VCEplus

Microsoft.Premium.AZ-720.VCEplus.20q - DEMO

Number: AZ-720
Passing Score: 800
Time Limit: 120 min

Exam Code: AZ-720
Exam Name: Troubleshooting Microsoft Azure Connectivity
Website: www.VCEplus.io - www.VCEup.com

Case Study 01
Mix Questions

CEplus

Case Study 01

QUESTION 1
Case 1, Contoso Ltd, Case Study
Background
Contoso, Ltd. is a financial services company based in Boston. MA, United States. Contoso hires you to manage their Azure environment and resolve several operational issues.
General
Contoso's Azure environment contains the following resources. All resources are associated with the same subscription and are located in the East US region. Users connect to resources from Windows 10 computers by using the built-in SSTP VPN software.

Resource type	Resource name	Description
Virtual network	VNet1	A hub virtual network
Virtual network	VNet2 and VNet3	Spoke virtual networks peered to VNet1
Private DNS Zone	contoso.com	A private DNS zone linked to VNet1, VNet2, and VNet3. The zone contains A records for all Azure virtual machines (VMs) deployed in the three virtual networks.
Public DNS Zone	contoso.com	A public DNS zone containing the A record of a public web site www.contoso.com
VPN Gateway	VPNGW1	This VPN gateway is deployed to VNet1. It provides site-to-site and point-to-site connectivity. The public IP address of the VPNGW1 has the DNS name of VPNGW1.eastus.cloudapp.azure.net.
Storage account	contosostorage1	An Azure Storage account hosting Contoso's internal data.
Key Vault	KV1, KV2, KV3, KV4, and KV5	There are five key vaults that store encryption keys for Azure VM workloads. All Azure key vaults are configured to use access policy for authorization.
Cosmos DB account	CosmosDB1	Cosmos DB account hosting a database containing financial services inventory.
Subnet	Subnet1a	Subnet on VNet1
Subnet	Subnet2a	Subnet on VNet2
Virtual machine	VM1	An Azure VM connected to Subnet1a
Virtual machine	VM2	An Azure VM connected to Subnet2a

Recent changes
The company implements the following changes:
Extend the IP address space of VNet1 and create subnets in the new IP address space.
Allow users with computers that run the current version of MacOS to use the built-in VPN client for connecting to the point-to-site VPN.
Enable a service endpoint on contosostoragel to provide direct access to the storage content from all Configure all business critical VM workloads to use encryption keys stored in all five key vaults.
Enable a private endpoint on CosmbsDBT to provide direct access to its content from VNetl.
Develop an automated process to deploy Azure VMs by using A2ure Bicep. The passwords for the local administrator accounts are stored in the key vaults. You grant the team that initiates the deployment the Reader RBAC role to all key vaults.
Deploy a multi-tier SharePoint Server environment into a subnet in VNet2. You implement network security groups (NSGs) to allow only specific ports between tiers in the subnet. You configure NSGs to use application security groups (ASGs) when designating the source and destination of cross-tier traffic.
Deploy a secondary multi-tier SharePoint Server environment into a subnet in VNet3.
Requirements
General requirements
You must adhere to the principle of least privilege when granting access to resources.
Reverse DNS lookup
You must identify the reason for the differences between reverse DNS lookup results in the hub and the spoke networks and recommend a solution that provides the reverse DNS lookup in the format [vmnameJ.contoso.com for all three virtual networks.
Public DNS lookup
You must verify that the Azure public DNS rone is currently used to resolve DNS name requests for www.contoso.com and recommend.a solution that uses the Azure public DNS zone.
Windows VPN
You must verify if VPN client connectivity issues are related to routing and recommend a solution.
MacOS VPN
You must verify if Remote ID and local ID VPN client settings on the MAcOS devices are properly configured.
Azure Storage connectivity
You must resolve the issues with the SMB-mounts from VNet2 and VNet3 as well as ensure that onpremises connections to contosostorage are successful. Your solution must ensure that, whenever possible, network traffic does not traverse public internet.
Cosmos DB connectivity
You must verify if on-premises connections to ContosoDB1 are using the CosmosDB1 public endpoint. You need to recommend a solution if connections are not using private endpoints.
DNS issues
Reverse DNS lookups from VNetl return two records. One DNS record is in the format [vmname].contoso.com and the other DNS record is in the format [vmname].internal.cloudapp.net.
Reverse DNS lookups from VNet2 and VNet3 return DNS names in the format [vmname].internal.cloudapp.net.
VMs on each virtual network can only resolve reverse DNS lookup names of VMs on the same virtual network.
Public DNS lookup
You are notified that name resolution requests for www,contoso.com are using the DNS zone hosted by the DNS registrar where the zone was originally created.
Connectivity and routing issues
Window VPN
Windows VPN clients cannot connect to Azure VMs on the subnets recently added to VNet1.

VCEûp CEplus IT Certification Exams - Questions & Answers | VCEplus.io CEplus VCEûp

