Free Questions for AZ-700 by dumpshq

Shared by Watson on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

Task 9

You need to ensure that subnet4-3 can accommodate 507 hosts.

Options:

A) See the Explanationbelow for step by step in structions

Answer:

A

Explanation:

Here are the steps and explanations for ensuring that subnet4-3 can accommodate 507 hosts:

To determine the subnet size that can accommodate 507 hosts, you need to use the formula:number of hosts = 2^(32 - n) - 2, wherenis the number of bits in the subnet mask1. You need to find the value ofnthat satisfies this equation for 507 hosts.

To solve this equation, you can use trial and error or a binary search method. For example, you can start withn = 24, which is the default subnet mask for Class C networks. Then, plug in the value ofninto the formula and see if it is too big or too small for 507 hosts.

If you tryn = 24, you getnumber of hosts = 2^(32 - 24) - 2 = 254, which is too small. You need to increase the value ofnto get a larger number of hosts.

If you tryn = 25, you getnumber of hosts = 2^(32 - 25) - 2 = 510, which is just enough to accommodate 507 hosts. You can stop here or try a smaller value ofnto see if it still works.

If you tryn = 26, you getnumber of hosts = 2^(32 - 26) - 2 = 254, which is too small again. You need to decrease the value ofnto get a larger number of hosts.

Therefore, the smallest value ofnthat can accommodate 507 hosts isn = 25. This means that the subnet mask for subnet4-3 should be/25or255.255.255.128in dot-decimal notation1.

To change the subnet mask for subnet4-3, you need to go to the Azure portal and select your virtual network. Then select Subnets under Settings and select subnet4-3 from the list2.

On the Edit subnet page, under Address range (CIDR block), change the value from/24to/25. Then select Save2.

Question 2

Question Type: **MultipleChoice**

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 Explanationbelow for step by step in structions

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 3

Question Type: MultipleChoice

Task 7

You need to ensure that hosts on VNET2 can access hosts on both VNET1 and VNET3. The solution must prevent hosts on VNET1 and VNET3 from communicating through VNET2.

Options:

A) See the Explanationbelow for step by step in structions

Answer:

A

Explanation:

Here are the steps and explanations for ensuring that hosts on VNET2 can access hosts on both VNET1 and VNET3, but hosts on VNET1 and VNET3 cannot communicate through VNET2:

To connect different virtual networks in Azure, you need to use virtual network peering. Virtual network peering allows you to create low-latency, high-bandwidth connections between virtual networks without using gateways or the internet1.

To create a virtual network peering, you need to go to the Azure portal and select your virtual network. Then select Peerings under Settings and select + Add2.

On the Add peering page, enter or select the following information:

Name: Type a unique name for the peering from the source virtual network to the destination virtual network.

Virtual network deployment model: Select Resource manager.

Subscription: Select the subscription that contains the destination virtual network.

Virtual network: Select the destination virtual network from the list or enter its resource ID.

Name of the peering from [destination virtual network] to [source virtual network]: Type a unique name for the peering from the destination virtual network to the source virtual network.

Configure virtual network access settings: Select Enabled to allow resources in both virtual networks to communicate with each other.

Allow forwarded traffic: Select Disabled to prevent traffic that originates from outside either of the peered virtual networks from being forwarded through either of them.

Allow gateway transit: Select Disabled to prevent either of the peered virtual networks from using a gateway in the other virtual network.

Use remote gateways: Select Disabled to prevent either of the peered virtual networks from using a gateway in the other virtual network as a transit point to another network.

Select Add to create the peering2.

Repeat the previous steps to create peerings between VNET2 and VNET1, and between VNET2 and VNET3. This will allow hosts on VNET2 to access hosts on both VNET1 and VNET3.

To prevent hosts on VNET1 and VNET3 from communicating through VNET2, you need to use network security groups (NSGs) to filter traffic between subnets. NSGs are rules that allow or deny inbound or outbound traffic based on source or destination IP address, port, or protocol3.

