AZ-700Q&As

Designing and Implementing Microsoft Azure Networking Solutions

Pass Microsoft AZ-700 Exam with 100% Guarantee

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

https://www.pass2lead.com/az-700.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

You have an Azure subscription that contains four virtual machines. The virtual machines host an app named App1.

You deploy an Azure Standard Load Balancer named LB1 to load balance incoming HTTPS requests to App1.

You need to reduce how long it takes for LB1 to stop sending App1 traffic to failed servers. The solution must minimize administrative effort.

What should you modify?

A. the Backend pools settings

B. the Diagnostic settings

C. the Load-balancing rules

D. the Health probes settings

Correct Answer: D

Azure Load Balancer rules require a health probe to detect the endpoint status. The configuration of the health probe and probe responses determines which backend pool instances will receive new connections. Use health probes to detect

the failure of an application. Generate a custom response to a health probe. Use the health probe for flow control to manage load or planned downtime. When a health probe fails, the load balancer will stop sending new connections to the

respective unhealthy instance. Outbound connectivity isn\\'t affected, only inbound.

Add a TCP health probe

In this example, you\\'ll create a TCP health probe to monitor port 80.

1.

Sign in to the Azure portal.

2.

In the search box at the top of the portal, enter Load balancer. Select Load balancers in the search results.

3.

Select myLoadBalancer or your load balancer.

4.

In the load balancer page, select Health probes in Settings.

5.

Select + Add in Health probes to add a probe.

6.

Etc.

Reference: https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-custom-probe-overview
https://learn.microsoft.com/en-us/azure/load-balancer/manage-probes-how-to

QUESTION 2

You have a web app named App1 that is hosted in on-premises servers and on four Azure virtual machines (VMs).

Each Azure region has one virtual machine.

You need to recommend a solution to ensure that users will always connect to the closest instance of App1.

The solution must prevent the users from attempting to connect to a failed instance of App1.

Which two possible should you recommendation achieve the goal?

A. Azure Front Door Service

B. Azure Load Balancer

C. round-robin DNS

D. Azure Traffic Manager

E. Azure Application Gateway

Correct Answer: AD

Correct Answers:

Azure Front Door Service - Front Door is an application delivery network that provides global load balancing and site acceleration service for web applications. It offers Layer 7 capabilities for your application like SSL offload, path-based

routing, fast failover, caching, etc. to improve performance and high-availability of your applications.

Azure Traffic Manager - Traffic Manager is a DNS-based traffic load balancer that enables you to distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness.

https://docs.microsoft.com/en-au/azure/architecture/guide/technology-choices/load-balancing-overview

Wrong Answers:

Azure Load Balancer - It is a regional load balancing solution.

round-robin DNS - Round-robin DNS is a load balancing technique where the balancing is done by a type of DNS server called an authoritative nameserver, rather than using a dedicated piece of load-balancing hardware.

Azure Application Gateway - It is a regional load balancing solution.

QUESTION 3

You have a web application that will be deployed to an Azure App Service Web App.

The web application has following requirements:

Secure all communications by using Secured Socket layer (SSL).

SSL encryption and decryption must be processed efficiently to support high traffic load on the web application.

What should you consider?

A. Use Azure Application Gateway

B. Use Azure Monitor

C. Use Azure Security Centre

D. Use Azure Traffic Manager

Correct Answer: A

Correct Answer(s):

Use Azure Application Gateway - Azure Application Gateway supports end-to-end encryption of traffic. Application Gateway terminates the SSL connection at the application gateway. The gateway then applies the routing rules to the traffic,

re-encrypts the packet, and forwards the packet to the appropriate back-end server

based on the routing rules defined.

https://docs.microsoft.com/en-us/azure/application-gateway/features#secure-sockets-layer-ssltls-termination

Azure provides a suite of fully managed load-balancing solutions for your scenarios. If you are looking for Transport Layer Security (TLS) protocol termination ("SSL offload") or per-HTTP/HTTPS request, application-layer processing, review

Application Gateway. If you are looking for regional load balancing, review Load Balancer.

Wrong Answers:

Use Azure Monitor - Azure Monitor is a comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments.