CEplus

Sales department VPN.
The sales department users connect by using the MacOs VPN client.
Azure Storage Connectivity
Server Message Block (SMB)-mount from VMs on VNet2 and VNet3 to file shares In contosostorage1 are failing Azure Storage Explorer connection using access keys from on-premses computer to contosostorage1 are failing Cosmos DB connectivity You observe that connections to ConsomosDB1 from the on-premises environment are using the CosmosDB1 public endpoint. However connections to CosmosDB1 from the on-premises environment should be using the private endpoint. You verify that connections to CosmosDB1 from VNet1 are using the private endpoint.
Azure Key vault
Access attempts to Azure Key vault oy VM workloads intermittently fail with the HTTP response code429. You must identify the reason for the failures and recommend a solution.
SharePoint
SharePoint In VNet2
SharePoint traffic between tiers is blocked by NSGs which is causing application failures. You need to identify the NSG rules that are blocking traffic. You also need to collect the data that is blocked by the NSG rules. The solution must minimize administrative effort.
SharePoint in VNet3.
ASGs used in the NSG rules associated with the VNet2 subnet are not visible when configuring NSG rules in VNet3. You need to create NSG rules for VNet3 with the same name, source and destination settings that are configured for the NSG associated with VNet2. The solution must minimize administrative effort.
Permission issues
Azure Biccp
You must identify the minimum privileges required to provision Azure VMs using Azure Bicep.
Data engineering team
You must identify the role-based access control (RBAQ roles required by the data engineering team to access the storage account by using Azure portal. The team requires minimum permissions to backup and restore blobs in contosostorage1. The Contoso data engineering tearn.js unable to view the contosostorage1 account in the Azure portal.
Azure VM deployment
Azure VM deployments that uses Azure Bicep are failing with an authorization error. The error indicates three are insufficient access permissions retrieve password of the local administrator account in the key vault.
VM1 and VM2
RT12 must be configured to route internal traffic from VM1 through VM2. You observe that internet traffic from VM1 is routed directly to the internet.
VM2
You configure VM2 to route internet traffic from VM1. After configuring RT12 to route internet traffic from VM1 through VM2, traffic reaches VM2 but then it is dropped. You that routing for VM2 is configured correctly.

A.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

www.VCEplus.io

QUESTION 2
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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 3
You need to resolve the issue with internet traffic from VM1 being routed directly to the internet.
What should you do?

A. Modify IP address prefix of RT12
B. Associate RT12 with Subnet1a.
C. Associate RT12 with Subnet2a.

VCEplus

D. Modify the next hop type of RT12.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
This will ensure that the route table RT12, which has a route to direct internet traffic to the virtual network gateway VNG1, is applied to the subnet where VM1 is located. This will override the default route that sends internet traffic to the internet gateway.

QUESTION 4
You need to resolve the VM2 routing issue.
What should you do?

A. Modify the IP configuration setting of the Azure network interface resource of VM1.
B. Add a network interface to VM1.
C. Add a network interface to VM2.
D. Modify the IP configuration setting of the Azure network interface resource of VM2.

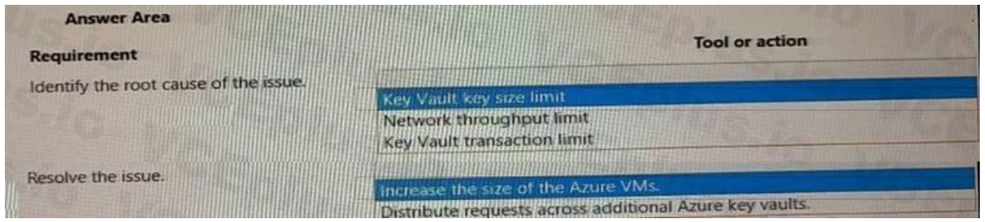
Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To resolve the VM2 routing issue, you should modify the IP configuration setting of the Azure network interface resource of VM2. This will ensure that VM2 can communicate with other resources in the virtual network.
Troubleshooting connectivity problems between Azure VMs involves several steps such as checking whether NIC is misconfigured, whether network traffic is blocked by NSG or UDR, whether network traffic is blocked by VM firewall, whether VM app or service is listening on the port and whether the problem is caused by SNAT1.
Topic 2, Misc. Questions Set

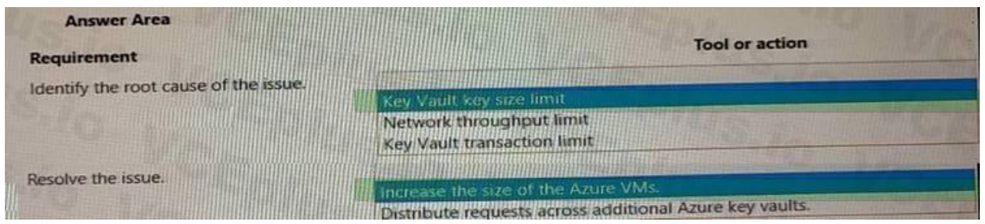
www.VCEplus.io

QUESTION 5
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.

Hot Area:



Correct Answer:



Section: (none)
Explanation

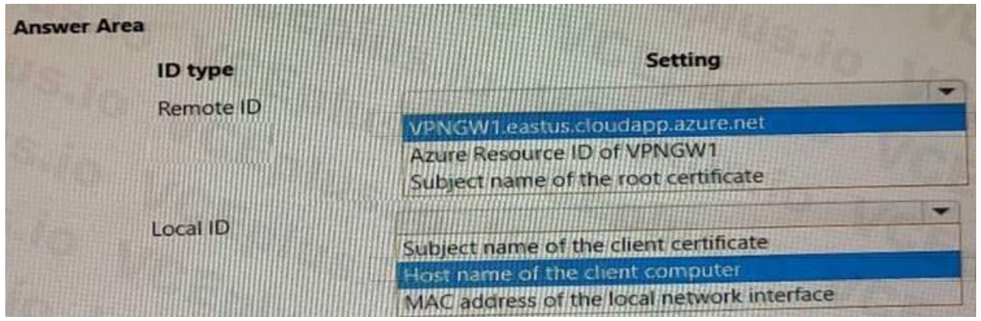
VCEûp VCEplus IT Certification Exams - Questions & Answers | VCEplus.io VCEplus VCEûp

