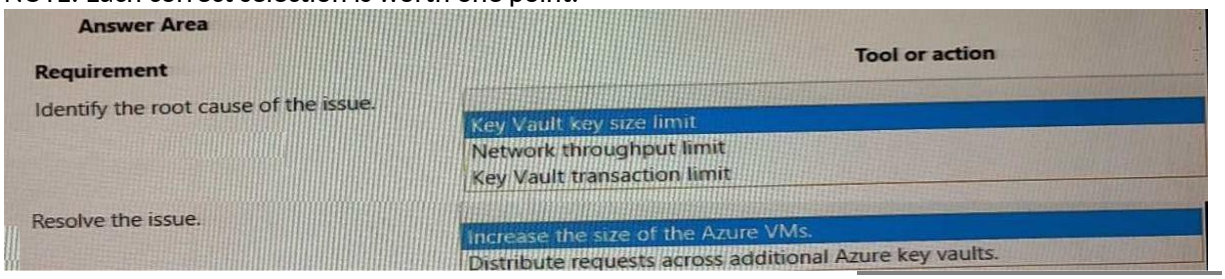
AZ-720 Demo

Question: 1

HOTSPOT
You need to troubleshoot the Azure Key Vault issues.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

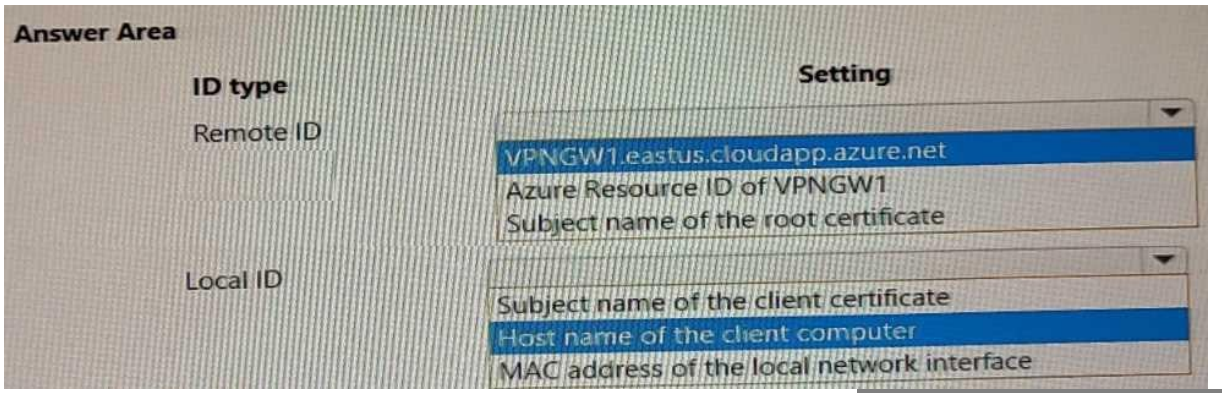
Explanation:
Box 1: Key Vault transaction limit.
Based on the given scenario, the issue is related to the number of transactions per second (TPS) being throttled. The Azure Key Vault has a transaction limit, which varies depending on the service tier. In the provided images, the error message states that the request rate is too large, indicating that the transaction limit has been reached. To resolve this issue, you can either distribute the transactions over a longer period, implement a retry policy, or consider upgrading to a higher service tier if the current tier's transaction limit is insufficient for your needs. Reference: https://docs.microsoft.com/en-us/azure/key-vault/general/service-limits

Box : 2 Distribute requests across additional Azure Key vaults

In the provided scenario, the issue is that the Azure Key Vault is experiencing throttling due to too many requests per second. Throttling occurs when the number of requests exceeds the allowed limits for a given time period. To resolve this issue, you should distribute the requests across additional Azure Key Vaults. By doing so, you can balance the load and prevent exceeding the request limits, thus avoiding throttling. Reference: https://docs.microsoft.com/en-us/azure/key-vault/general/overview-throttling

Question: 2

HOTSPOT
You need to troubleshoot the sales department issues.
How should you configure the system? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Box 1: Subject name of the root certificate.