Use Azure Security Centre - Azure Security Center is a unified infrastructure security management system that strengthens the security posture of your data centers and provides advanced threat protection across your hybrid workloads in the

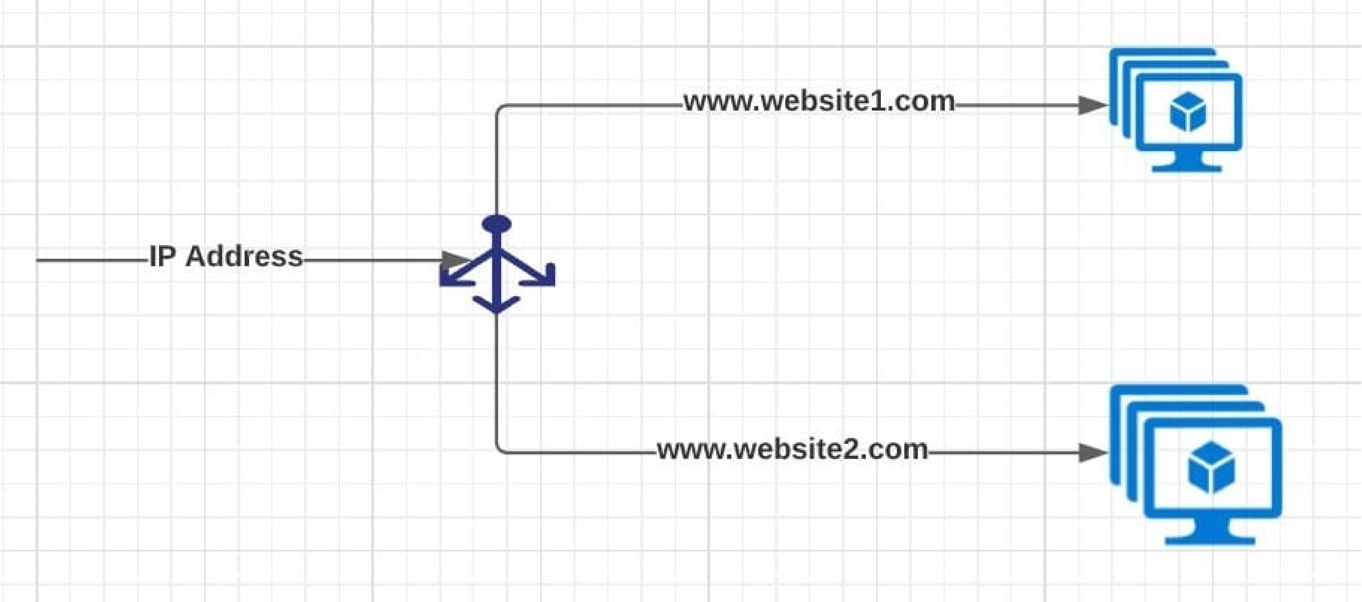
cloud.

Use Azure Traffic Manager - Traffic Manager does not support SSL offloading.

QUESTION 4

You have deployed multiple websites in Internet Information Server (IIS) by using Azure virtual machine scale sets (VMSS).

User sessions must be routed to the same server by using cookie-based session affinity. The below image depicts the network traffic flow for the websites to the VMSS.



What should you configure to make sure web traffic arrives at the appropriate server in the VMSS?

A. Routing rules and backend listeners

B. CNAME and A records

C. Routing method and DNS time to live (TTL)

D. Path-based redirection and websockets

Correct Answer: A

Correct Answer(s):

Routing rules and backend listeners - You can configure the hosting of multiple web sites when you create an application gateway. You need to define backend address pools using virtual machines. You then configure listeners and rules

based on domains that you own to make sure web traffic arrives at the appropriate servers in

the pools.

https://docs.microsoft.com/bs-latn-ba/azure//application-gateway/create-multiple-sites-portal

Wrong Answers:

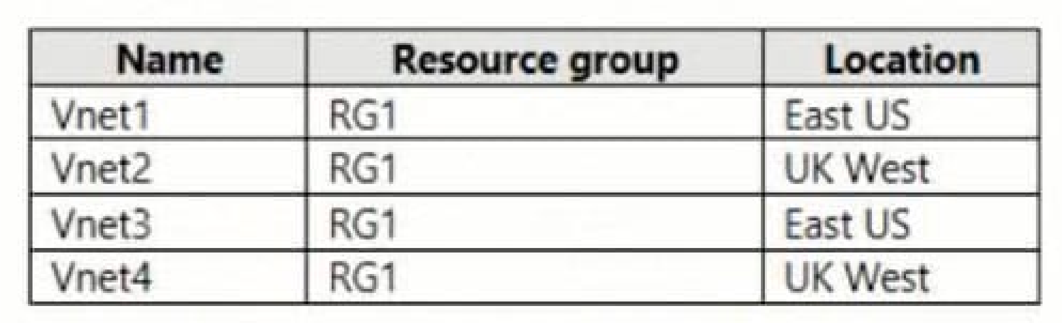
CNAME and A records - These are used for domain registrations.

