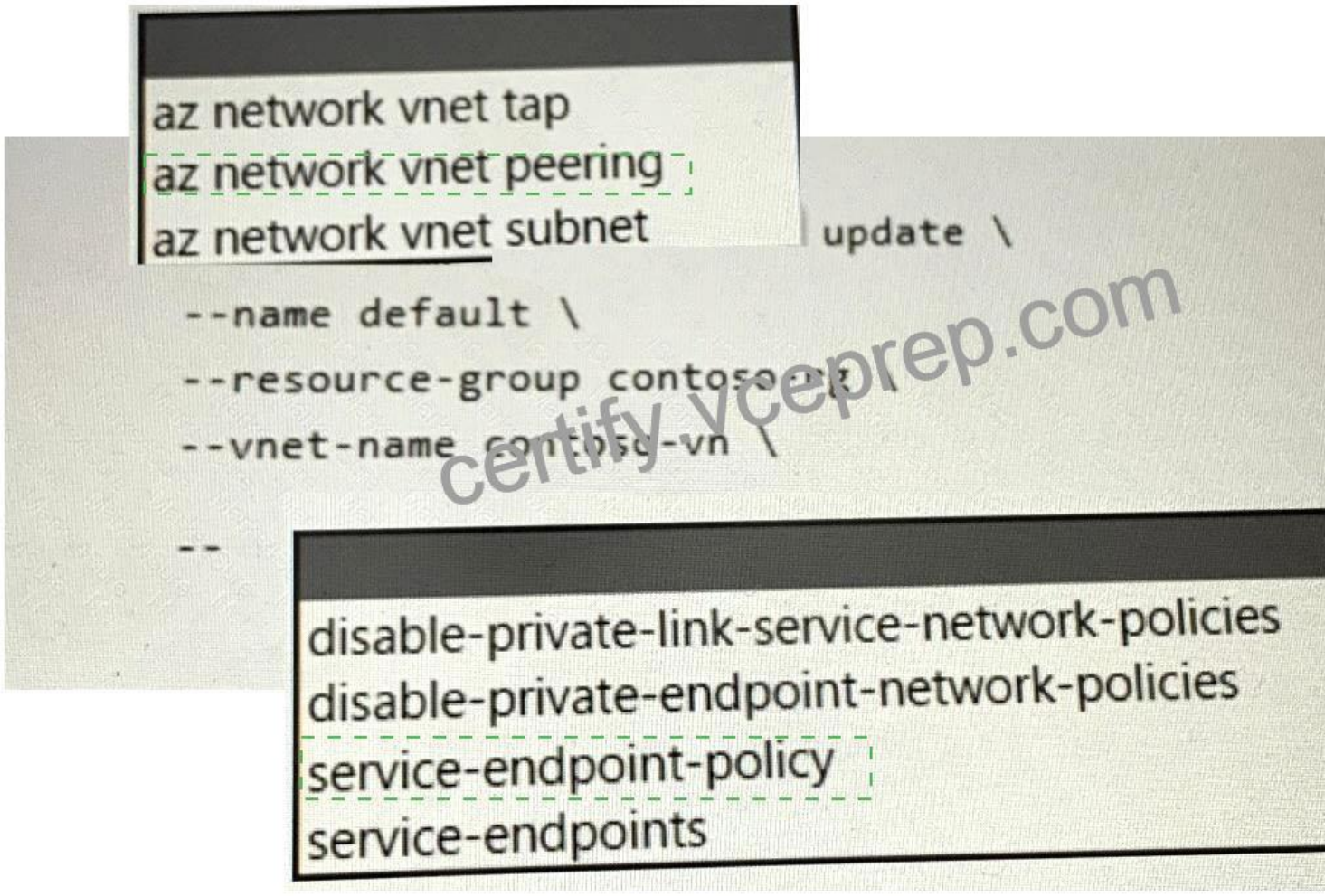
**NO.50** A company named Contoso connects to Azure PaaS services using Azure Private Link. The company has a virtual network named contoso-vn in a resource group named contoso-rg.

