Free Questions for AZ-700 by go4braindumps

Shared by Blanchard on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

SIMULATION

Task 5

You need to ensure that requests for wwwjelecloud.com from any of your Azure virtual networks resolve to frontdoor1.azurefd.net.

Options:

A- See the Explanation below for step by step instructions

Answer:

A

Explanation:

Here are the steps and explanations for ensuring that requests for wwwjelecloud.com from any of your Azure virtual networks resolve to frontdoor1.azurefd.net:

To use a custom domain with your Azure Front Door, you need to create a CNAME record with your domain provider that points to the Front Door default frontend host.A CNAME record is a type of DNS record that maps a source domain name to a destination domain name1.

To create a CNAME record, you need to sign in to your domain registrar's website and go to the page for managing DNS settings1.

Create a CNAME record with the following information1:

Source domain name: wwwjelecloud.com

Destination domain name: frontdoor1.azurefd.net

Save your changes and wait for the DNS propagation to take effect1.

To verify the custom domain, you need to go to the Azure portal and select your Front Door profile.Then select Domains under Settings and select Add2.

On the Add a domain page, select Non-Azure validated domain as the Domain type and enter wwwjelecloud.com as the Domain name.Then select Add2.

On the Domains page, select wwwjelecloud.com and select Verify.This will check if the CNAME record is correctly configured2.

Once the domain is verified, you can associate it with your Front Door endpoint. On the Domains page, select wwwjelecloud.com and select Associate endpoint.Then select your Front Door endpoint from the drop-down list and select Associate2.

Question 2

Question Type: MultipleChoice

SIMULATION

Task 4

You need to ensure that connections to the storage34280945 storage account can be made by using an IP address in the 10.1.1.0/24 range and the name storage34280945.pnvatelinlcblob.core.windows.net.

Options:

A- See the Explanation below for step by step instructions

Answer:

A

Explanation:

Here are the steps and explanations for ensuring that connections to the storage34280945 storage account can be made by using an IP address in the 10.1.1.0/24 range and the name stor-age34280945.pnvatelinlcblob.core.windows.net:

To allow access from a specific IP address range, you need to configure the Azure Storage firewall and virtual network settings for your storage account.You can do this in the Azure portal by selecting your storage account and then selecting Networking under Settings1.

On the Networking page, select Firewalls and virtual networks, and then select Selected networks under Allow access from1. This will block all access to your storage account except from the networks or resources that you specify.

Under Firewall, select Add rule, and then enter 10.1.1.0/24 as the IP address or range.You can also enter an optional rule name and description1. This will allow access from any IP address in the 10.1.1.0/24 range.

Select Save to apply your changes1.

To map a custom domain name to your storage account, you need to create a CNAME record with your domain provider that points to your storage account endpoint2. A CNAME record is a type of DNS record that maps a source domain name to a destination domain name.

Sign in to your domain registrar's website, and then go to the page for managing DNS settings2.

Create a CNAME record with the following information2:

Source domain name: stor-age34280945.pnvatelinlcblob.core.windows.net

Destination domain name: stor-age34280945.pnvatelinlcblob.core.windows.net

Save your changes and wait for the DNS propagation to take effect2.

To register the custom domain name with Azure, you need to go back to the Azure portal and select your storage account.Then select Custom domain under Blob service2.

On the Custom domain page, enter stor-age34280945.pnvatelinlcblob.core.windows.net as the custom domain name and select Save2.

Question 3

Question Type: MultipleChoice

SIMULATION

Task 3

You plan to implement an Azure application gateway in the East US Azure region. The application gateway will have Web Application Firewall (WAF) enabled.

You need to create a policy that can be linked to the planned application gateway. The policy must block connections from IP addresses in the 131.107.150.0/24 range. You do NOT need to provision the application gateway to complete this task.

Options:

A- See the Explanation below for step by step instructions

Answer:

A

Explanation:

Here are the steps and explanations for creating a policy that can be linked to the planned application gateway and block connections from IP addresses in the 131.107.150.0/24 range:

To create a policy, you need to go to the Azure portal and selectCreate a resource.Search forWAF, selectWeb Application Firewall, then selectCreate1.