Routing method and DNS time to live (TTL) - DNS TTL (time to live) is a setting that tells the DNS resolver how long to cache a query before requesting a new one. This is nothing to do with routing.

Path-based redirection and websockets - Path Based Routing allows you to route traffic to back-end server pools based on URL Paths of the request.

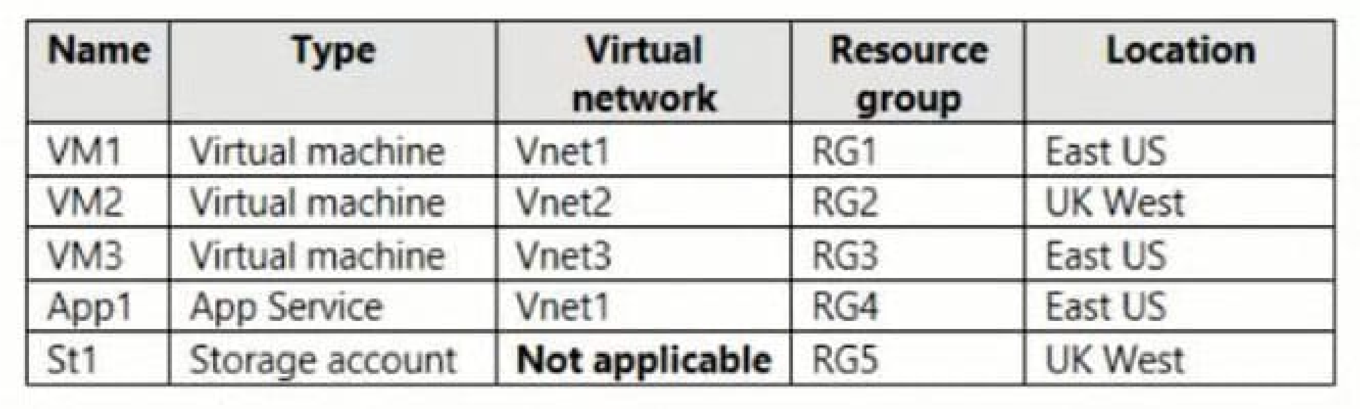
QUESTION 5

You have the Azure virtual networks shown in the following table.



Name	Resource group	Location
Vnet1	RG1	East US
Vnet2	RG1	UK West
Vnet3	RG1	East US
Vnet4	RG1	UK West

You have the Azure resources shown in the following table.



Name	Type	Virtual network	Resource group	Location
VM1	Virtual machine	Vnet1	RG1	East US
VM2	Virtual machine	Vnet2	RG2	UK West
VM3	Virtual machine	Vnet3	RG3	East US
App1	App Service	Vnet1	RG4	East US
St1	Storage account	**Not applicable**	RG5	UK West

You need to check latency between the resources by using connection monitors in Azure Network Watcher.

What is the minimum number of connection monitors that you must create?

A. 1

B. 2

C. 3

D. 4

E. 5

Correct Answer: B

As per MS guidelines *Region: Select a region for your connection monitor. You can select only the source VMs that are created in this region. Here you see only VMs or Virtual Machine Scale Sets that are bound to the region that you specified when you created the connection monitor. By default, VMs and Virtual Machine Scale Sets are grouped into the subscription that they belong to

* Destination can be anywhere as per this Destinations: You can monitor connectivity to an Azure VM, an on-premises machine, or any endpoint (a public IP, URL, or FQDN) by specifying it as a destination. In a single test group, you can add Azure VMs, on-premises machines, Office 365 URLs, Dynamics 365 URLs, and custom endpoints.

https://learn.microsoft.com/en-us/azure/network-watcher/connection-monitor-create-using-portal

QUESTION 6

Which three actions should you perform in sequence from the below list of actions?

1.

Create a health probe

2.

Create a public load balancer in the Standard SKU

3.

Create a public load balancer in the Basic SKU

4.

Create a backend pool that contains VMScaleSet1

5.

Create a NAT rule

6.