CEplus

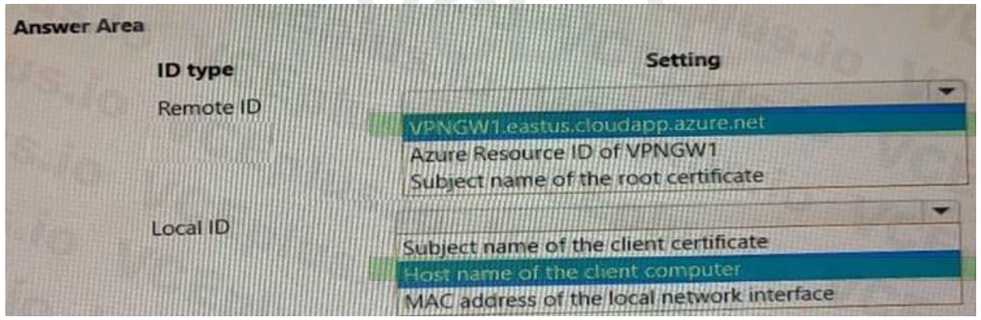
Explanation/Reference:
Box 1: Key Vault transaction limit.
Based on the given scenario, the issue is related to the number of transactions per second (TPS) being throttled. The Azure Key Vault has a transaction limit, which varies depending on the service tier. In the provided images, the error message 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-limitsBox : 2 Distribute requests across additional Azure Key vaultsIn the provided scenario, the issue is that the Azure Key Vault is experiencing throttling due to toomany requests per second. Throttling occurs when the number of requests exceeds the allowedlimits for a given time period. To resolve this issue, you should distribute the requests acrossadditional Azure Key Vaults. By doing so, you can balance the load and prevent exceeding the requestlimits, thus avoiding throttling. Reference: https://docs.microsoft.com/en-us/azure/keyvault/general/overview-throttling

QUESTION 6
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.

Hot Area:



Correct Answer:



Section: (none)
Explanation

Explanation/Reference:
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

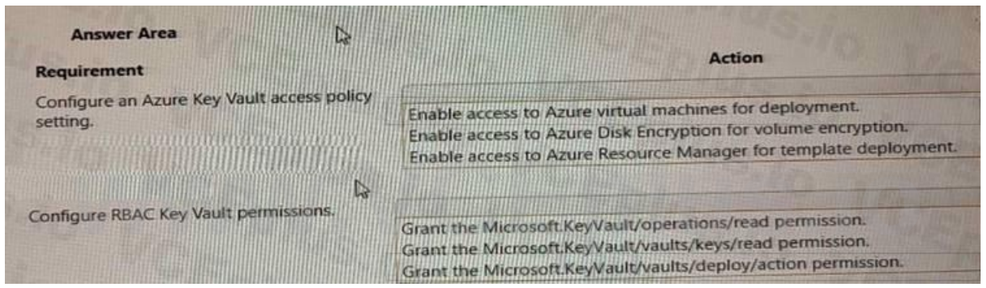
VCEûp CEplus

CEplus VCEûp

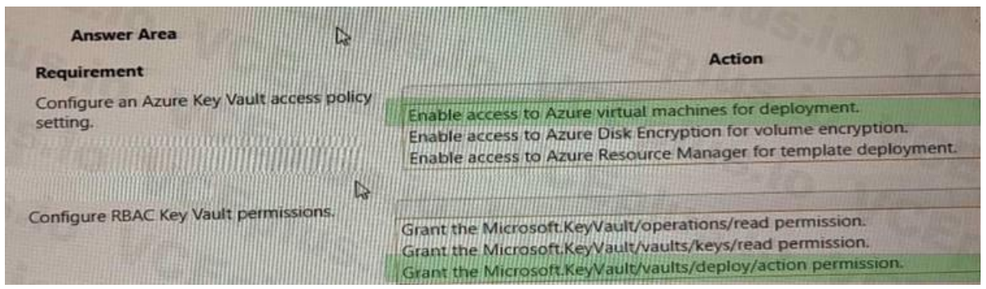
In the provided scenario, the sales department is using a VPN to connect to the corporate network, and the VPN server is configured to use certificate-based authentication. To troubleshoot the sales department issues, you should configure the system Local ID to use the subject name of the client certificate. 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 7
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.

Hot Area:



Correct Answer:



Section: (none)
Explanation

Explanation/Reference:
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/keyvault/ general/tutorial-net-create-vault-azure-web-app

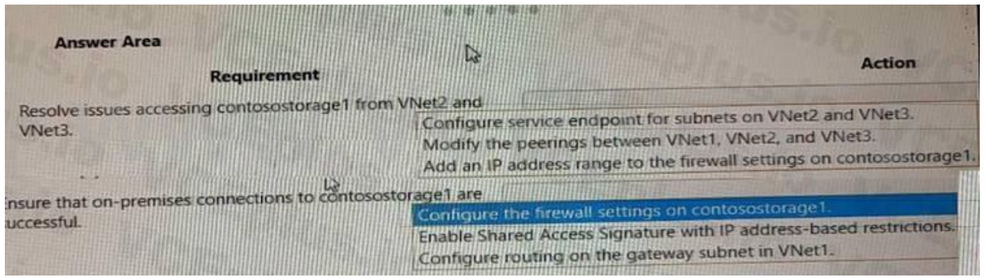
Box 2: Grant the Microsoft.KeyVault/vaults/deploy/action permission
This is the permission that you should configure on an RBAC Key Vault role to resolve the Azure virtual machine (VM) deployment issues. This permission allows Azure Resource Manager to retrieve secrets from the key vault when deploying resources using an ARM template1. Therefore, option C is correct.
A detailed explanation with references is as follows:

CEplus

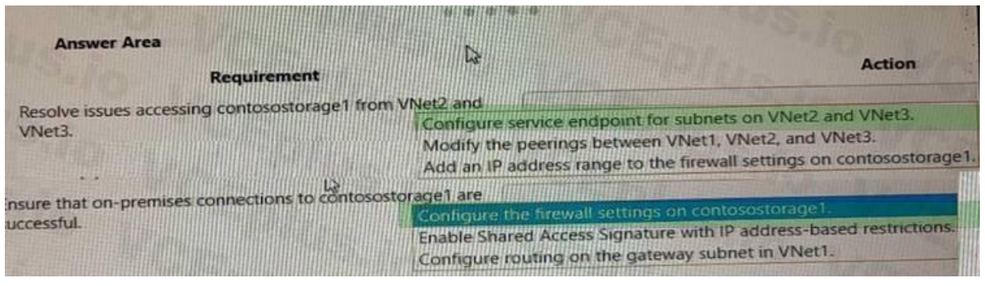
As mentioned in the scenario, the Azure virtual machine (VM) deployment issues are caused by the inability of Azure Resource Manager to retrieve secrets from the key vault when deploying resources using an ARM template. To resolve this issue, you need to configure an RBAC Key Vault role that grants Azure 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 rolebased 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 8
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.

