

Free Questions for AZ-700

Shared by Hoffman on 04-10-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

SIMULATION

Task 11

You need to ensure that only hosts on VNET1 can access the slcnage42150372 storage account. The solution must ensure that access occurs over the Azure backbone network.

Options:

A- See the Explanation below for step by step instructions

Answer:

A

Explanation:

To ensure that only hosts on VNET1 can access the slcnage42150372 storage account and that access occurs over the Azure backbone network, you can use Azure Private Endpoints. This method secures the connection by assigning a private IP address from your virtual

network to the storage account, ensuring that traffic does not traverse the public internet.

Step-by-Step Solution

Step 1: Create a Private Endpoint for the Storage Account

Navigate to the Azure Portal.

Search for "Storage accounts" and select the `slcnage42150372` storage account.

In the storage account blade, select "Networking" under the "Security + networking" section.

Under "Private endpoint connections", click on "Add private endpoint".

Enter the following details:

Name: Enter a name for the private endpoint (e.g., `PrivateEndpoint-VNET1`).

Region: Select the same region as your virtual network (VNET1).

Click on "Next: Resource".

Step 2: Configure the Resource

Select "Target sub-resource": Choose the storage service you want to connect to (e.g., `blob`, `file`, `queue`, `table`).

Click on "Next: Virtual network".

Step 3: Select the Virtual Network and Subnet

Select the virtual network: Choose VNET1.

Select the subnet: Choose the appropriate subnet within VNET1.

Click on "Next: Configuration".

Step 4: Configure DNS Integration (Optional)

Configure DNS settings if needed to ensure proper name resolution within your virtual network.

Click on "Next: Tags", add any tags if necessary, and then click on "Review + create".

Review your settings and click on "Create".

Step 5: Restrict Public Network Access

Navigate back to the storage account.

Select "Networking" under the "Security + networking" section.

Under "Firewalls and virtual networks", select "Selected networks".

Ensure that only VNET1 is listed under the virtual networks section.

Click on "Save".

Explanation

Private Endpoints: These provide secure connectivity to Azure services by assigning a private IP address from your VNet to the service, ensuring that traffic stays within the Azure backbone network¹².

Firewall and Virtual Networks: Configuring the storage account to allow access only from selected networks (VNET1) ensures that no other network can access the storage account³.

By following these steps, you can ensure that only hosts on VNET1 can access the storage account, and that all access occurs over the secure Azure backbone network.

Question 2

Question Type: MultipleChoice

SIMULATION

Task 10

You plan to deploy several virtual machines to subnet1-2.

You need to prevent all Azure hosts outside of subnet1-2 from connecting to TCP port 5585 on hosts on subnet1-2. The solution must minimize administrative effort.

Options:

A- See the Explanation below for step by step instructions

Answer:

A

Explanation:

To prevent all Azure hosts outside of subnet1-2 from connecting to TCP port 5585 on hosts within subnet1-2, you can use a Network Security Group (NSG). This solution is straightforward and minimizes administrative effort.

Step-by-Step Solution

Step 1: Create a Network Security Group (NSG)

Navigate to the Azure Portal.

Search for "Network security groups" and select it.

Click on "Create".

Enter the following details:

Subscription: Select your subscription.

Resource Group: Select an existing resource group or create a new one.

Name: Enter a name for the NSG (e.g.,NSG-Subnet1-2).

Region: Select the region where your virtual network is located.

Click on "Review + create"and then"Create".

Step 2: Create an Inbound Security Rule

Navigate to the newly created NSG.

Select "Inbound security rules"from the left-hand menu.

Click on "Add"to create a new rule.

Enter the following details:

Source: SelectService Tag.

Source Service Tag: SelectVirtualNetwork.

Source port ranges: Leave as*.

Destination: SelectIP Addresses.

Destination IP addresses/CIDR ranges: Enter the IP range of subnet1-2 (e.g.,10.1.2.0/24).

Destination port ranges: Enter5585.

Protocol: SelectTCP.

Action: SelectDeny.

Priority: Enter a priority value (e.g.,100).

Name: Enter a name for the rule (e.g.,Deny-TCP-5585).

Click on "Add"to create the rule.

Step 3: Associate the NSG with Subnet1-2

Navigate to the virtual networkthat contains subnet1-2.

Select "Subnets"from the left-hand menu.

Select subnet1-2from the list of subnets.

Click on "Network security group".

Select the NSGyou created (NSG-Subnet1-2).

Click on "Save".