On theCreate a WAF policypage,Basicstab, enter or select the following information and accept the defaults for the remaining settings:

Policy for: Regional WAF (Application Gateway)

Subscription: Select your subscription name

Resource group: Select your resource group

Policy name: Type a unique name for your WAF policy

On theCustom rulestab, selectAdd a ruleto create a custom rule that blocks connections from IP addresses in the 131.107.150.0/24 range2. Enter or select the following information for the custom rule:

Rule name: Type a unique name for your custom rule

Priority: Type a number that indicates the order of evaluation for this rule

Rule type: Select Match rule

Match variable: Select RemoteAddr

Operator: Select IPMatch

Match values: Type 131.107.150.0/24

Action: Select Block

On theReview + createtab, review your settings and selectCreateto create your WAF policy1.

To link your policy to the planned application gateway, you need to go to theApplication Gatewayservice in the Azure portal and select your application gateway3.

On theWeb application firewalltab, select your WAF policy from the drop-down list and selectSave

Question 4

Question Type: **MultipleChoice**

SIMULATION

Task 2

You need to create an Azure Firewall instance named FW1 that meets the following requirements:

* Has an IP address from the address range of 10.1.255.0/24

* Uses a new Premium firewall policy named FW-pohcy1

* Routes traffic directly to the internet

Options:

A- See the Explanation below for step by step instructions

Answer:

A

Explanation:

To create an Azure Firewall instance, you need to go to the Azure portal and select Create a resource. Type firewall in the search box and press Enter.Select Firewall and then select Create1.

To assign an IP address from the address range of 10.1.255.0/24 to the firewall, you need to select a public IP address that belongs to that range.You can either create a new public IP address or use an existing one1.

To use a new Premium firewall policy named FW-policy1, you need to select Premium as the Firewall tier and create a new policy with the name FW-policy12.A Premium firewall policy allows you to configure advanced features such as TLS Inspection, IDPS, URL Filtering, and Web Categories3.

To route traffic directly to the internet, you need to enable SNAT (Source Network Address Translation) for the firewall.SNAT allows the firewall to use its public IP address as the source address for outbound traffic4.

Question 5

Question Type: MultipleChoice

SIMULATION

Task 1

You plan to deploy a firewall to subnetl-2. The firewall will have an IP address of 10.1.2.4.

You need to ensure that traffic from subnetl-1 to the IP address range of 192.168.10.0/24 is routed through the firewall that will be deployed to subnetl-2. The solution must be achieved without using dynamic routing protocols.

Options:

A- See the Explanation below for step by step instructions

Answer:

A

Explanation:

To deploy a firewall to subnetl-2, you need to create a network virtual appliance (NVA) in the same virtual network as subnetl-2.An NVA is a virtual machine that performs network functions, such as firewall, routing, or load balancing1.

To create an NVA, you need to create a virtual machine in the Azure portal and select an image that has the firewall software installed.You can choose from the Azure Marketplace or upload your own image2.

To assign the IP address of 10.1.2.4 to the NVA, you need to create a static private IP address for the network interface of the virtual machine.You can do this in the IP configurations settings of the network interface3.

To ensure that traffic from subnetl-1 to the IP address range of 192.168.10.0/24 is routed through the NVA, you need to create a user-defined route (UDR) table and associate it with subnetl-1.A UDR table allows you to override the default routing behavior of Azure and specify custom routes for your subnets4.

To create a UDR table, you need to go to the Route tables service in the Azure portal and select + Create.You can give a name and a resource group for the route table5.

To create a custom route, you need to select Routes in the route table and select + Add.You can enter the following information for the route5:

Destination: 192.168.10.0/24

Next hop type: Virtual appliance

Next hop address: 10.1.2.4

To associate the route table with subnetl-1, you need to select Subnets in the route table and select + Associate.You can select the virtual network and subnet that you want to associate with the route table5.

Question 6

Question Type: MultipleChoice

You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains the following subnets.