This is the value that should be configured as the system Remote ID for the VPN client on the sales department devices. The system Remote ID is used to identify the VPN server that the client is connecting to, and it must match the value that is configured on the VPN gateway in Azure. For Azure VPN Gateway, the system Remote ID is the subject name of the root certificate that is used for authentication1. Therefore, option C is correct.
A detailed explanation with references is as follows:
As mentioned in the scenario, the sales department devices are using Point-to-Site VPN connections to access Azure resources. A Point-to-Site VPN connection lets you create a secure connection to your virtual network from an individual client computer2. To configure a Point-to-Site VPN connection, you need to create a virtual network gateway of type VPN in Azure, and then install a VPN client on each device that needs to connect2. The VPN client configuration includes several settings, such as the VPN server address, the tunnel type, and the authentication method. One of these settings is the system Remote ID, which is used to identify the VPN server that the client is connecting to1. The system Remote ID must match the value that is configured on the VPN gateway in Azure, otherwise the connection will fail.
For Azure VPN Gateway, there are three authentication methods available for Point-to-Site VPN connections: certificate-based authentication, OpenVPN with Azure AD authentication, and OpenVPN with certificate-based authentication2. For certificate-based authentication, which is used in this scenario, the system Remote ID is the subject name of the root certificate that is used for authentication1. The root certificate is uploaded to Azure when creating a Point-to-Site VPN connection, and it must be installed on each device that needs to connect2. The subject name of the root certificate can be obtained by using PowerShell or OpenSSL commands1. For example, using PowerShell:
$cert = Get-ChildItem -Path Cert:\CurrentUser\My | Where-Object {$_.Subject -
like “ContosoRootCert”} $cert.Subject
The output of this command will show the subject name of the root certificate that matches ContosoRootCert. This value should be configured as the system Remote ID for the VPN client on each device.

Box 2: Subject name of the client certificate

In the provided scenario, the sales department is using a VPN to connect to the corporate network,

and the VPN server is configured to use certificate-based authentication. To troubleshoot the sales department issues, you should configure the system Local ID to use the subject name of the client certificate. The subject name of a client certificate uniquely identifies the client and is used during the certificate-based authentication process. This allows the VPN server to verify the client's identity and grant access to the corporate network.
This is the value that should be configured as the system Local ID for the VPN client on the sales department devices. The system Local ID is used to identify the VPN client that is connecting to the VPN server, and it must match the value that is configured on the VPN gateway in Azure. For Azure VPN Gateway, the system Local ID is the subject name of the client certificate that is used for authentication1. Therefore, option A is correct.
A detailed explanation with references is as follows:
As mentioned in the scenario, the sales department devices are using Point-to-Site VPN connections to access Azure resources. A Point-to-Site VPN connection lets you create a secure connection to your virtual network from an individual client computer2. To configure a Point-to-Site VPN connection, you need to create a virtual network gateway of type VPN in Azure, and then install a VPN client on each device that needs to connect2. The VPN client configuration includes several settings, such as the VPN server address, the tunnel type, and the authentication method. One of these settings is the system Local ID, which is used to identify the VPN client that is connecting to the VPN server1. The system Local ID must match the value that is configured on the VPN gateway in Azure, otherwise the connection will fail.
For Azure VPN Gateway, there are three authentication methods available for Point-to-Site VPN connections: certificate-based authentication, OpenVPN with Azure AD authentication, and OpenVPN with certificate-based authentication2. For certificate-based authentication, which is used in this scenario, the system Local ID is the subject name of the client certificate that is used for authentication1. The client certificate is generated from a root certificate that is uploaded to Azure when creating a Point-to-Site VPN connection, and it must be installed on each device that needs to connect2. The subject name of the client certificate can be obtained by using PowerShell or OpenSSL commands1. For example, using PowerShell:
$cert = Get-ChildItem -Path Cert:\CurrentUser\My | Where-Object {$_.Subject -
like “ContosoClientCert”} $cert.Subject
The output of this command will show the subject name of the client certificate that matches ContosoClientCert. This value should be configured as the system Local ID for the VPN client on each device.

Question: 3

You need to troubleshoot the CosmosDB1 issues from the on-premises environment. What should you use?

A. route command
B. Network Watcher next hop diagnostic tool
C. Network Watcher Connection troubleshoot diagnostic tool
D. nslookup command

Answer: C

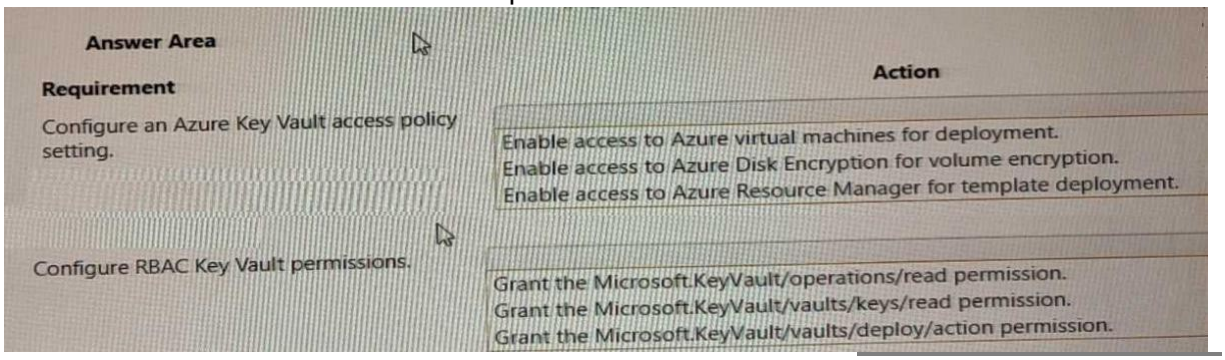
Explanation:

This tool helps you troubleshoot network connectivity issues from a virtual machine to a given endpoint. It tests for reachability from the virtual machine to the endpoint and provides information

about why a connection fails1. In this case, you can use this tool to troubleshoot the connectivity issues from the on-premises environment to CosmosDB1.

Question: 4

HOTSPOT
You need to resolve the Azure virtual machine (VM) deployment issues.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

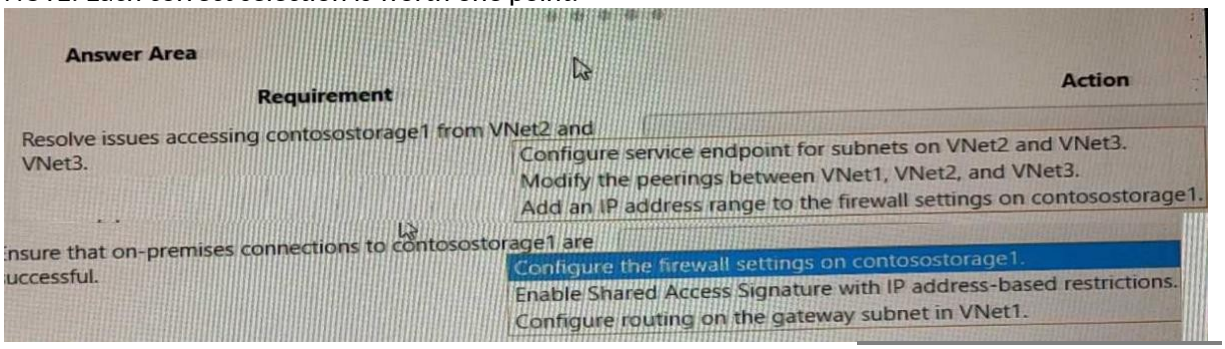
Explanation:
Box 1: Enable access to Azure Resource Manager for template deployment.
In the given scenario, you are trying to resolve Azure VM deployment issues. To configure an Azure Key Vault access policy setting for VM deployment, you need to enable access to Azure Resource Manager for template deployment. This will allow the VM deployment process to access the secrets and certificates stored in the Key Vault during the deployment of the VM using an ARM (Azure Resource Manager) template. Reference: - https://docs.microsoft.com/en-us/azure/key-vault/general/tutorial-net-create-vault-azure-web-app
BoX 2: Grant the Microsoft.KeyVault/vaults/deploy/action permission

This is the permission that you should configure on an RBAC Key Vault role to resolve the Azure virtual machine (VM) deployment issues. This permission allows Azure Resource Manager to retrieve secrets from the key vault when deploying resources using an ARM template1. Therefore, option C is correct.
A detailed explanation with references is as follows:
As mentioned in the scenario, the Azure virtual machine (VM) deployment issues are caused by the inability of Azure Resource Manager to retrieve secrets from the key vault when deploying resources using an ARM template. To resolve this issue, you need to configure an RBAC Key Vault role that grants Azure Resource Manager the permission to access the key vault.
RBAC Key Vault roles are roles that can be assigned to users, groups, or applications to manage access to key vault secrets, keys, and certificates2. RBAC Key Vault roles are based on Azure role-based access control (Azure RBAC), which is an authorization system that provides fine-grained access management of Azure resources3. With Azure RBAC, you can control access to resources by creating role assignments, which consist of three elements3:
The security principal: The user, group, or application that you want to grant or deny access to the