Hot Area:



Correct Answer:



Section: (none)
Explanation

Explanation/Reference:
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.

VCEûp CEplus IT Certification Exams - Questions & Answers | VCEplus.io CEplus VCEûp

CEplus

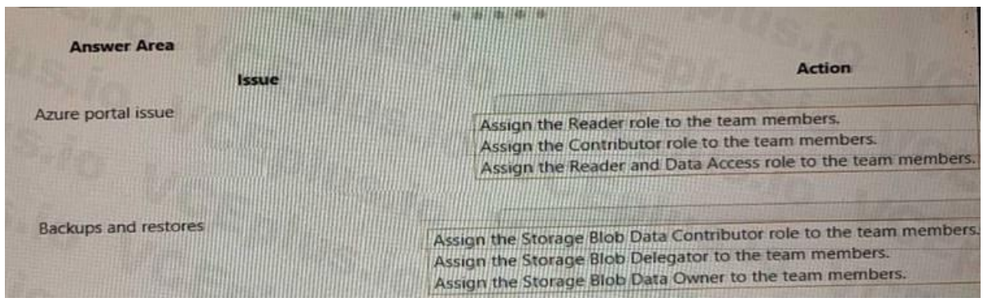
To configure service endpoints for a subnet using the Azure portal, follow these steps1:
In the Azure portal, navigate to the Virtual Network resource.
Select Subnets, then select the subnet that needs to access the storage account.
Under Service endpoints, select Microsoft.Storage from the drop-down 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.
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 steps1:
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.

www.VCEplus.io

QUESTION 9
HOTSPOT
You need to resolve the issue.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

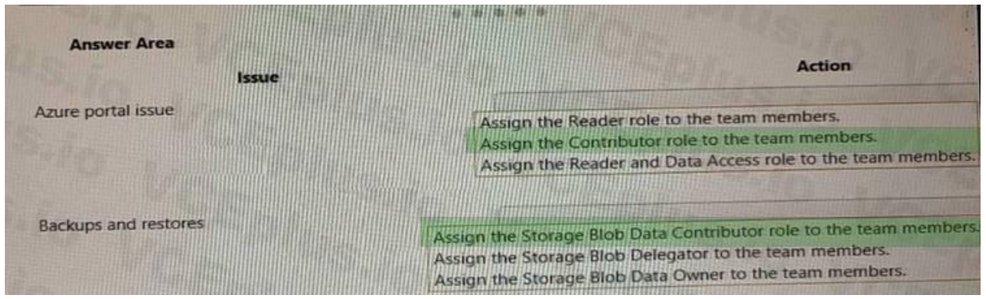
Hot Area:



Correct Answer:

VCEûp CEplus IT Certification Exams - Questions & Answers | VCEplus.io CEplus VCEûp

CEplus



Section: (none)
Explanation

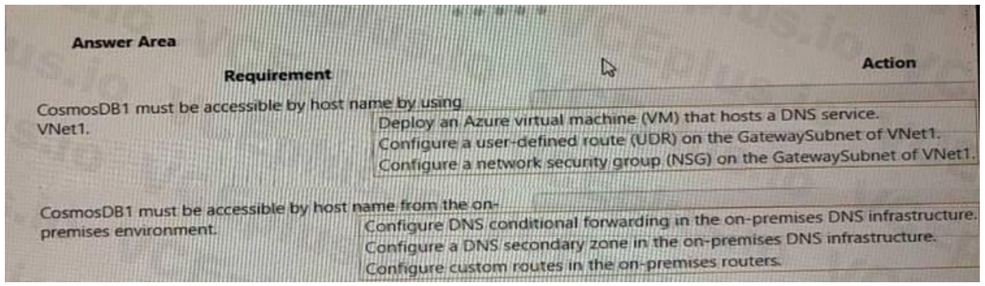
Explanation/Reference:
Box 1: Assign the Contributor role to the team members.
In the given scenario, the team members are unable to create or manage resources in the Azure portal. To allow them to do so, you should assign the Contributor role to the team members. The Contributor role allows users to create and manage resources within the scope of their access, but they cannot grant access to others. The Reader role only provides read access to resources and does not allow creation or management of resources. The Reader and Data Access role is not a valid combined role in Azure. Reference: - Azure built-in roles: https://docs.microsoft.com/enus/ azure/role-based-access-control/built-in-roles As mentioned in the scenario, the team members are unable to create resources in Azure Portal. This indicates that they do not have sufficient permissions to perform this operation. To grant them permissions, you need to assign them an Azure role that allows creating and managing Azure resources.
Azure roles are roles that can be assigned to users, groups, or applications to manage access to Azure resources1. Azure roles are based on Azure role-based access control (Azure RBAC), which is an authorization system that provides fine-grained access management of Azure resources2. With Azure RBAC, you can control access to resources by creating role assignments, which consist of three elements2:
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 assign an Azure role that allows creating and managing Azure resources, you can use the Contributor role. The Contributor role is a built-in role that has full access to all resources except granting access to others1. This means that users who are assigned the Contributor role can create and manage any type of Azure resource, such as virtual machines, storage accounts, web apps, etc.
To assign the Contributor role using the Azure portal, follow these steps3:
In the Azure portal, navigate to the scope where you want to assign the role. For example, a subscription or a resource group.
Select Access control (IAM), then select Add > Add role assignment.
Under Role, select Contributor from the drop-down list.
Under Assign access to, select User, group, or service principal.
Under Select, find and select the users or groups that you want to assign the role to. You can type in the Select box to search the directory for display name or email address.
Select Save to create the role assignment.
To assign the Contributor role using the Azure CLI or PowerShell, see Assign Azure roles using CLI or PowerShell.
Box 2: Assign the Storage Blob Data Contributor role to the team members.
A detailed explanation with references is as follows:
As mentioned in the scenario, the team members are unable to perform backups and restores of blob dat a. This indicates that they do not have sufficient permissions to access blob storage resources. To grant them permissions, you need to assign them an Azure role that allows read/write/delete permissions to blob storage resources.
Azure roles are roles that can be assigned to users, groups, or applications to manage access to Azure resources2. Azure 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 assign an Azure role that allows read/write/delete permissions to blob storage resources, you can use the Storage Blob Data Contributor role. The Storage Blob Data Contributor role is a built-in role that has full access to blob storage resources except granting access to others1. This means that users who are assigned the Storage Blob Data Contributor role can perform backups and restores of blob data.
To assign the Storage Blob Data Contributor role using the Azure portal, follow these steps4:
In the Azure portal, navigate to the scope where you want to assign the role. For example, a storage account or a container.
Select Access control (IAM), then select Add > Add role assignment.
Under Role, select Storage Blob Data Contributor from the drop-down list.
Under Assign access to, select User, group, or service principal.
Under Select, find and select the users or groups that you want to assign the role to. You can type in the Select box to search the directory for display name or email address.
Select Save to create the role assignment.
To assign the Storage Blob Data Contributor role using the Azure CLI or PowerShell, see Assign Azure roles using CLI or PowerShell.