Explanation

[Network Security Group \(NSG\)](#): NSGs are used to filter network traffic to and from Azure resources in an Azure virtual network.They contain security rules that allow or deny inbound and outbound traffic based on source and destination IP addresses, port, and protocol1.

Inbound Security Rule: By creating a rule that denies traffic on TCP port 5585 from any source outside of subnet1-2, you ensure that only hosts within subnet1-2 can connect to this port.

Association with Subnet: Associating the NSG with subnet1-2 ensures that the security rules are applied to all resources within this subnet.

By following these steps, you can effectively prevent all Azure hosts outside of subnet1-2 from connecting to TCP port 5585 on hosts within subnet1-2, while minimizing administrative effort.

Question 3

Question Type: MultipleChoice

SIMULATION

Task 9

You plan to use VNET4 for an Azure API Management implementation.

You need to configure a policy that can be used by an Azure application gateway to protect against known web attack vectors. The policy must only allow requests that originate from IP addresses in Canada

a. You do NOT need to create the application gateway to complete this task.

Options:

A- See the Explanation below for step by step instructions

Answer:

A

Explanation:

To configure a policy in Azure API Management that can be used by an Azure Application Gateway to protect against known web attack vectors and only allow requests from IP addresses in Canada, follow these steps:

Step-by-Step Solution

Step 1: Create or Access Your API Management Instance

Navigate to the Azure Portal.

Search for "API Management services" and select your API Management instance.

Step 2: Configure the Policy

In the API Management instance, go to the "APIs" section.

Select the API you want to apply the policy to.

Go to the "Design" tab.

Select "All operations" if you want to apply the policy to all operations, or select a specific operation.

Step 3: Add the Inbound Policy

In the Inbound processing section, click on "+ Add policy".

Select "IP filter" from the list of policies.

Add the IP address ranges for Canada. You can find the IP ranges for Canada from a reliable source or use a service that provides this information.

Here is an example of the XML configuration for the policy:

```
<inbound>
```

```
<ip-filter action='allow'>
```

```
<!-- Add other Canadian IP ranges as needed -->
```

```
</ip-filter>
```

```
<ip-filter action='deny'>
```

```
</ip-filter>
```

</inbound>

Save the policy to apply the changes.

Explanation

IP Filter Policy: This policy allows you to filter incoming requests based on their IP addresses. By specifying the IP ranges for Canada, you ensure that only requests originating from these IPs are allowed.

Inbound Processing: Applying the policy in the inbound section ensures that the requests are filtered before they reach your API.

By following these steps, you can configure a policy in Azure API Management that restricts access to your API to only those requests originating from IP addresses in Canada, thereby enhancing security and compliance

Question 4

Question Type: MultipleChoice

SIMULATION

Task 8

You plan to deploy an appliance to subnet3-2- The appliance will perform packet inspection and will have an IP address of 10.3.2.100.

You need to ensure that all traffic to the internet from subnet3-1 is forwarded to the appliance for inspection.

Options:

A- See the Explanation below for step by step instructions

Answer:

A

Explanation:

To ensure that all traffic to the internet from subnet3-1 is forwarded to the appliance in subnet3-2 for packet inspection, you can use User-Defined Routes (UDRs) to direct the traffic. Here's how you can do it:

Step-by-Step Solution

Step 1: Create a Route Table

Navigate to the Azure Portal.

Search for "Route tables" and select it.

Click on "Create".

Enter the following details:

Subscription: Select your subscription.

Resource Group: Select an existing resource group or create a new one.

Name: Enter a name for the route table (e.g.,RouteTable-Subnet3-1).

Region: Select the region where your virtual network is located.

Click on "Review + create"and then"Create".

Step 2: Add a Route to the Route Table

Navigate to the newly created route table.

Select "Routes"from the left-hand menu.

Click on "Add"to create a new route.

Enter the following details:

Route name: Enter a name for the route (e.g.,RouteToAppliance).

Address prefix: Enter0.0.0.0/0to route all internet traffic.

Next hop type: SelectVirtual appliance.

Next hop address: Enter the IP address of the appliance (10.3.2.100).

Click on "OK"to add the route.

Step 3: Associate the Route Table with Subnet3-1

Navigate to the route table.

Select "Subnets" from the left-hand menu.

Click on "Associate".

Select the virtual network that contains subnet3-1.

Select subnet3-1 from the list of subnets.

Click on "OK".

