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.geekcert.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

SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

A company deploys an ExpressRoute circuit.

You need to verify accepted peering routes from the ExpressRoute circuit.

Which PowerShell cmdlet should you run?

A. Get-AzExpressRouteCrossConnectionPeering

B. Get-AzExpressRouteCircuit

C. Get-AzExpressRouteCircuitPeeringConfig

D. Get-AzExpressRouteCircuitRouteTable

E. Get-AzExpressRouteCircuitStats

Correct Answer: D

To verify accepted peering routes from the ExpressRoute circuit, you should run the PowerShell cmdlet Get-AzExpressRouteCircuitRouteTable. According to 1, this cmdlet returns a list of routes advertised by an ExpressRoute circuit peering. You can specify which peering type (AzurePrivatePeering, AzurePublicPeering, or MicrosoftPeering) and which route table (AdvertisedPublicPrefixes or AdvertisedPublicPrefixesState) you want to view.

QUESTION 2

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?

A. Yes

B. No

Correct Answer: B

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-password-writeback

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.

D. Modify the next hop type of RT12.

Correct Answer: B

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

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.

Correct Answer: B

QUESTION 5

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

1.

West Central US

2.

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.

Correct Answer: A

To ensure that traffic uses global VNet peering instead of ExpressRoute private peering, you should add a user-defined route to the subnets route table. According to 2, global VNet peering allows virtual networks across regions to communicate using private IP addresses as if they were in the same region. However, if there is an existing ExpressRoute private peering between two regions that also have global VNet peering enabled, traffic will prefer ExpressRoute over global VNet peering by default. To override this behavior and force traffic to use global VNet peering instead of ExpressRoute private peering for a specific subnet or virtual network gateway connection, you need to add a user-defined route with a next hop type of Virtual Network Peering.

Latest AZ-720 Dumps AZ-720 VCE Dumps AZ-720 Exam Questions