resource.
The role definition: The predefined or custom set of permissions that you want to grant or deny on the resource. For example, read, write, delete, backup, restore, etc.
The scope: The level at which you want to apply the role assignment. For example, at the management group, subscription, resource group, or individual resource level.
To configure a role assignment that allows Azure Resource Manager to retrieve secrets from the key vault when deploying resources using an ARM template, you need to grant the Microsoft.KeyVault/vaults/deploy/action permission1. This is a special permission that grants Azure Resource Manager a limited permission to get secrets from the key vault during resource deployment1. This permission does not grant any other permissions to Azure Resource Manager on the key vault or its contents1.
To grant the Microsoft.KeyVault/vaults/deploy/action permission using the Azure portal, follow these steps1:
In the Azure portal, navigate to the Key Vault resource.
Select Access control (IAM), then select Add > Add role assignment. Under Role, select a built-in or custom role that includes the Microsoft.KeyVault/vaults/deploy/action permission. For example, you can select Key Vault Administrator or Key Vault Secrets User.
Under Assign access to, select Azure AD user, group, or service principal.
Under Select, enter Azure Resource Manager in the search field and select it.
Select Save to create the role assignment.
To grant the Microsoft.KeyVault/vaults/deploy/action permission using the Azure CLI or PowerShell, see Grant permissions for template deployment.

Question: 5

HOTSPOT
You need to troubleshoot and resolve issues reported for contosostorage1.
What should you do? To answer, select the appropriate option in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Box 1: Configure service endpoint for subnet on VNet2 and VNet3.
This is what you should do to resolve issues accessing contosostorage1 from VNet2 and VNet3.
A service endpoint is a feature that enables you to secure your Azure Storage account to a specific virtual network subnet1.
As mentioned in the scenario, contosostorage1 is a storage account that has firewall and virtual network settings enabled. This means that only requests from allowed networks can access the

storage account2. By default, storage accounts accept connections from clients on any network, but you can configure firewall rules to allow or deny access based on the source IP address or virtual network subnet2.
In this scenario, you want to allow access to contosostorage1 from VNet2 and VNet3, which are peered with VNet1. To do this, you need to configure service endpoints for the subnets on VNet2 and VNet3 that need to access the storage account1. A service endpoint is a feature that enables you to secure your Azure Storage account to a specific virtual network subnet1. When you enable a service endpoint for a subnet, you can then grant access to the storage account only from that subnet1. This way, you can restrict access to your storage account and improve network performance by routing traffic through an optimal path.
To configure service endpoints for a subnet using the Azure portal, follow these steps1:
In the Azure portal, navigate to the Virtual Network resource.
Select Subnets, then select the subnet that needs to access the storage account.
Under Service endpoints, select Microsoft.Storage from the drop-down list.
Select Save to apply the changes.
To configure service endpoints for a subnet using the Azure CLI or PowerShell, see Enable a service endpoint.
After configuring service endpoints for the subnets on VNet2 and VNet3, you also need to grant access to contosostorage1 from those subnets. To do this, you need to modify the firewall rules on the storage account2.
To modify the firewall rules on the storage account using the Azure portal, follow these steps2:

In the Azure portal, navigate to the Storage Account resource.
Select Firewalls and virtual networks under Settings.
Under Allow access from selected networks, select Add existing virtual network.
Select the virtual network and subnet that have service endpoints enabled for Microsoft.Storage.
Select Add to save the changes.
To modify the firewall rules on the storage account using the Azure CLI or PowerShell, see Configure Azure Storage firewalls and virtual networks.

Box 2: Configure the firewall settings on contosostorage1.

Explanation: The issue reported is that on-premises connections to contosostorage1 are unsuccessful. The main reason for this could be that the firewall settings on the storage account are blocking the connections. By configuring the firewall settings on contosostorage1 to allow the on-premises IP addresses, you can ensure that the on-premises connections are successful.

As mentioned in the scenario, contosostorage1 is a storage account that has firewall and virtual network settings enabled. This means that only requests from allowed networks can access the storage account1. By default, storage accounts accept connections from clients on any network, but you can configure firewall rules to allow or deny access based on the source IP address or virtual network subnet1.
In this scenario, you want to allow access to contosostorage1 from the on-premises environment, which is connected to Azure using a Site-to-Site VPN connection. A Site-to-Site VPN connection lets you create a secure connection between your on-premises network and an Azure virtual network over an IPsec/IKE VPN tunnel2. To allow access to contosostorage1 from the on-premises environment, you need to configure the firewall settings on contosostorage1 to include the public IP address of your VPN device or gateway3.

To configure the firewall settings on contosostorage1 using the Azure portal, follow these steps[1]:

In the Azure portal, navigate to the Storage Account resource.
Select Firewalls and virtual networks under Settings.
Under Allow access from selected networks, select Add existing virtual network.
Select VNet1 and the subnet that has service endpoints enabled for Microsoft.Storage.
Under Firewall, enter the public IP address of your VPN device or gateway under Address Range.
Select Save to apply the changes.

To configure the firewall settings on contosostorage1 using the Azure CLI or PowerShell, see Configure Azure Storage firewalls and virtual networks.