Explanation

User-Defined Routes (UDRs): These allow you to control the routing of traffic within your virtual network. By defining a route that directs all internet-bound traffic to the appliance, you ensure that the traffic is inspected before it reaches the internet¹.

Virtual Appliance: This is a network appliance that performs specific functions, such as packet inspection, and is treated as a next hop in the routing table².

Route Table Association: Associating the route table with subnet3-1 ensures that all traffic from this subnet follows the defined routes.

By following these steps, you can ensure that all internet-bound traffic from subnet3-1 is forwarded to the appliance in subnet3-2 for inspection, thereby enhancing your network security.

Question 5

Question Type: MultipleChoice

SIMULATION

Task 7

You plan to deploy 100 virtual machines to subnet4-1. The virtual machines will NOT be assigned a public IP address. The virtual machines will call the same API, which is hosted by a third party. The virtual machines will make more than 10,000 calls per minute to the API.

You need to minimize the risk of SNAT port exhaustion. The solution must minimize administrative effort.

Options:

A- See the Explanation below for step by step instructions

Answer:

A

Explanation:

To minimize the risk of SNAT port exhaustion for your 100 virtual machines in subnet4-1, while ensuring minimal administrative effort, you can use an Azure NAT Gateway. This service provides scalable and resilient outbound connectivity for virtual networks, dynamically allocating SNAT ports to avoid exhaustion.

Step-by-Step Solution

Step 1: Create a NAT Gateway

Navigate to the Azure Portal.

Search for "NAT gateways" and select it.

Click on "Create".

Enter the following details:

Subscription: Select your subscription.

Resource Group: Select an existing resource group or create a new one.

Name: Enter a name for the NAT gateway (e.g., NATGateway-Subnet4-1).

Region: Select the region where your virtual network is located.

Click on "Next: Outbound IP".

Step 2: Configure Outbound IP Addresses

Choose whether to use existing public IP addresses or create new ones.

If creating new ones, click on "Add new" and configure the new public IP addresses.

Click on "Next: Subnet".

Step 3: Associate the NAT Gateway with Subnet4-1

Click on "Associate subnet".

Select the virtual network that contains subnet4-1.

Select subnet4-1 from the list of subnets.

Click on "OK".

Step 4: Review and Create

Review your settings to ensure everything is correct.

Click on "Review + create" and then "Create".

Explanation

[Azure NAT Gateway](#): This service provides outbound connectivity for virtual networks, dynamically allocating SNAT ports across all VM instances within a subnet. This dynamic allocation helps prevent SNAT port exhaustion, especially in scenarios with high outbound connection volumes¹².

[Dynamic SNAT Port Allocation](#): Unlike static allocation methods, NAT Gateway dynamically allocates SNAT ports based on demand, ensuring efficient use of available ports and reducing the risk of exhaustion².

By following these steps, you can ensure that your 100 virtual machines in subnet4-1 can make the necessary API calls without running into SNAT port exhaustion, all while minimizing administrative effort.

Question 6

Question Type: MultipleChoice

SIMULATION

Task 6

You have two servers that are each hosted by a separate service provider in New York and Germany. The server hosted in New York is accessible by using a host name of ny.contoso.com. The server hosted in Germany is accessible by using a host name of de.contoso.com.

You need to provide a single host name to access both servers. The solution must ensure that traffic originating from Germany is routed to de.contoso.com. All other traffic must be routed to ny.contoso.com.

Options:

A- See the Explanation below for step by step instructions

Answer:

A

Explanation:

To provide a single host name that routes traffic based on the origin, you can use Azure Traffic Manager. This service allows you to route traffic to different endpoints based on various routing methods, including geographic routing.

Step-by-Step Solution

Step 1: Create a Traffic Manager Profile

Navigate to the Azure Portal.

Search for "Traffic Manager profiles" and select it.

Click on "Create".

Enter the following details:

Name: Enter a name for the Traffic Manager profile (e.g., ContosoTrafficManager).

Routing method: Select Geographic.

Subscription: Select your subscription.

Resource group: Select an existing resource group or create a new one.

Resource group location: Choose a location (this does not affect the routing).

Click on "Create".

Step 2: Configure Endpoints

Navigate to the newly created Traffic Manager profile.

Select "Endpoints" from the left-hand menu.

Click on "Add" to add a new endpoint.

Enter the following details:

Type: Select External endpoint.

Name: Enter a name for the endpoint (e.g., NewYorkEndpoint).

FQDN: Enterny.contoso.com.