To create an NSG, you need to go to the Azure portal and select Create a resource. Search for network security group and select Network security group. Then select Create4.

On the Create a network security group page, enter or select the following information:

Subscription: Select your subscription name.

Resource group: Select your resource group name.

Name: Type a unique name for your NSG.

Region: Select the same region as your virtual networks.

Select Review + create and then select Create to create your NSG4.

To add rules to your NSG, you need to go to the Network security groups service in the Azure portal and select your NSG. Then select Inbound security rules or Outbound security rules under Settings and select + Add4.

On the Add inbound security rule page or Add outbound security rule page, enter or select the following information:

Source or Destination: Select CIDR block.

Source CIDR blocks or Destination CIDR blocks: Enter the IP address range of the source or destination subnet that you want to filter. For example, 10.0.1.0/24 for VNET1 subnet 1, 10.0.2.0/24 for VNET2 subnet 1, and 10.0.3.0/24 for VNET3 subnet 1.

Protocol: Select Any to apply the rule to any protocol.

Action: Select Deny to block traffic from or to the source or destination subnet.

Priority: Enter a number between 100 and 4096 that indicates the order of evaluation for this rule. Lower numbers have higher priority than higher numbers.

Name: Type a unique name for your rule.

Select Add to create your rule4.

Repeat the previous steps to create inbound and outbound rules for your NSG that deny traffic between VNET1 and VNET3 subnets. For example, you can create an inbound rule that denies traffic from 10.0.1.0/24 (VNET1 subnet 1) to 10.0.3.0/24 (VNET3 subnet 1), and an outbound rule that denies traffic from 10.0.3.0/24 (VNET3 subnet 1) to 10.0.1.0/24 (VNET1 subnet 1).

To associate your NSG with a subnet, you need to go to the Virtual networks service in the Azure portal and select your virtual network. Then select Subnets under Settings and select the subnet that you want to associate with your NSG5.

On the Edit subnet page, under Network security group, select your NSG from the drop-down list. Then select Save5.

Repeat the previous steps to associate your NSG with the subnets in VNET1 and VNET3 that you want to isolate from each other.

Question 4

Question Type: MultipleChoice

Task 6

You need to ensure that all hosts deployed to subnet3-2 connect to the internet by using the same static public IP address. The solution must minimize administrative effort when adding hosts to the subnet.

Options:

A) See the Explanationbelow for step by step in structions

Answer:

A

Explanation:

Here are the steps and explanations for ensuring that all hosts deployed to subnet3-2 connect to the internet by using the same static public IP address:

To use the same static public IP address for multiple hosts, you need to create a NAT gateway and associate it with subnet3-2. A NAT gateway is a resource that performs network address translation (NAT) for outbound traffic from a subnet1. It allows you to use a single public IP address for multiple private IP addresses2.

To create a NAT gateway, you need to go to the Azure portal and selectCreate a resource. Search forNAT gateway, selectNAT gateway, then selectCreate3.

On theCreate a NAT gatewaypage, enter or select the following information and accept the defaults for the remaining settings:

Subscription: Select your subscription name

Resource group: Select your resource group

Name: Type a unique name for your NAT gateway

Region: Select the same region as your virtual network

Public IP address: SelectCreate newand type a name for your public IP address. SelectStandardas the SKU andStaticas the assignment method4.

SelectReview + createand then selectCreateto create your NAT gateway3.

To associate the NAT gateway with subnet3-2, you need to go to theVirtual networksservice in the Azure portal and select your virtual network.

On theVirtual networkpage, selectSubnetsunderSettings, and then select subnet3-2 from the list.

On theEdit subnetpage, underNAT gateway, select your NAT gateway from the drop-down list. Then selectSave.

Question 5

Question Type: MultipleChoice

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 Explanationbelow for step by step in structions

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 6

Question Type: MultipleChoice

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 Explanationbelow for step by step in structions

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 7

Question Type: **MultipleChoice**

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 Explanationbelow for step by step in structions

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