Create an outbound rule

A. 1,4,6

B. 3,4,5

C. 3,4,6

D. 2,4,6

E. 2,4,5

Correct Answer: D

Only standard SKU load balancer supports outbound connections.

The backend pool must be VMScaleSet1 since the requirement is to implement outbound connectivity for VMScaleSet1.

Outbound rules allow you to explicitly define SNAT(source network address translation) for a public standard load balancer.

https://docs.microsoft.com/en-us/azure/load-balancer/skus

https://docs.microsoft.com/en-us/azure/load-balancer/outbound-rules

QUESTION 7

Which rules should you configure in Azure firewall to allow inbound internet connections?

A. Application rules

B. Network rules

C. NAT rules

Correct Answer: C

Correct Answer(s):

NAT rules: Configure DNAT rules to allow incoming Internet connections.

https://docs.microsoft.com/en-us/azure/firewall/firewall-faq#what-are-some-azure-firewall-concepts

Wrong Answers:

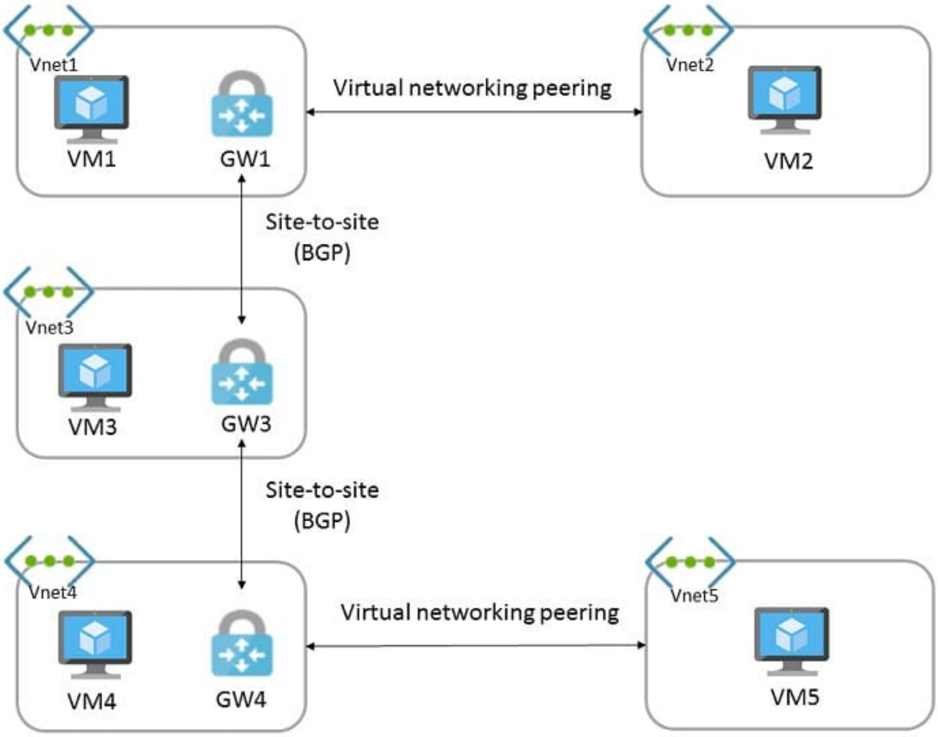
Application rules - Configure fully qualified domain names (FQDNs) that can be accessed from a subnet.

Network rules - Configure rules that contain source addresses, protocols, destination ports, and destination addresses.