Geographic region: Select "World" (this will be adjusted later).

Click on "Add" to save the endpoint.

Repeat the process to add the second endpoint:

Type: Select External endpoint.

Name: Enter a name for the endpoint (e.g., GermanyEndpoint).

FQDN: Enterde.contoso.com.

Geographic region: SelectEurope.

Step 3: Adjust Geographic Routing

Navigate to the Traffic Manager profile.

Select "Configuration" from the left-hand menu.

Under "Geographic routing", adjust the regions:

For theGermanyEndpoint, ensure that the geographic region is set toEurope.

For theNewYorkEndpoint, ensure that the geographic region is set toWorld(excluding Europe).

Step 4: Test the Configuration

Use a DNS query tool to test the routing.

From a location in Germany, query the Traffic Manager profile's DNS name and ensure it resolves tode.contoso.com.

From a location outside Europe, query the Traffic Manager profile's DNS name and ensure it resolves tony.contoso.com.

Explanation

Azure Traffic Manager: This service uses DNS to direct client requests to the most appropriate endpoint based on the routing method you choose. Geographic routing ensures that traffic is directed based on the origin of the request.

Geographic Routing: This method allows you to route traffic based on the geographic location of the DNS query origin, ensuring that users are directed to the nearest or most appropriate endpoint.

By following these steps, you can provide a single host name that routes traffic to `de.contoso.com` for users in Germany and `us.contoso.com` for users from other locations, ensuring efficient and appropriate traffic management.

Question 7

Question Type: MultipleChoice

SIMULATION

Task 5

You need to archive all the metrics of VNET1 to an existing storage account.

Options:

A- See the Explanation below for step by step instructions

Answer:

A

Explanation:

To archive all the metrics of VNET1 to an existing storage account, you can use Azure Monitor's diagnostic settings. Here's how you can do it:

Step-by-Step Solution

Step 1: Navigate to VNET1 in the Azure Portal

Open the Azure Portal.

Search for "Virtual networks" and select VNET1 from the list.

Step 2: Configure Diagnostic Settings

In the VNET1 blade, select "Diagnostic settings" under the "Monitoring" section.

Click on "Add diagnostic setting".

Step 3: Set Up the Diagnostic Setting

Enter a name for the diagnostic setting (e.g., VNET1-Metrics-Archive).

Select the metrics you want to archive. You can choose from various metrics like TotalBytesReceived, TotalBytesSent, etc.

Under "Destination details", select "Archive to a storage account".

Choose the existing storage account where you want to archive the metrics.

Configure the retention period if needed.

Step 4: Save the Configuration

Review your settings to ensure everything is correct.

Click on "Save" to apply the diagnostic setting.

Explanation

Diagnostic Settings: These allow you to collect and route metrics and logs from your Azure resources to various destinations, including storage accounts, Log Analytics workspaces, and Event Hubs.

Metrics: Metrics provide numerical data about the performance and health of your resources. Archiving these metrics helps in long-term analysis and compliance.

Storage Account: Using an existing storage account ensures that the metrics are stored securely and can be accessed for future analysis.

By following these steps, you can ensure that all the metrics of VNET1 are archived to your existing storage account, enabling you to monitor and analyze the performance and health of your virtual network over time.

Question 8

Question Type: MultipleChoice

SIMULATION

Task 4

You need to ensure that the owner of VNET3 receives an alert if an administrative operation is performed on the virtual network.

Options:

A- See the Explanation below for step by step instructions

Answer:

A

Explanation:

To ensure that the owner of VNET3 receives an alert whenever an administrative operation is performed on the virtual network, you can set up an Activity Log Alert in Azure Monitor. Here's how you can do it:

Step-by-Step Solution

Step 1: Create an Activity Log Alert

Navigate to the Azure Portal.

Search for "Monitor" and select it.

In the Monitor blade, select "Alerts" from the left-hand menu.

Click on "New alert rule".

Step 2: Configure the Alert Rule

Select the Scope:

Click on "Select resource".

Choose "Virtual Network" as the resource type.

Select VNET3 from the list of virtual networks.

Define the Condition:

Click on "Add condition".

In the "Signal type" dropdown, select "Activity Log".

Choose "Administrative" as the category.

Select the specific operations you want to monitor (e.g., Microsoft.Network/virtualNetworks/write for any write operations on the virtual network).

Set the Alert Details:

Enter a name for the alert rule (e.g., VNET3 Admin Operations Alert).

Provide a description if needed.

