DUMPSARENA

Troubleshooting Microsoft Azure Connectivity

Microsoft AZ-720

Version Demo

Total Demo Questions: 10

Total Premium Questions: 102

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Contoso Ltd, Case Study	12
Topic 2, Misc. Questions Set	90
Total	102

QUESTION NO: 1

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

ANSWER: B

Explanation:

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:

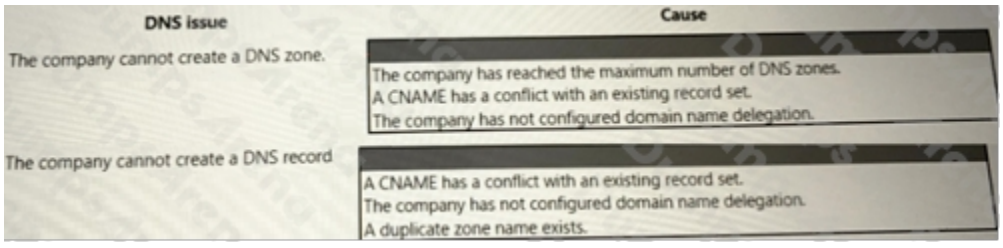
QUESTION NO: 2 - (HOTSPOT)

A company uses public Azure DNS zones.

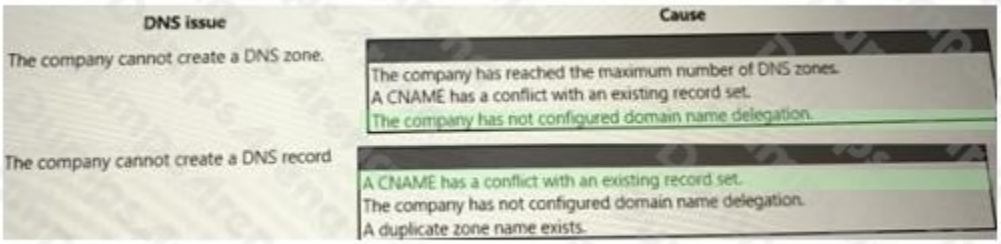
The company reports DNS record creation and name resolution issues.

You need to troubleshoot the issues.

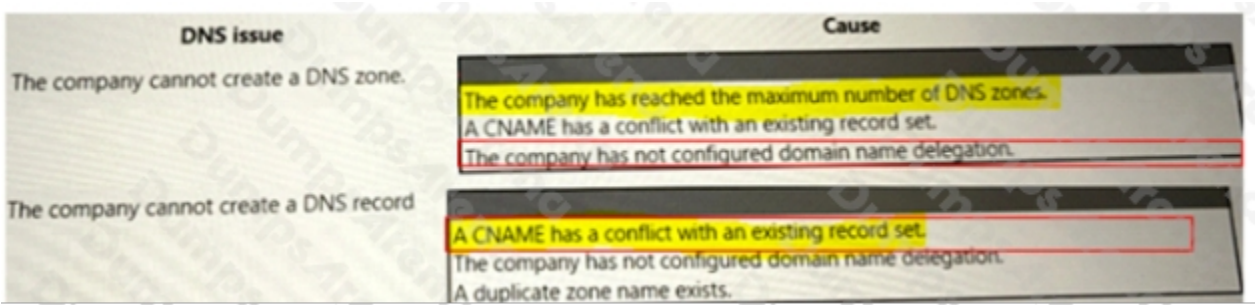
What are the causes of the issues?



ANSWER:



Explanation:



QUESTION NO: 3

A company has two virtual networks (VNets) that are configured to use peering. Several Azure virtual machines are connected to each network. An on-premises network is connected to one of the VNets by using Azure VPN Gateway.

An administrator reports that communication between applications across the VNets is failing.

You need to troubleshoot the issue.

Which two features can you use to achieve the goal?

A. IP flow verify

B. AzureNetworkWatchExtension

C. Next hop

D. Network Watcher topology

E. NSG flow logs

ANSWER: A C

Explanation:

According to Microsoft, you can use Network Watcher IP Flow Verify and NSG Flow Logging to determine whether there is a Network Security Group (NSG) or User-Defined Route (UDR) that is interfering with traffic flow1.