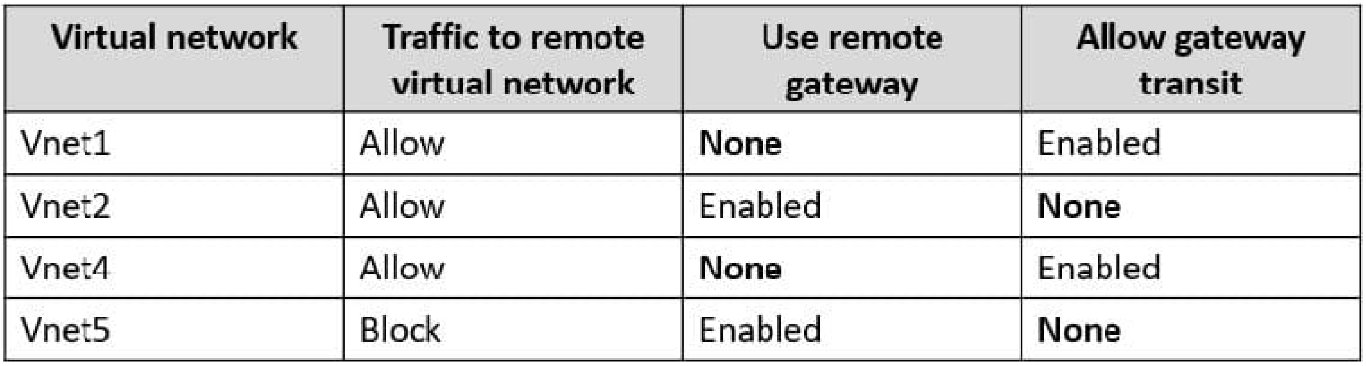
QUESTION 8

HOTSPOT

You have the Azure environment shown in the exhibit.



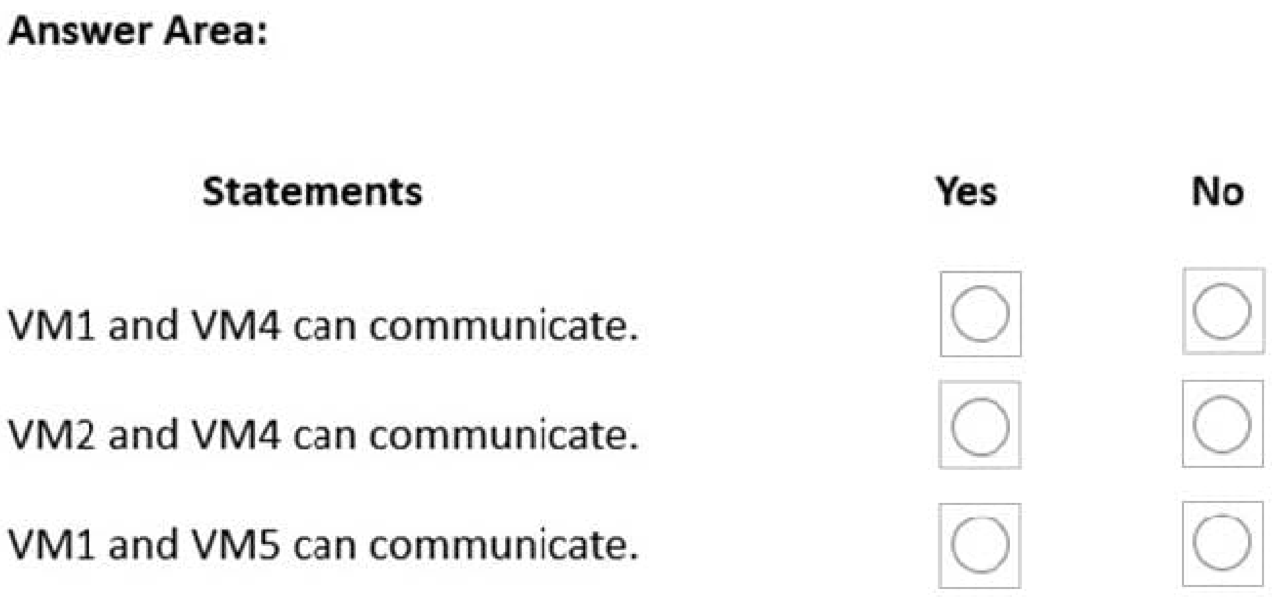
You have virtual network peering between Vnet1 and Vnet2. You have virtual network peering between Vnet4 and Vnet5. The virtual network peering is configured as shown in the following table.



Virtual network	Traffic to remote virtual network	Use remote gateway	Allow gateway transit
Vnet1	Allow	**None**	Enabled
Vnet2	Allow	Enabled	**None**
Vnet4	Allow	**None**	Enabled
Vnet5	Block	Enabled	**None**