Configure the Action Group:

Click on "Add action group".

Enter a name for the action group.

Select the action type (e.g., Email/SMS/Push/Voice).

Enter the details of the recipient (e.g., the email address of the owner of VNET3).

Review and Create:

Review the alert rule settings.

Click on "Create alert rule".

Explanation

Activity Log Alerts: These alerts notify you when specific operations are performed on your Azure resources. By setting up an alert for administrative operations, you ensure that any changes to VNET3 are promptly reported.

Action Groups: These define the actions to take when an alert is triggered. You can configure notifications via email, SMS, or other methods to ensure the owner of VNET3 is informed immediately.

Administrative Operations: Monitoring these operations helps in tracking changes and maintaining the security and integrity of your virtual network.

By following these steps, you can ensure that the owner of VNET3 receives timely alerts for any administrative operations performed on the virtual network, helping to maintain oversight and security.

Question 9

Question Type: MultipleChoice

SIMULATION

Task 3

You need to ensure that hosts on VNET1 and VNET2 can communicate. The solution must minimize latency between the virtual networks.

Options:

A- See the Explanation below for step by step instructions

Answer:

A

Explanation:

To ensure that hosts on VNET1 and VNET2 can communicate with minimal latency, you can use Virtual Network Peering. This method connects the two virtual networks directly through the Microsoft backbone network, ensuring low-latency and high-bandwidth communication.

Step-by-Step Solution

Step 1: Set Up Virtual Network Peering

Navigate to the Azure Portal.

Search for "Virtual networks" and select VNET1.

In the left-hand menu, select "Peerings" under the "Settings" section.

Click on "Add" to create a new peering.

Enter the following details:

Name: Enter a name for the peering (e.g., VNET1-to-VNET2).

Peer virtual network: Select VNET2.

Allow virtual network access: Ensure this is enabled.

Allow forwarded traffic: Enable if needed.

Allow gateway transit: Enable if needed.

Click on "Add".

Step 2: Configure Peering on VNET2

Navigate to VNET2 in the Azure Portal.

In the left-hand menu, select "Peerings" under the "Settings" section.

Click on "Add" to create a new peering.

Enter the following details:

Name: Enter a name for the peering (e.g., VNET2-to-VNET1).

Peer virtual network: Select VNET1.

Allow virtual network access: Ensure this is enabled.

Allow forwarded traffic: Enable if needed.

Allow gateway transit: Enable if needed.

Click on "Add".

Explanation

Virtual Network Peering: This feature connects two virtual networks in the same or different regions, allowing resources in both networks to communicate with each other as if they were part of the same network. The traffic between peered virtual networks uses the Microsoft backbone infrastructure, ensuring low latency and high bandwidth¹².

Allow Virtual Network Access: This setting ensures that the virtual networks can communicate with each other.

Allow Forwarded Traffic: This setting allows traffic forwarded from a network security appliance in the peered virtual network.

Allow Gateway Transit: This setting allows the peered virtual network to use the gateway in the local virtual network.

By following these steps, you can ensure that hosts on VNET1 and VNET2 can communicate with minimal latency, leveraging the high-speed Microsoft backbone network.

Question 10

Question Type: MultipleChoice

SIMULATION

Task 2

You need to ensure that you can deploy Azure virtual machines to the France Central Azure region. The solution must ensure that virtual machines in the France Central region are in a network segment that has an IP address range of 10.5.1.0/24.

Options:

A- See the Explanation below for step by step instructions

Answer:

A

Explanation:

To deploy Azure virtual machines to the France Central region and ensure they are in a network segment with an IP address range of 10.5.1.0/24, follow these steps:

Step-by-Step Solution

Step 1: Create a Virtual Network in France Central

Navigate to the Azure Portal.

Search for "Virtual networks" in the search bar and select it.

Click on "Create".

Enter the following details:

Subscription: Select your subscription.

Resource Group: Select an existing resource group or create a new one.

Name: Enter a name for the virtual network (e.g., VNet-FranceCentral).

Region: Select France Central.

Click on "Next: IP Addresses".

Step 2: Configure the Address Space and Subnet

In the IP Addresses tab, enter the address space as 10.5.1.0/24.

Click on "Add subnet".

Enter the following details:

Subnet name: Enter a name for the subnet (e.g., Subnet-1).

Subnet address range: Enter 10.5.1.0/24.

Click on "Add".

Click on "Review + create" and then "Create".

Step 3: Deploy Virtual Machines to the Virtual Network

Navigate to the Azure Portal.

