



AZ-720^{Q&As}

Troubleshooting Microsoft Azure Connectivity

Pass Microsoft AZ-720 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/az-720.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



**QUESTION 1**

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

Correct Answer: BE

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 2

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. Enable FlowLog1 in a network security group associated with the subnet of VM1.
- B. Configure the FlowTimeoutInMinutes property on VNet2 to a non-null value.



C. Configure the FlowTimeoutInMinutes property on VNet1 to a non-null value.

D. Configure FlowLog1 for version 2.

Correct Answer: A

According to 2, when FastPath is enabled on an ExpressRoute gateway, network traffic between your on-premises network and your virtual network bypasses the gateway and goes directly to virtual machines in the virtual network. Therefore, if you want to capture outbound flow traffic from VM1, you need to enable flow logging on an NSG associated with the subnet of VM1.

QUESTION 3

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

Correct Answer: C

To troubleshoot an issue with the Phase 1 proposal from an Azure Virtual Network gateway when connecting to a site-to-site VPN connection by reviewing logs, you should analyze the IKE Diagnostic log. Therefore, option C is correct. You should analyze the IKE Diagnostic log.

QUESTION 4

A company plans to use an Azure PaaS service by using Azure Private Link service. The Azure Private Link service and an endpoint have been configured.

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

You need to resolve the connectivity issue.

What should you do?

A. Disable the endpoint network policies.

B. Validate the VPN device.

C. Approve the connection state.



D. Disable the service network policies.

Correct Answer: C

To resolve the connectivity issue, you should approve the connection state. According to 1, Azure Private Link service requires manual approval of connection requests from private endpoints by default. You can approve or reject a connection request by using PowerShell cmdlets or Azure portal.

QUESTION 5

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:

1.

A certificate could not be found

2.

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.

Correct Answer: BFG

[Latest AZ-720 Dumps](#)

[AZ-720 Study Guide](#)

[AZ-720 Exam Questions](#)