QUESTION 10
HOTSPOT
You need to resolve the connectivity issue with the on-premises database named CosmosDB1.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

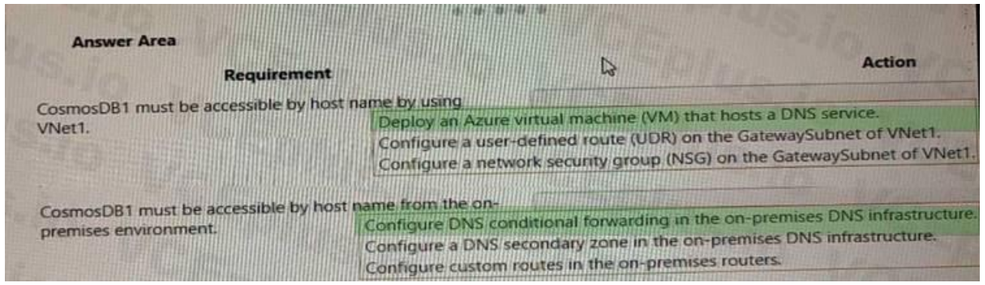
VCEûp CEplus IT Certification Exams - Questions & Answers | VCEplus.io CEplus VCEûp

VCEplus

Hot Area:



Correct Answer:



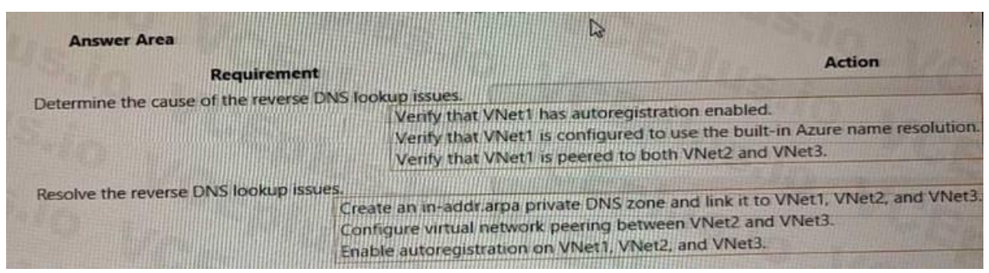
Section: (none)
Explanation

Explanation/Reference:
Box 1: Deploy an Azure virtual machine (VM) that hosts a DNS service.
In the given scenario, CosmosDB1 is an on-premises database, and you need to make it accessible by host name using VNet1. To achieve this, you should deploy an Azure virtual machine that hosts a DNS service. This will allow you to configure custom DNS settings for VNet1, enabling the resolution of the on-premises database's host name. Reference: https://docs.microsoft.com/en-us/azure/virtualnetwork/ virtual-networks-name-resolution-for-vms-and-role-instances#name-resolution-that-usesyour- own-dns-server

Box 2: Configure DNS conditional forwarding in the on-premises DNS infrastructure.
In the given scenario, you need to resolve the connectivity issue with the on-premises database named CosmosDB1, and it must be accessible by hostname from the on-premises environment. To achieve this, you should configure DNS conditional forwarding in the on-premises DNS infrastructure.
DNS conditional forwarding allows you to specify that DNS queries for a specific domain (in this case, the Azure Cosmos DB) are forwarded to a specific DNS server or set of servers. This ensures that the on-premises environment can resolve the hostname of CosmosDB1 by forwarding the DNS queries to the appropriate DNS server responsible for that domain. Reference: 1. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc782142(v=ws.10) 2. https://docs.microsoft.com/en-us/azure/private-link/private-endpointdns#on-premises-workloads-using-a-dns-forwarder

QUESTION 11
HOTSPOT
You need to troubleshoot and resolve the reverse DNS lookup issues.
What should you do? To answer, select the appropriate option in the answer area.
NOTE: Each correct selection is worth one point.

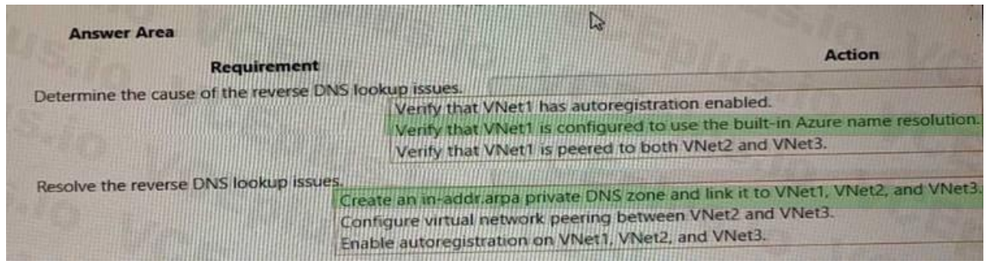
Hot Area:



Correct Answer:

VCEûp VCEplus IT Certification Exams - Questions & Answers | VCEplus.io VCEplus VCEûp