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

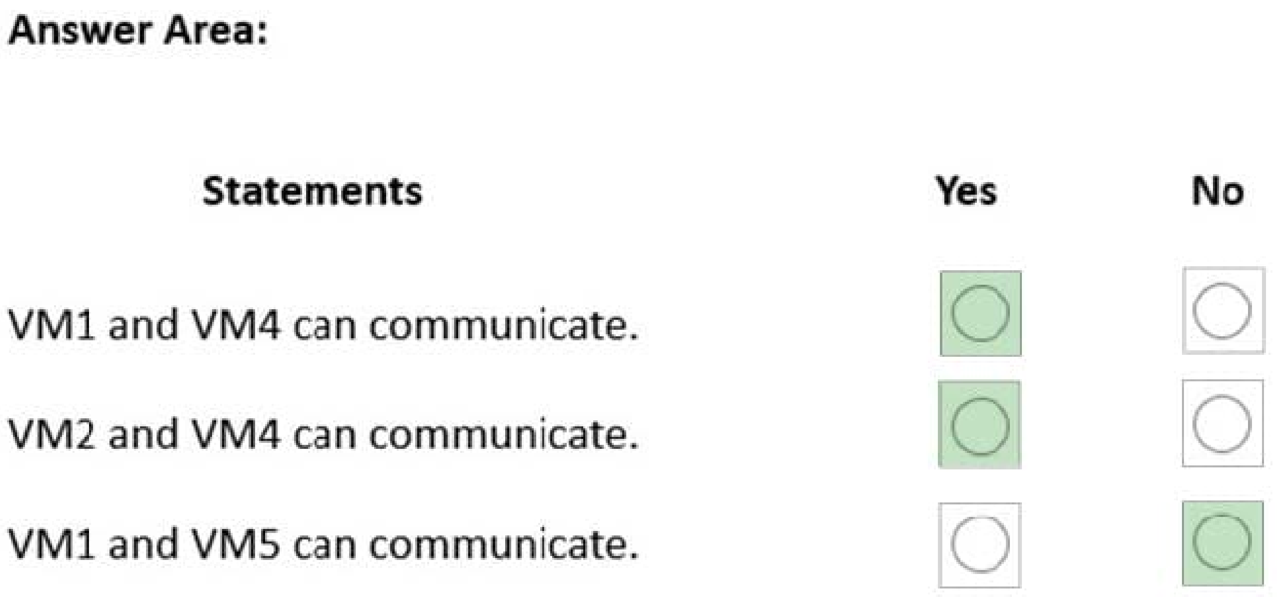
Hot Area:



Answer Area:

Statements	Yes	No
VM1 and VM4 can communicate.	○	○
VM2 and VM4 can communicate.	○	○
VM1 and VM5 can communicate.	○	○

Correct Answer:

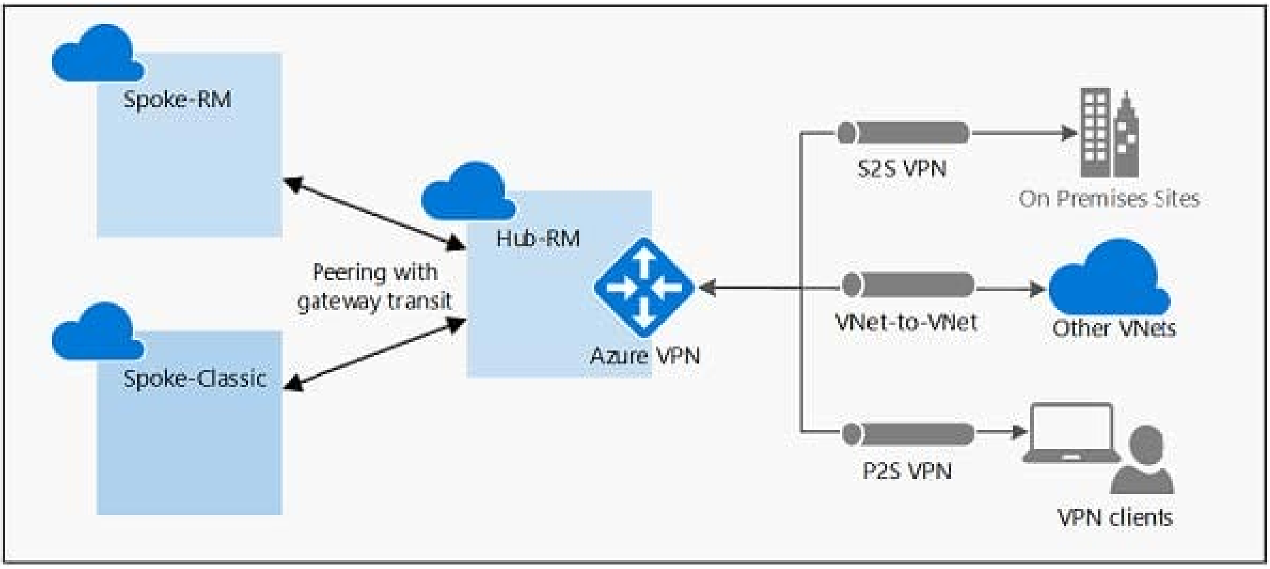


Answer Area:

Statements	Yes	No
VM1 and VM4 can communicate.	[✓ ○]	○
VM2 and VM4 can communicate.	[✓ ○]	○
VM1 and VM5 can communicate.	○	[✓ ○]

Box 1: Yes

Virtual network peering seamlessly connects two Azure virtual networks, merging the two virtual networks into one for connectivity purposes. Gateway transit is a peering property that lets one virtual network use the VPN gateway in the peered virtual network for cross-premises or VNet-to-VNet connectivity.



The following diagram shows how gateway transit works with virtual network peering.

In the diagram, gateway transit allows the peered virtual networks to use the Azure VPN gateway in Hub-RM. Connectivity available on the VPN gateway, including S2S, P2S, and VNet-to-VNet connections, applies to all three virtual

networks.

In hub-and-spoke network architecture, gateway transit allows spoke virtual networks to share the VPN gateway in the hub, instead of deploying VPN gateways in every spoke virtual network.

Box 2: Yes

VM2 uses the remote gateway GW1 to reach VM4.

Box 3: No

VM2 can reach VM4 through GW1, but not VM5 as VNEt1 does not use remote Gateways.

Reference:

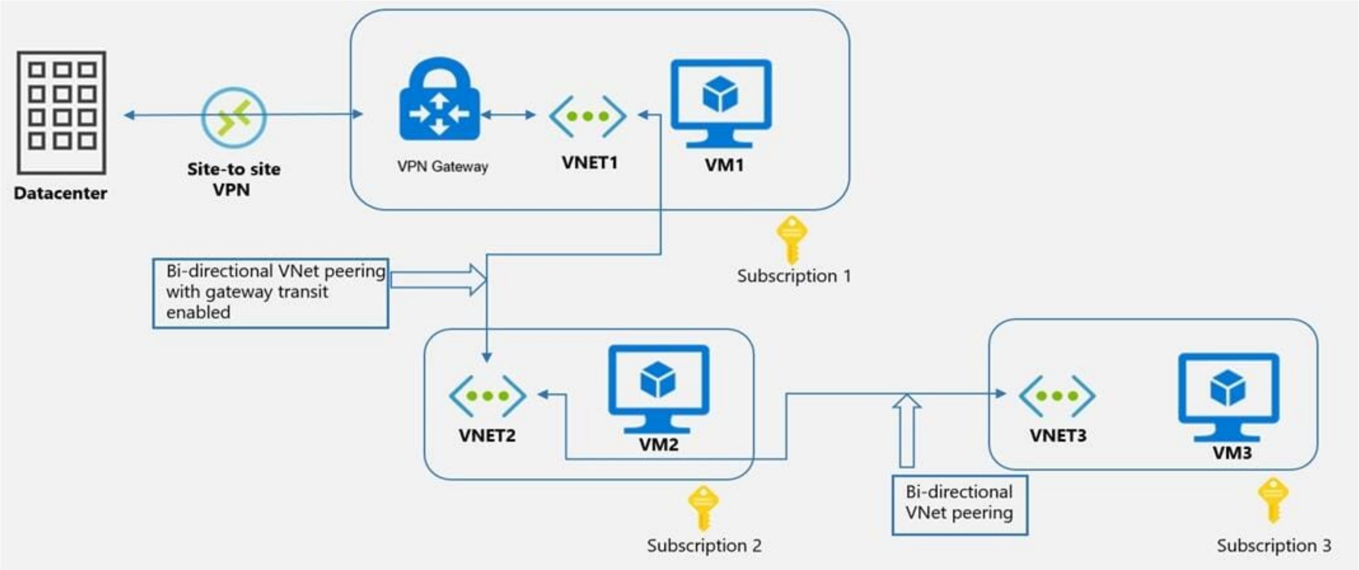
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-peering-gateway-transit

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-troubleshoot-peering-issues