QUESTION NO: 4

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: Enable replication and create a recovery plan for the backup vault.

Does the solution meet the goal?

A. Yes

B. No

ANSWER: B

QUESTION NO: 5 - (DRAG DROP)

You manage an Azure point-to-site (P2S) VPN deployment. All users connect regularly from their personal Windows computer through a P2S VPN by using certificate-based authentication.

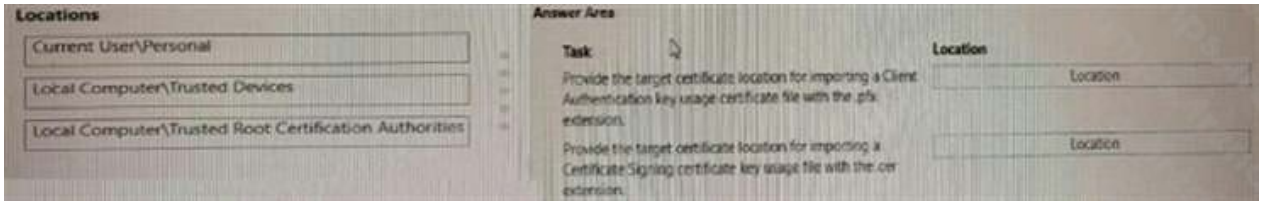
A new user attempts to establish a P25S VPN connection. The user receives the following error message:

A certificate could not be found that can be used with this Extensible Authentication protocol. (Error 798)

You need to assists the user with resolving the certificate issue.

What should you do? To answer, drag the appropriate locations to the correct task. Each location maybe used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



ANSWER:

Explanation:

A) Provide the target certificate location for importing a Client Authentication key usage certificate file with the .pfx extension.

Current User\Personal

This is the location where the client certificate should be installed on the user's personal Windows computer. The client certificate is generated from the self-signed root certificate and then exported with the .pfx extension. The client certificate is used to authenticate the user to the Azure point-to-site VPN gateway1.

B) Provide the target certificate location for importing a Certificate Signing certificate key usage file with the .cer extension

Local Computer\Trusted Root Certification Authorities

This is the location where the root certificate should be installed on the user's personal Windows computer. The root certificate is a self-signed certificate that is used to sign the client certificates. The root certificate public key data is also uploaded to Azure point-to-site VPN configuration. The root certificate is exported with the .cer extension1.

QUESTION NO: 6

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?

A. Uninstall the Volume Shadow Copy Service (VSS) Provider service.

B. Use AzCopy to upload data to a cache storage account.

C. Create a network service endpoint in a virtual network.

D. Upgrade the target storage disk.

ANSWER: D

Explanation:

Azure Site Recovery has limits on data change rates depending on the type of disk used for replication. If a VM has a data change rate higher than the supported limit for its disk type, it can cause replication issues or errors. To resolve this issue, you can upgrade the target storage disk to a higher tier that supports higher data change rates.

QUESTION NO: 7

A company has an Azure Active Directory (Azure AD) tenant. The company deploys Azure AD Connect to synchronize users from an Active Directory Domain Services (AD DS).

The synchronization of a user object is failing.

You need to troubleshoot the failing synchronization by using a built-in Azure AD Connect troubleshooting task.

Which two pieces of information should you collect before you start troubleshooting?

A. Object common name

B. AD connector name

C. Object globally unique identifier

D. Azure AD connector name

E. Object distinguished name

ANSWER: B E

Explanation:

the two pieces of information that should be collected before starting to troubleshoot the failing synchronization by using a built-in Azure AD Connect troubleshooting task are: B. AD connector name E. Object distinguished name

Azure AD Connect is a tool used to synchronize users from an on-premises Active Directory Domain Services (AD DS) to Azure AD. When troubleshooting synchronization issues, it is important to have information about the object that is failing to synchronize. The AD connector name refers to the name of the connector used to connect to the on-premises AD DS. The object distinguished name refers to the unique identifier of the object in the on-premises AD DS. Having this information can help identify and resolve synchronization issues.