CEplus

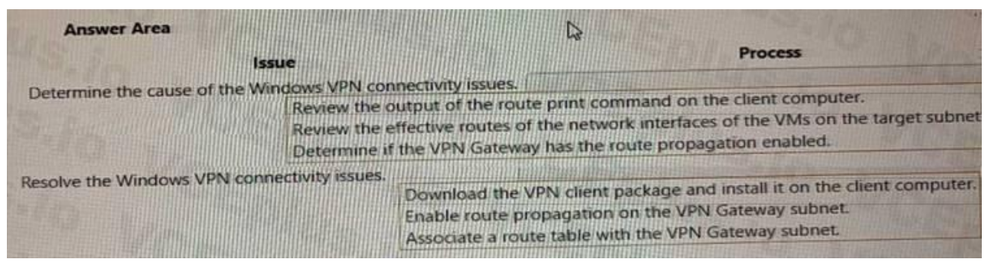


Section: (none)
Explanation

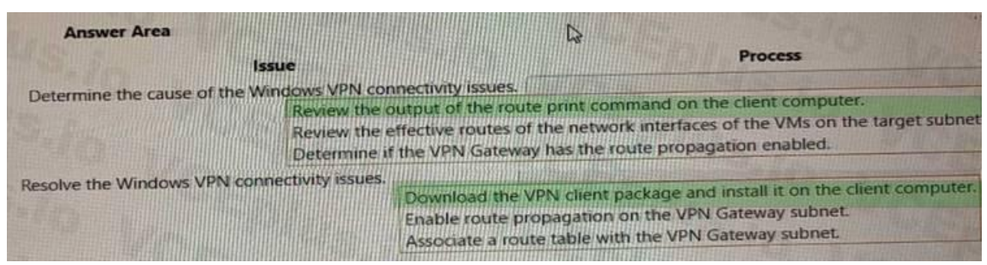
Explanation/Reference:
Box 1: Verify that VNet1 is configured to use the built-in Azure resolution As mentioned in the scenario, you need to troubleshoot and resolve the reverse DNS lookup issues. Reverse DNS lookup is a process of resolving an IP address to a host name2. For example, if you have a virtual machine with an IP address of 10.0.0.4 and a host name of vm1.contoso.com, you can use reverse DNS lookup to find the host name from the IP address.
One way to perform reverse DNS lookup in Azure is to use the built-in Azure resolution. The built-in Azure resolution is a feature that allows reverse DNS lookup (PTR DNS queries) for virtual machine IP addresses by default1. This feature works for both IPv4 and IPv6 addresses, and it supports both public and private IP addresses. The built-in Azure resolution uses the host name of the virtual machine as the reverse DNS record.
To use the built-in Azure resolution, you need to configure your virtual network to use the default Azure-provided DNS servers. These are the DNS servers that are automatically assigned to your virtual network when you create it3. You can verify or change the DNS server settings of your virtual network using the Azure portal, PowerShell, CLI, or REST API.
To verify that VNet1 is configured to use the built-in Azure resolution using the Azure portal, follow these steps:
In the Azure portal, navigate to the Virtual Network resource.
Select DNS servers under Settings.
Check if Default (Azure-provided) is selected under DNS servers. If not, select it and click Save to apply the changes.
After configuring your virtual network to use the built-in Azure resolution, you can test the reverse DNS lookup using tools such as nslookup or dig. For example, you can use the following command to perform a reverse DNS lookup for an IP address of 10.0.0.4: nslookup -type=PTR 10.0.0.4 The output should show the host name of the virtual machine that has that IP address.
Box 2: Create an in-addr.arpa private DNS zone and link it to VNet1, VNet2, and VNet3.
Reverse DNS lookup issues are related to resolving IP addresses to their corresponding hostnames.
In the given scenario, the issue is with reverse DNS lookups for the resources in the three virtual networks. Creating an in-addr.arpa private DNS zone and linking it to VNet1, VNet2, and VNet3 would ensure that the reverse DNS lookups can be resolved correctly across all three virtual networks. Reference: 1. Azure Private DNS: https://docs.microsoft.com/en-us/azure/dns/privatedns- overview 2. Reverse DNS lookup in Azure: https://docs.microsoft.com/en-us/azure/dns/privatedns- reverse-public-ip

QUESTION 12
HOTSPOT
You need to troubleshoot and resolve the reverse VPN connectivity issues.
What should you do? To answer, select the appropriate option in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



VCEûp CEplus IT Certification Exams - Questions & Answers | VCEplus.io CEplus VCEûp

CEplus

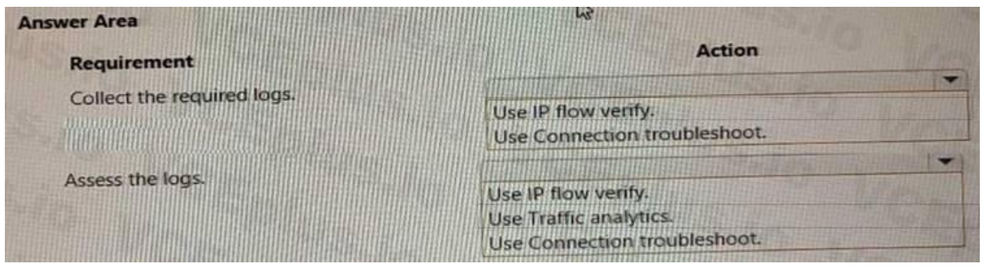
Section: (none)
Explanation

Explanation/Reference:
BOX1: Review the output of the route print command on the client computer.
A Windows VPN connection is a point-to-site connection that allows a client computer to connect to an Azure virtual network gateway using IKEv2 or SSTP protocols1. To troubleshoot Windows VPN connectivity issues, you need to check the configuration and status of the VPN client on the client computer.
One of the common problems that can cause Windows VPN connectivity issues is incorrect routing configuration on the client computer1. The client computer needs to have a route that directs the traffic destined for the target subnet in Azure to the VPN interface. If the route is missing or incorrect, the traffic will not reach the Azure virtual network gateway.
To check the routing configuration on the client computer, you can use the route print command in a command prompt window. This command displays the routing table of the client computer, which shows the destination network, the gateway address, and the interface for each route2. You can compare the output of this command with the expected routes for your VPN connection.
For example, if your target subnet in Azure is 10.0.0.0/24 and your VPN interface has an IP address of 172.16.0.1, you should see a route like this in the output of route print:
Destination Network | Gateway Address | Interface 10.0.0.0/24 | On-link | 172.16.0.1 This route means that any traffic destined for 10.0.0.0/24 will be sent directly to the VPN interface (On-link) with an IP address of 172.16.0.1.
If you do not see this route or see a different gateway address or interface, you need to correct the routing configuration on the client computer. You can use the route add command to add a new route or use the route change command to modify an existing route2.

