Microsoft

Exam Questions AZ-720

Troubleshooting Microsoft Azure Connectivity

NEW QUESTION 1
A company has an Azure Virtual Network gateway named VNetGW1. The company enables point-to-site connectivity on VNetGW1. An administrator configures VNetGW1 for the following:

❯ OpenVPN for the tunnel type.

❯ Azure certificate for the authentication type.
Users receive a certificate mismatch error when connecting by using a VPN client. You need to resolve the certificate mismatch error.
What should you do?

A. Install an IKEv2 VPN client on the user's computers.
B. Reissue the client certificate with client authentication enabled.
C. Create a profile manually, add the server FQDN and reissue the client certificate.
D. Configure the tunnel type for IKEv2 and OpenVPN on VNetGW1.

Answer: D

NEW QUESTION 2
A company configures an Azure site-to-site VPN between an on-premises network and an Azure virtual network.
The company reports that after completing the configuration, the VPN connection cannot be established. You need to troubleshoot the connection issue.
What should you do first?

A. Identify the shared key by running this PowerShell cmdlet: Get-AzVirtualNetworkGatewayConnectionSharedKey.
B. Identify the shared key by running this PowerShell cmdlet:Get-AzVirtualNetworkGatewayConnectionVpnDeviceConfigScript.
C. Verify the AzureRoot.cer file exists.
D. Verify the AzureClient.pfx file exists.

Answer: B

NEW QUESTION 3
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

NEW QUESTION 4
A company plans to implement ExpressRoute by using the provider connectivity model.
The company creates an ExpressRoute circuit. You are unable to connect to resources through the circuit. You need to determine the provisioning state of the service provider.
Which PowerShell cmdlet should you run?

A. Get-AzExpressRouteCircuitPeeringConfig
B. Get-AzExpressRouteCircuitRouteTable
C. Get-AzExpressRouteCircuitConnectionConfig
D. Get-AzExpressRouteCircuit
E. Get-AzExpressRouteCircuitARPTable

Answer: C

NEW QUESTION 5
A company deploys the Azure Application Gateway Web Application Firewall (WAF) to protect their web applications.
Users in a remote office location report the following issues:

❯ Unable to access part of a web application.

❯ Part of the web application is failing to load.

❯ Parts of the web application has activities that are not performing as expected.
You need to troubleshoot the issue. Which diagnostic log should you review?

A. Performance
B. Firewall
C. Access
D. Azure Activity

Answer: D

NEW 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 could 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. What should you do?

A. Restart the Azure AD Connect service.
B. Configure Azure AD Connect using a global administrator account that is not federated.
C. Configure Azure AD Connect using a global administrator account with a password that is less than 256 characters.
D. Disable password writeback and then enable password writeback using the Azure AD Connect configuration.

Answer: C

NEW QUESTION 7

A company has virtual machines (VMs) in the following Azure regions:

➤ West Central US

➤ Australia East

The company uses ExpressRoute private peering to provide connectivity to VMs hosted on each region and on-premises services.
The company implements global VNet peering between a VNet in each region. After configuring VNet peering, VM traffic attempts to use ExpressRoute private peering.
You need to ensure that traffic uses global VNet peering instead of ExpressRoute private peering. The solution must preserve existing on-premises connectivity to Azure VNets.
What should you do?

A. Add a user-defined route to the subnets route table.
B. Add a filter to the on-premises routers.
C. Add a second VNet to the virtual machines and configure VNet peering between the VNets.
D. Disable the ExpressRoute peering connections for one of the regions.

Answer: B

NEW QUESTION 8

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?

A. Configure the hashing algorithm to be different on both gateways.
B. Rest the VPN gateway.
C. Configure the pre-shared key to be the same on the Azure VPN gateway and the on-premises VPN gateways.
D. Rest the VPN connection.
E. Configure the hashing algorithm to be the same on both gateways.
F. Configure the pre-shared key to be different on the Azure VPN gateway and the on-premises VPN gateways.

Answer: CEF

NEW QUESTION 9

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?