QUESTION NO: 8

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:

A certificate could not be found

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.

ANSWER: B F G

Explanation:

To resolve the issue where a user reports an error message stating “A certificate could not be found” when trying to connect to an Azure point-to-site VPN that uses certificate-based authentication, you should perform the following three actions: B. Install a root certificate on the user’s device. F. Generate a client certificate. G. Install a client certificate on the user’s device.

Azure point-to-site VPNs that use certificate-based authentication require both a root certificate and a client certificate to be installed on the user’s device. The root certificate is used to validate the identity of the VPN gateway, while the client certificate is used to authenticate the user. If either of these certificates is missing or invalid, the user will not be able to connect to the VPN and may receive an error message stating that a certificate could not be found.

QUESTION NO: 9

A company hosts a network virtual appliance (VNA) and Azure Route Server in different virtual networks (VNets). Border Gateway Protocol (BGP) peering is enabled between the NVA loses internet connectivity after it advertises the default route to the route server.

You need to resolve the problem with the NVA.

What should you do?

A. Configure a user-defined route on the NVA subnet.

B. Move the route server to the same VNet as the NVA.

C. Configure a unique autonomous system number (ASN) on the NVA.

D. Configure a public IP address on the route server.

ANSWER: C

Explanation:

According to 2, when using Azure Route Server with network virtual appliances (NVAs), you need to ensure that each NVA has a unique ASN that is different from the route server’s ASN and any other BGP peer’s ASN. Otherwise, there will be routing issues due to BGP loop prevention mechanisms.

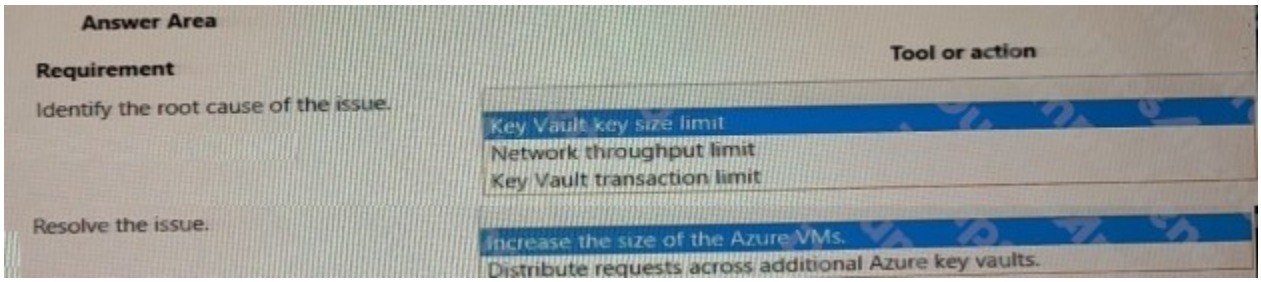
You can configure the ASN on the NVA by using its own configuration tools or commands. For more information, see 2.

QUESTION NO: 10 - (HOTSPOT)

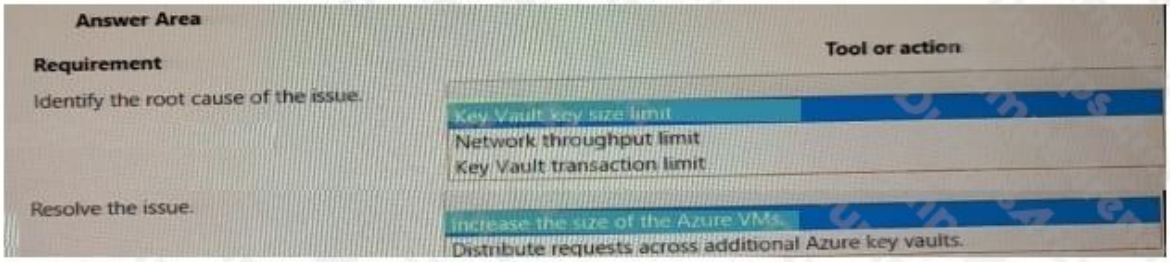
You need to troubleshoot the Azure Key Vault issues.

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