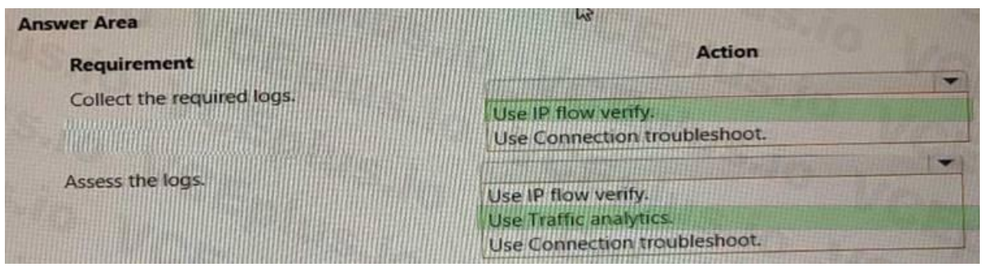
BOX 2: Download the VPN client package and install it on the client computer A Windows VPN connection is a point-to-site connection that allows a client computer to connect to an Azure virtual network gateway using IKEv2 or SSTP protocols1. To establish a Windows VPN connection, you need to install a VPN client package on the client computer that contains the configuration files and certificates required for the connection1.
One of the common problems that can cause Windows VPN connectivity issues is missing or outdated VPN client package on the client computer1. The VPN client package may be missing if it was not installed properly or deleted accidentally. The VPN client package may be outdated if the Azure virtual network gateway configuration has changed since the package was downloaded.
To resolve this problem, you need to download the latest VPN client package from the Azure portal and install it on the client computer1. To download the VPN client package, follow these steps:
Go to the Azure portal and select your virtual network gateway.
On the Overview page, click Point-to-site configuration.
On the Point-to-site configuration page, click Download VPN client.
Select the appropriate version of Windows for your client computer and click Download.
Extract the contents of the downloaded ZIP file to a folder on your client computer.
Run the executable file in the folder to install the VPN client package.

QUESTION 13
HOTSPOT
You need to troubleshoot the issues with the SharePoint workload in VNet2.
What should you do? To answer, select the appropriate option in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Section: (none)
Explanation

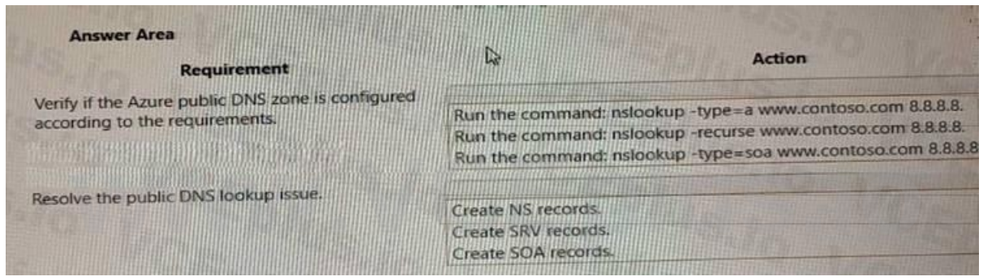
VCEûp CEplus IT Certification Exams - Questions & Answers | VCEplus.io CEplus VCEûp

CEplus

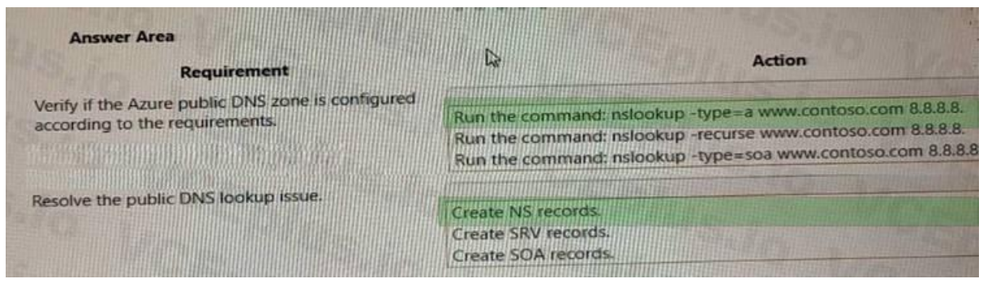
Explanation/Reference:
Box 1 = Use IP flow verify.
IP flow verify is a feature of Azure Network Watcher that checks if a packet is allowed or denied to or from a virtual machine. It can help diagnose connectivity issues caused by network security groups, user-defined routes, or Azure Virtual Network Manager rules1. IP flow verify can also return the name of the rule that denied the packet, which can be useful for troubleshooting2.
Connection troubleshoot is another feature of Azure Network Watcher that helps reduce the time to diagnose and resolve network connectivity issues. However, it can only test TCP or ICMP connections from certain Azure resources, such as virtual machines, Azure Bastion instances, or application gateways3. Connection troubleshoot can also detect issues such as high VM CPU utilization, DNS resolution failures, or inability to open a socket at the specified source port3.
In this scenario, you need to collect the required logs for the SharePoint workload in VNet2. Since you are not testing a specific TCP or ICMP connection, but rather checking if packets are allowed or denied by any network configuration, IP flow verify is more suitable than connection troubleshoot. You can use IP flow verify to check the direction, protocol, local IP, remote IP, local port, and remote port of the packets and see which rule is blocking them12.
To use IP flow verify, you need to enable a network watcher in the same region as the virtual machines you want to troubleshoot. Then you can use the Azure portal, PowerShell, or Azure CLI to run IP flow verify and get the results24.
Box 2 = Use Traffic analytics
To troubleshoot issues related to the SharePoint workload in VNet2, we can use Traffic Analytics. It is a networking monitoring solution that uses Network Watcher to analyze and report on traffic flows in your Azure virtual network. With Traffic Analytics, you could see information about the traffic flow patterns and security concerns detected across Azure subscriptions using network security group (NSG) flow logs. IP Flow Verify is used to verify if packets are flowing as expected between two endpoints within an Azure virtual network or between a public IP address and an endpoint inside an azure virtual network. But it doesn't provide visibility into overall traffic patterns or identify potential security threats.
Connection Troubleshoot can be used when you have connectivity problems while interacting with a specific instance of a resource type being served out from Microsoft datacenters over Internet, but for troubleshooting SharePoint workloads related issue which might not necessarily correspond to internet routing/connectivity problems this may not apply.