An engineer modifies the Private Link service by using Azure CLI. They are unable to use a source IP address from a subnet named default.

You need to resolve the issue.

How should you complete the command?








**NO.51** 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?

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

* Enable FlowLog1 in a network security group associated with the subnet of VM1.
* Configure the FlowTimeoutInMinutes property on VNet1 to a non-null value.

**NO.52** 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?
* Yes
* No

**NO.53** 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?
* Request an increase in networking quotas.
* Increase the size of the VM instance.
* Disable the Azure Firewall and implement network security groups in its place.
* Move two of the servers behind a separate load balancer and configure round robin routing in Traffic Manager.

**NO.54** A company creates an Azure resource group named RG1. RG1 has an Azure SQL Database logical server named sqlsvr1 that hosts the following resources:

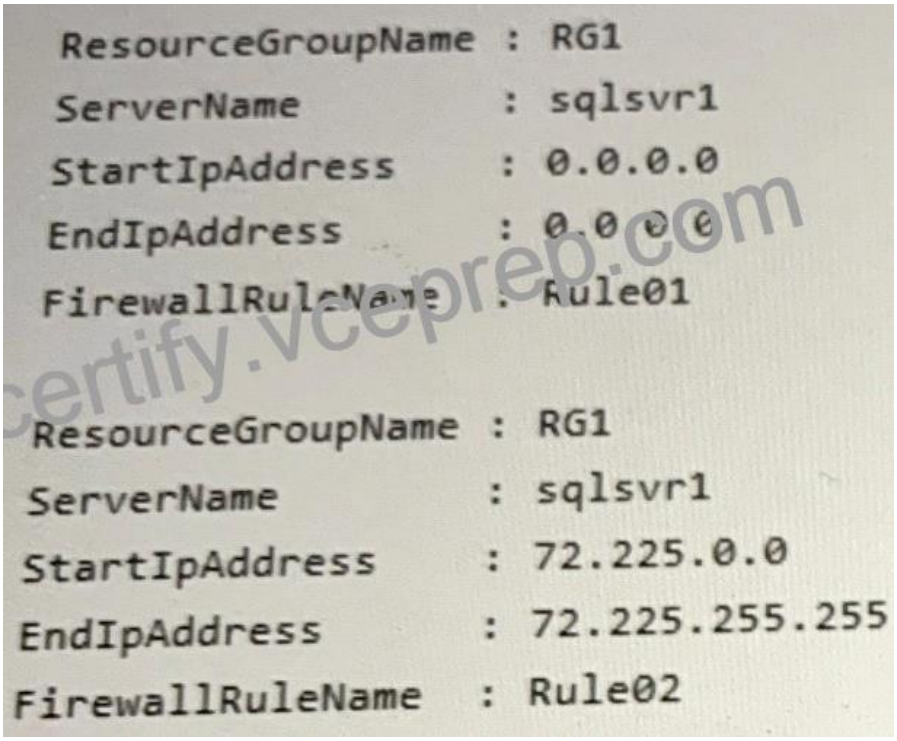
| Resource | Description |
|---|---|
| VM1 | Virtual machine |
| SQLDB1 | Azure SQL database |
| SQLDB2 | Azure SQL database |

An administrator grants a user named User1 the Reader RBAC role in RG1. The administrator grants User2 the Contributor role in sqlsvr1.

User1 reports that they can connect to SQLDB1 from the IP address 155.127.95.212. User1 cannot connect to SQLDB2. User2 can connect to both SQLDB1 and SQLDB2 from the IP address 121.19.27.18. Both users can successfully connect to SQLDB1 and SQLDB2 from VM1.