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 10

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: Configure the retention range for the current VM backup policy. Does the solution meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 10
A company has an ExpressRoute gateway between their on-premises site and Azure. The ExpressRoute gateway is on a virtual network named VNet1. The company enables FastPath on the gateway. You associate a network security group (NSG) with all of the subnets.
Users report issues connecting to VM1 from the on-premises environment. VM1 is on a virtual network named VNet2. Virtual network peering is enabled between VNet1 and VNet2.
You create a flow log named FlowLog1 and enable it on the NSG associated with the gateway subnet. You discover that FlowLog1 is not reporting outbound flow traffic.
You need to resolve the issue with FlowLog1. What should you do?

A. Create the storage account for FlowLog1 as a premium block blob.
B. Create the storage account for FlowLog1 as a premium page blob.
C. Enable FlowLog1 in a network security group associated with the subnet of VM1.
D. Configure the FlowTimeoutInMinutes property on VNet1 to a non-null value.

Answer: B

NEW QUESTION 13
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: CD

NEW QUESTION 18
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?

A. The administrator is using the Microsoft Defender for Cloud free tier.
B. The VMs were provisioned by using a classic deployment.
C. The VMs were recently provisioned by using an Azure Resource Manager deployment.
D. The administrator does not have the SecurityReader role.

Answer: B

NEW QUESTION 22
A company has users in Azure Active Directory (Azure AD). The company enables the users to use Azure AD multi-factor authentication (MFA).
A user named User1 reports they receive the following error while setting up additional security verification settings for MFA:
Sorry! We can't process your request. Your session is invalid or expired. There was an error processing your request because your session is invalid or expired.
Please try again.
You need to help the user complete the MFA setup. What should you do?

A. From the Microsoft 365 Admin portal, clear the Block this user from signing in option for the user.
B. Instruct the user to complete the setup process within 10 minutes.
C. Instruct the user to enter the correct verification code.
D. Instruct the user to clear their web browser cache.
E. From the Azure AD portal, reset the user's password.

Answer: E

NEW QUESTION 24
A company deploys an Azure Virtual Network gateway. The company connects to the gateway by using a site-to-site VPN connection.
The company's on-premises VPN gateway is reporting an issue with the Phase 1 proposal from the Azure Virtual Network gateway.
You need to troubleshoot the issue by reviewing the logs. Which log should you analyze?

A. P2SDiagnosticLog
B. GatewayDiagnosticLog
C. IKEDiagnosticLog
D. RouteDiagnosticLog

Answer: C

NEW QUESTION 27
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:

```
ResourceGroupName  :  RG1
ServerName         :  sqlsvr1
StartIpAddress     :  0.0.0.0
EndIpAddress       :  0.0.0.0
FirewallRuleName   :  Rule01


ResourceGroupName  :  RG1
ServerName         :  sqlsvr1
StartIpAddress     :  72.225.0.0
EndIpAddress       :  72.225.255.255
FirewallRuleName   :  Rule02
```

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?

Requirement	Action
Tool to use to determine the reason for the connection failure.	Transact-SQL stored procedure Azure CLI command Azure PowerShell cmdlet
Resolve the issue.	Modify the RBAC assignment for User2. Modify the firewall rules of sqlsvr1. Modify the firewall rules of SQLDB2.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Requirement	Action
Tool to use to determine the reason for the connection failure.	Transact-SQL stored procedure Azure CLI command Azure PowerShell cmdlet
Resolve the issue.	Modify the RBAC assignment for User2. Modify the firewall rules of sqlsvr1. Modify the firewall rules of SQLDB2.

NEW QUESTION 29

A company develops an Azure Cosmos DB solution. The solution has the following components:
- A virtual network named VNet1 in a resource group named RG1.
- A subnet named Subnet1 in VNet1.
-

A Private Link service.
The company is unable to configure a source IP address for the Private Link service from Subnet1. You need to resolve the issue for Subnet1.
How should you complete the PowerShell commands?

```
$virtualSubnetName = "Subnet1"
$virtualNetwork= Get-AzVirtualNetwork -Name "VNet1" -ResourceGroupName "RG1"
($virtualNetwork | Select -ExpandProperty subnets | Where-Object  {$_.Name -eq
  $virtualSubnetName} ).                    [▼]           =
$virtualNetwork | Set-AzVir
        privateLinkServiceId                     Approved
        privateLinkServiceConnection             Disabled
        privateLinkServiceNetworkPolicies        Enabled
        privateEndpointConnections
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:

```
$virtualSubnetName = "Subnet1"
$virtualNetwork= Get-AzVirtualNetwork -Name "VNet1" -ResourceGroupName "RG1"
($virtualNetwork | Select -ExpandProperty subnets | Where-Object  {$_.Name -eq
  $virtualSubnetName} ).                    [▼]           =
$virtualNetwork | Set-AzVir
        privateLinkServiceId                     Approved
        privateLinkServiceConnection             Disabled
        privateLinkServiceNetworkPolicies        Enabled
        privateEndpointConnections
```

NEW QUESTION 31
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?