QUESTION 14
HOTSPOT
You need to troubleshoot and resolve the public DNS lookup issues.
What should you do? To answer, select the appropriate option in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Section: (none)
Explanation

Explanation/Reference:
BOX 1: Run the command: nslookup -type=a www.contoso.com 8.8.8.8
nslookup is a command-line tool that queries DNS servers for information about domain names and IP addresses. It can be used to troubleshoot DNS issues and verify DNS configurations1.
The -type option specifies the type of DNS record to query. The -type=a option queries for A records, which map domain names to IPv4 addresses1. The www.contoso.com argument specifies the domain name to query. The 8.8.8.8 argument specifies the DNS server to use for the query, which is a public DNS server provided by Google2.
By running this command, you can verify if the Azure Public DNS zone is configured according to the requirements by checking if the A record for www.contoso.com matches the expected IPv4 address. If the A record is missing or incorrect, you can use the Azure portal, PowerShell, or Azure CLI to create or update it in your DNS zone3.

Box2: Create NS records
NS (Name Server) records are used to delegate a domain or subdomain name to a set of authoritative DNS servers, which can provide information about that domain. In this scenario, there appears to be an issue with resolving the domain in question via public DNS lookup since it's only resolving locally on one server and not across all networks. By creating NS records for the domain, authoritative nameservers will be identified and designated as responsible for providing

VCEplus

accurate information about the specific zone. This will ensure your domain is properly distributed on various different network zones and help users globally reach your website without any delays or connectivity problems. Alternatively, SRV (Service locator) record is used when you have multiple servers offering similar services such as email or SIP but want to use a weight system indication greater trustworthiness/proximity of datacenters within providers dns infrastructure. And SOA (Start Of Authority) - indicates who in control ofthe DNS zone and provides other related information such as the serial number and default TTL values. Therefore, option
A. Create NS records would be the best solution for resolving public DNS lookup issues in this scenario. Reference: - "NS record," Microsoft Docs, accessed March 27, 2023. [Online]. Available: https://docs.microsoft.com/en-us/windows-server/networking/dns/deploy/create-a-dns-record-fordomain-access#ns-record - "SRV record," Cloudflare Help Center, accessed March 27, 2023. [Online]. Available: https://support.cloudflare.com/hc/en-us/articles/216672888-SRV-Record-Setup - "SOArecord," DigitalOcean Product Documentation, accessed March 27, 2023. [Online]. Available: https://www.digitalocean.com/community/tutorials/how-to-manage-dns-using-the-digitaloceancontrol-panel#start-of-authority-record

www.VCEplus.io

VCEplus

Mix Questions

QUESTION 1
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
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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 onpremises 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-customroute-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#toroute-to-a-null-interface.

www.VCEplus.io

QUESTION 2
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: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Disabling peering on the virtual network will not prevent the on-premises network from reaching the new subnet. Virtual network peering is a way to connect virtual networks and allows resources in both virtual networks to communicate with each other securely. It does not affect connectivity between on-premises and virtual network resources.
A better solution would be to create a network security group (NSG) and associate it with the new subnet. The NSG can be configured to deny traffic from the on-premises network to the new subnet.
This way, the new subnet will be isolated from the on-premises network.
Reference:
Azure Virtual Network peering: https://docs.microsoft.com/en-us/azure/virtual-network/virtualnetwork-peering-overviewAzure Network Security Groups: https://docs.microsoft.com/en-us/azure/virtual-network/networksecurity-groups-overview

QUESTION 3
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: Scale the gateway to Generation2.
Does the solution meet the goal?

A. Yes

VCEplus

B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Scaling the gateway to Generation2 will not prevent the on-premises network from reaching the new subnet. Scaling the gateway changes the hardware configuration of the VPN gateway, but it does not affect the routing or connectivity between the on-premises network and the virtual network.
A better solution would be to create a network security group (NSG) and associate it with the new subnet. The NSG can be configured to deny traffic from the on-premises network to the new subnet.
This way, the new subnet will be isolated from the on-premises network.
Reference:
VPN Gateway Generation 2: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gatewayabout-vpngateways#gwgen2

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 subnet delegation.
Does the solution meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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

QUESTION 5
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: Restart the Azure AD Connect service.
Does the solution meet the goal?

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 6
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:

VCEplus

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
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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-passwordwriteback#troubleshooting-steps

QUESTION 7
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 that is not federated to configure Azure AD Connect.
Does the solution meet the goal?

www.VCEplus.io

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The proposed solution to use a global administrator account that is not federated to configure Azure AD Connect does not directly address the error message "Error getting auth token" described in the scenario , so it is unlikely to solve the issue.
To resolve this issue, you should verify that the Azure AD Connect server can authenticate to the Azure AD tenant using valid credentials. If authentication is successful, then you can investigate other possible causes such as network connectivity problems, misconfigured firewall rules, expired certificates, etc.
Therefore, the correct answer remains 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-passwordwriteback