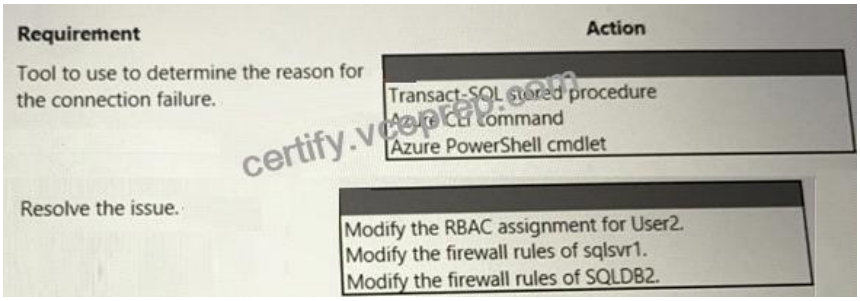
You are helping the administrator troubleshoot the issue. You run the following PowerShell command:

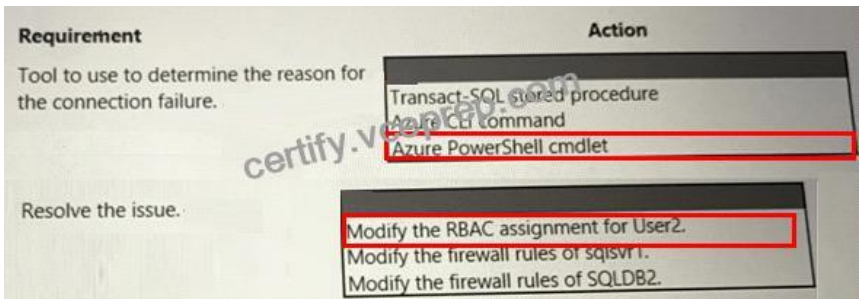
Get-AzSqlServerFirewallRule -ResourceGroupName ‘RG1’ -ServerName ‘sqlsvr1’ The following output displays:




You need to identify the cause for the reported issue and resolve User1’s issues. The solution must satisfy the principle of least privilege.

What should you do?






**NO.55** A company uses Azure Site Recovery (ASR) to replicate and recover Azure virtual machines (VM) between Azure regions.

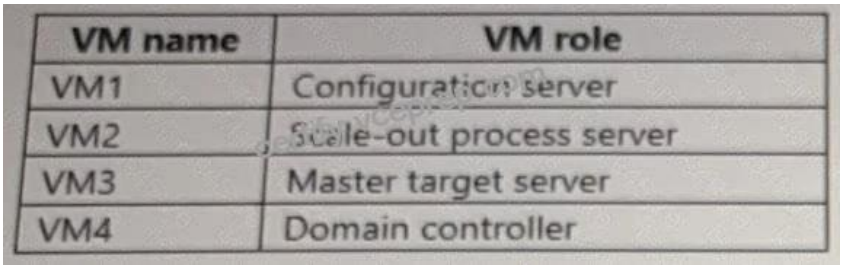
An administrator receives the following warning from ASR about a VM that uses P10 disks: Data change rate beyond supported limits You add OS Disk Write Bytes/Sec and Data Disk Write Bytes/Sec to the list of metrics for monitoring. You discover that the VM consistently has a data churn of greater than 8 MB/s but less than 10 MB/s.

You need to resolve the issue.

What should you do?
* Uninstall the Volume Shadow Copy Service (VSS) Provider service.
* Use AzCopy to upload data to a cache storage account.
* Create a network service endpoint in a virtual network.
* Upgrade the target storage disk.

**NO.56** A company uses Azure Site Recovery (ASR) for a VMware environment that includes the following virtual

machines (VMs):




The company reports that they are unable to configure all of the servers for replication.

You need to evaluate the servers and server roles to determine which servers can be protected.

Which server can you protect by using ASR?
* VM1
* VM2
* VM3
* VM4

**Pass Your AZ-720 Exam Easily With 100% Exam Passing Guarantee:** https://www.vceprep.com/AZ-720-latest-vce-prep.html]