* AzureFirewallSubnet

* GatewaySubnet

* Subnet 1

* Subnet2

* Subnet3

Subnet2 has a delegation to the Microsoft.Web/serverfarms service. The subscription contains the resources shown in the following table.

Name	Type	Connected to
AZVNGW1	Azure VPN Gateway	GatewaySubnet
AZFW1	Azure Firewall Premium	AzureFirewallSubnet
VMSS1	Virtual machine scale set	Subnet1

You need to implement an Azure application gateway named AG1 that will be integrated with an Azure Web Application Firewall (WAF). AG1 will be used to publish VMSS1.

To which subnet should you connect AG1?

Options:

A- Subrwt2

B- Subnet 1

C- Subnet3

D- AzureFjrewall Subnet

E- GatewaySubnet

Answer:

C

Explanation:

Topic 4, Labs / Tasks

Question 7

Question Type: MultipleChoice

You have an Azure Private Link service named PL1 that uses an Azure load balancer named LB1. You need to ensure that PL1 can support a higher volume of outbound traffic. What should you do?

Options:

A- Redeploy LB1 with a different SKU.

B- Increase the number of NAT IP addresses assigned to PL1.

C- Deploy an Azure Application Gateway v2 instance to the source NAT subnet.

D- Increase the number of frontend IP configurations for LB1.

Answer:

B

Question 8

Question Type: Hotspot

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
VNet1	Virtual network	In the West Europe Azure region
VNet2	Virtual network	In the East US Azure region
VM1	Virtual machine	On VNet1
VM2	Virtual machine	On VNet1
VM3	Virtual machine	On VNet2
VM4	Virtual machine	On VNet2

ements.

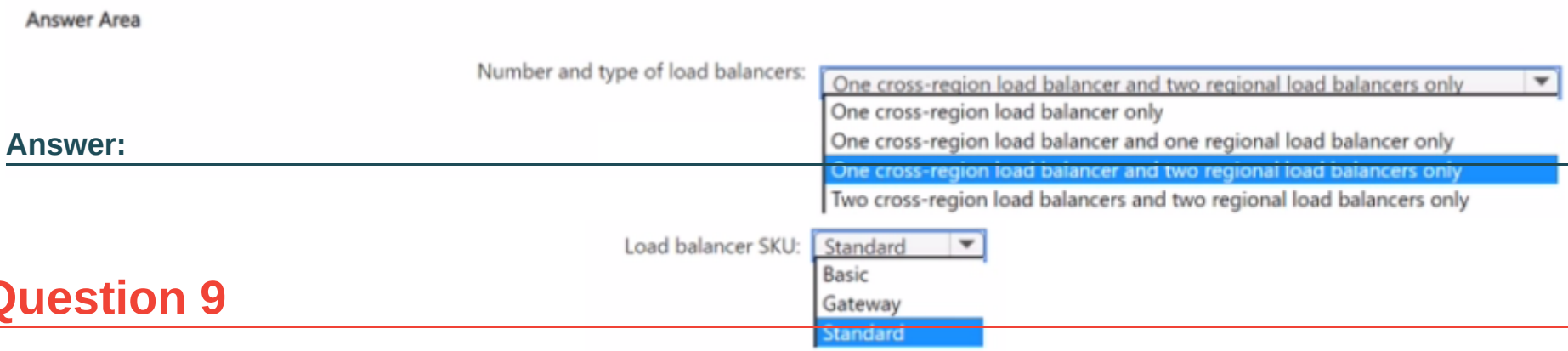
* App1 must be available if an Azure region fails.

* Costs must be minimized.

You need to implement a global load balancer solution for App.

What should you configure? To answer, select the appropriate options in the answer area

NOTE: Bach correct answer is worth one point.



Answer:

Question 9

Question Type: MultipleChoice

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription that contains an Azure Virtual WAN named VWAN1. VWAN1 contains a hub named Hub1.

Hub1 has a security status of Unsecured.

You need to ensure that the security status of Hub1 is marked as Secured.

Solution: You implement Azure Web Application Firewall (WAF).

Does this meet the requirement?

Options:

A- Yes

B- No

Answer:

B