```
Answer Area

        Get-AzSubscriptionDiagnosticSettingCategory      New-AzDiagnosticDetailSetting
        Get-AzDiagnosticSetting                          New-AzDiagnosticSetting
        New-AzDiagnosticSetting                          Get-AzDiagnosticSetting
        Get-AzDiagnosticSettingCategory                  Get-AzDiagnosticSettingCategory

$list = @()
                                  [▼] | ForEach-Object {
        $list +=                          [▼]
{
$setting =                        [▼]   -Name "contoso" -SubscriptionId "contoso-sub-id" -WorkspaceId
"contoso-workspace" -Setting $list
Set-AzDiagnosticSetting -InputObject $setting

                        New-AzDiagnosticDetailSetting
                        New-AzDiagnosticSetting
                        Get-AzDiagnosticSetting
                        Get-AzDiagnosticSettingCategory
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:

```
Get-AzSubscriptionDiagnosticSettingCategory
Get-AzDiagnosticSetting
New-AzDiagnosticSetting
Get-AzDiagnosticSettingCategory
```

```
New-AzDiagnosticDetailSetting
New-AzDiagnosticSetting
Get-AzDiagnosticSetting
Get-AzDiagnosticSettingCategory
```

Answer Area

```
$list = @()
                                    ▼ | ForEach-Object {
        $list +=                    ▼
    {
    $setting =                              ▼ -Name "contoso" -SubscriptionId "contoso-sub-id" -WorkspaceId
    "contoso-workspace" -Setting $list
    Set-AzDiagnosticSetting -InputObject $setting
```

```
New-AzDiagnosticDetailSetting
New-AzDiagnosticSetting
Get-AzDiagnosticSetting
Get-AzDiagnosticSettingCategory
```

NEW QUESTION 36

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

Answer: B

NEW QUESTION 41

A company uses Azure AD Connect. The company plans to implement self-service password reset (SSPR). An administrator receives an error that password writeback cloud not be enabled during the Azure AD Connect configuration. The administrator observes the following event log error:
Error getting auth token
You need to resolve the issue.
Solution: Use a global administrator account with a password that is less than 256 characters to configure Azure AD Connect.
Does the solution meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 45

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?

A. The administrator is using the Microsoft Defender for Cloud free tier.
B. The VMs were provisioned by using a classic deployment.
C. The administrator does not have the SecurityReader role.
D. The administrator does not have permissions to request JIT access to the VMs.

Answer: B

NEW QUESTION 50

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?

Answer Area

```
AzureMetrics
AzureActivity
AzureDiagnostics

                    IKEDiagnosticLog
                    RouteDiagnosticLog
                    TunnelDiagnosticLog
                    GatewayDiagnosticLog

| where Category ==  "                                    "

| where remoteIP_s == "203.0.113.20"

| where status_s == "Disconnected"

| project TimeGenerated, OperationName, instance_s, Resource, ResourceGroup, _ResourceId
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:


```
Answer Area

AzureMetrics
AzureActivity
AzureDiagnostics

IKEDiagnosticLog
RouteDiagnosticLog
TunnelDiagnosticLog
GatewayDiagnosticLog

| where Category == "
| where remoteIP_s == "203.0.113.20"
| where status_s == "Disconnected"
| project TimeGenerated, OperationName, instance_s, Resource, ResourceGroup, _ResourceId
```
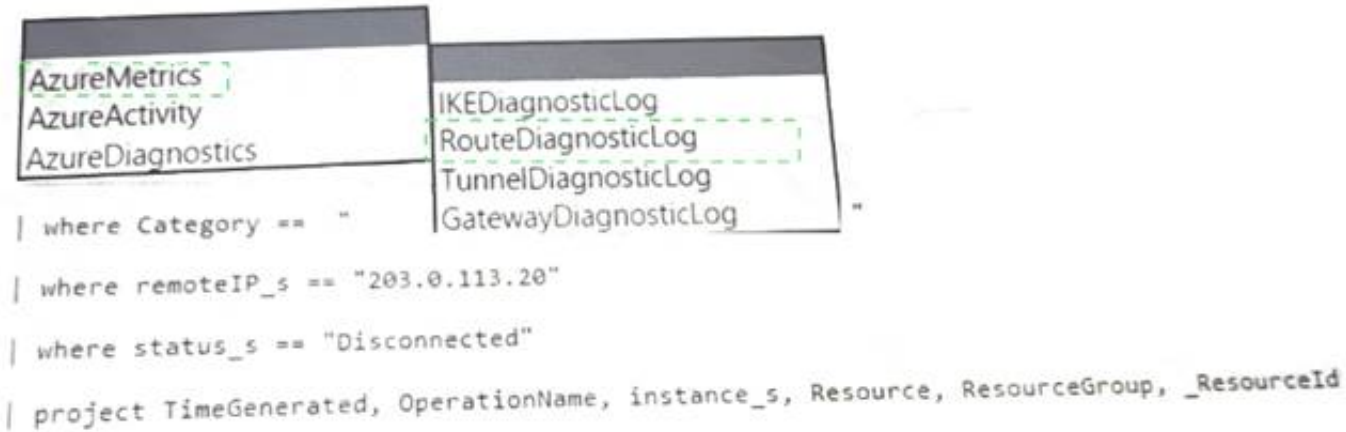
NEW QUESTION 51
A company connects their on-premises network by using Azure VPN Gateway. The on-premises environment includes three VPN devices that separately tunnel to the gateway by using Border Gateway Protocol (BGP).
A new subnet should be unreachable from the on-premises network. You need to implement a solution.
Solution: Configure subnet delegation. Does the solution meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 55
A company has an Azure Virtual Network gateway named VNetGW1. The company enables point-to-site connectivity on VNetGW1. An administrator configures VNetGW1 for the following:
⟫ OpenVPN for the tunnel type.
⟫ Azure certificate for the authentication type.
Users receive a certificate mismatch error when connecting by using a VPN client. You need to resolve the certificate mismatch error.
What should you do?

A. Configure the tunnel type for IKEv2 and OpenVPN on VNetGW1.
B. Create a profile manually, add the server FQDN and reissue the client certificate.
C. Install a Secure Socket Tunneling Protocol (SSTP) VPN client on the user's computers.
D. Configure preshared key for authentication on the VPN profile.

Answer: B

NEW QUESTION 60
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

Answer: B

NEW QUESTION 61
A company has an Azure Virtual Network gateway named VNetGW1. The company enables point-to-site connectivity on VNetGW1. An administrator configures VNetGW1 for the following:
⟫ OpenVPN for the tunnel type.
⟫ Azure certificate for the authentication type.
Users receive a certificate mismatch error when connecting by using a VPN client. You need to resolve the certificate mismatch error.
What should you do?

A. Reissue the client certificate with client authentication enabled.
B. Configure preshared key for authentication on the VPN profile.
C. Install an IKEv2 VPN client on the user's computers.
D. Reissue the client certificate with server authentication enabled.

Answer: D

NEW QUESTION 64
A company has an ExpressRoute gateway between their on-premises site and Azure. The ExpressRoute gateway is on a virtual network named VNet1. The company enables FastPath on the gateway. You associate a network security group (NSG) with all of the subnets.
Users report issues connecting to VM1 from the on-premises environment. VM1 is on a virtual network named VNet2. Virtual network peering is enabled between VNet1 and VNet2.
You create a flow log named FlowLog1 and enable it on the NSG associated with the gateway subnet. You discover that FlowLog1 is not reporting outbound flow traffic.

You need to resolve the issue with FlowLog1. What should you do?

A. Configure FlowLog1 for version 2.
B. Create the storage account for FlowLog1 as a premium block blob.
C. Configure the FlowTimeoutInMinutes property on VNet2 to a non-null value.
D. Enable FlowLog1 in a network security group associated with the network interface of VM1.

Answer: A

NEW QUESTION 66
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

AZ-720 Practice Exam Features:

* AZ-720 Questions and Answers Updated Frequently

* AZ-720 Practice Questions Verified by Expert Senior Certified Staff

* AZ-720 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* AZ-720 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The AZ-720 Practice Test Here