Search for "Virtual machines" in the search bar and select it.

Click on "Create" and then "Azure virtual machine".

Enter the following details:

Subscription: Select your subscription.

Resource Group: Select the same resource group used for the virtual network.

Virtual machine name: Enter a name for the VM.

Region: Select France Central.

Image: Select the desired OS image.

Size: Select the appropriate VM size.

Click on "Next: Disks", configure the disks as needed, and then click on "Next: Networking".

In the Networking tab, select the virtual network (VNet-FranceCentral) and subnet (Subnet-1) created earlier.

Complete the remaining configuration steps and click on "Review + create" and then "Create".

Explanation

Virtual Network: A virtual network in Azure allows you to create a logically isolated network that can host your Azure resources.

Address Space: The address space 10.5.1.0/24 ensures that the VMs are in a specific network segment.

Subnet: Subnets allow you to segment the virtual network into smaller, manageable sections.

Region: Deploying the virtual network and VMs in the France Central region ensures that the resources are physically located in that region.

By following these steps, you can ensure that your Azure virtual machines in the France Central region are deployed within the specified IP address range of 10.5.1.0/24.

Question 11

Question Type: MultipleChoice

SIMULATION

Task 1

You need to ensure that virtual machines on VNET1 and VNET2 are included automatically in a DNS zone named contoso.azure. The solution must ensure that the virtual machines on VNET1 and VNET2 can resolve the names of the virtual machines on either virtual network.

Options:

A- See the Explanation below for step by step instructions

Answer:

A

Explanation:

To achieve the task of ensuring that virtual machines on VNET1 and VNET2 are included automatically in a DNS zone named contoso.azure, and that they can resolve the names of the virtual machines on either virtual network, you can follow these steps:

Step-by-Step Solution

Step 1: Create a Private DNS Zone

Navigate to the Azure Portal.

Search for "Private DNS zones" in the search bar and select it.

Click on "Create".

Enter the DNS zone name as contoso.azure.

Select the appropriate subscription and resource group.

Click on "Review + create" and then "Create".

Step 2: Link VNET1 and VNET2 to the DNS Zone

Go to the newly created DNS zone (contoso.azure).

Select "Virtual network links" from the left-hand menu.

Click on "Add".

Enter a name for the link (e.g., VNET1-link).

Select the subscription and virtual network (VNET1).

Enable auto-registration to ensure that VMs are automatically registered in the DNS zone.

Click on "OK".

Repeat the process for VNET2.

Step 3: Configure DNS Settings for VNET1 and VNET2

Navigate to VNET1 in the Azure Portal.

Select "DNS servers" under the "Settings" section.

Ensure that the DNS server is set to "Default (Azure-provided)".

Repeat the process for VNET2.

Step 4: Verify Name Resolution

Deploy a virtual machine in VNET1 and another in VNET2.

Connect to the virtual machines using Remote Desktop Protocol (RDP) or Secure Shell (SSH).

Test name resolution by pinging the VM in VNET2 from the VM in VNET1 using its hostname (e.g., ping <VM-name>.contoso.azure).

Explanation

Private DNS Zone: This allows you to manage and resolve domain names in a private network without exposing them to the public internet.

Virtual Network Links: Linking VNET1 and VNET2 to the DNS zone ensures that VMs in these networks can register their DNS records automatically.

Auto-registration: This feature automatically registers the DNS records of VMs in the linked virtual networks, simplifying management.

DNS Settings: Using Azure-provided DNS ensures that the VMs can resolve each other's names without additional configuration.

By following these steps, you ensure that virtual machines on VNET1 and VNET2 are included automatically in the DNS zone contoso.azure and can resolve each other's names seamlessly.

Question 12

Question Type: Hotspot

You have an Azure subscription that contains multiple virtual machine scale sets and multiple Azure load balancers. The load balancers balance traffic across the scale sets.


You plan to deploy Azure Front Door to load balance traffic across the load balancers.


You need to identify which Front Door SKU to configure, and what to use to route the traffic to the load balancers. The solution must minimize costs.

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

NOTE: Each correct selection is worth one point.

Answer Area

SKU: 
Classic
Premium
Standard

Use: 
Azure Private Link
Azure Route Server
A service endpoint

Answer:

To Get Premium Files for AZ-700 Visit

<https://www.p2pexams.com/products/az-700>

For More Free Questions Visit

<https://www.p2pexams.com/microsoft/pdf/az-700>