QUESTION 9

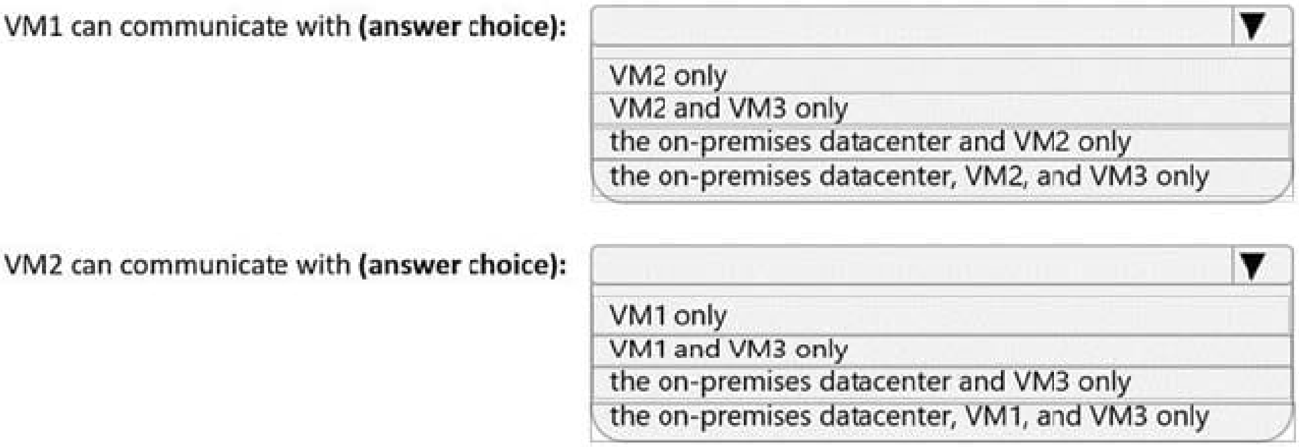
HOTSPOT

You have the Azure environment shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

Hot Area:



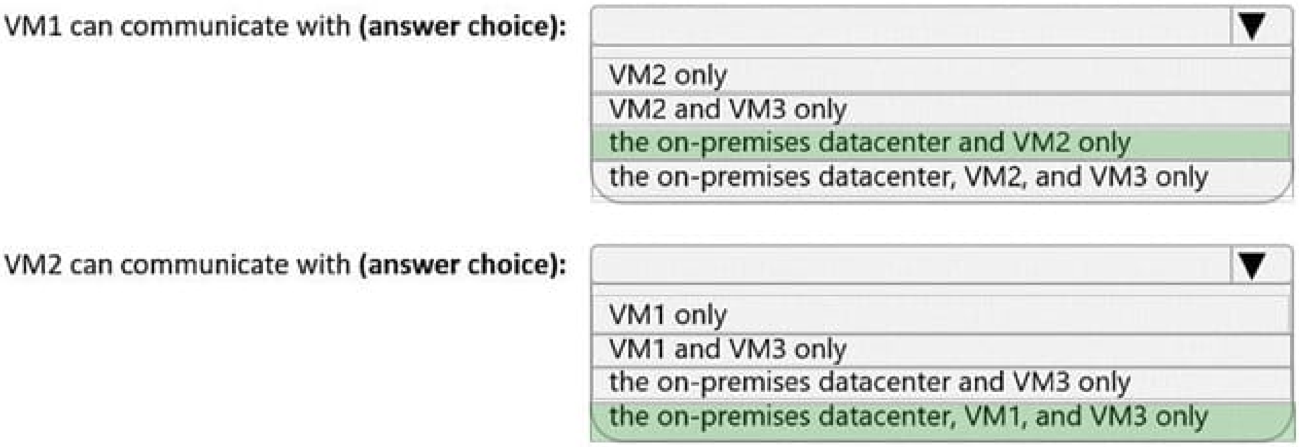
VM1 can communicate with **(answer choice):** ▼

- VM2 only
- VM2 and VM3 only
- the on-premises datacenter and VM2 only
- the on-premises datacenter, VM2, and VM3 only

VM2 can communicate with **(answer choice):** ▼

- VM1 only
- VM1 and VM3 only
- the on-premises datacenter and VM3 only
- the on-premises datacenter, VM1, and VM3 only

Correct Answer:



VM1 can communicate with **(answer choice):** ▼

- VM2 only
- VM2 and VM3 only
- [✓ the on-premises datacenter and VM2 only]
- the on-premises datacenter, VM2, and VM3 only

VM2 can communicate with **(answer choice):** ▼

- VM1 only
- VM1 and VM3 only
- the on-premises datacenter and VM3 only
- [✓ the on-premises datacenter, VM1, and VM3 only]

Reference: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-peering-gateway-transit?toc=/azure/virtual-network/toc.json

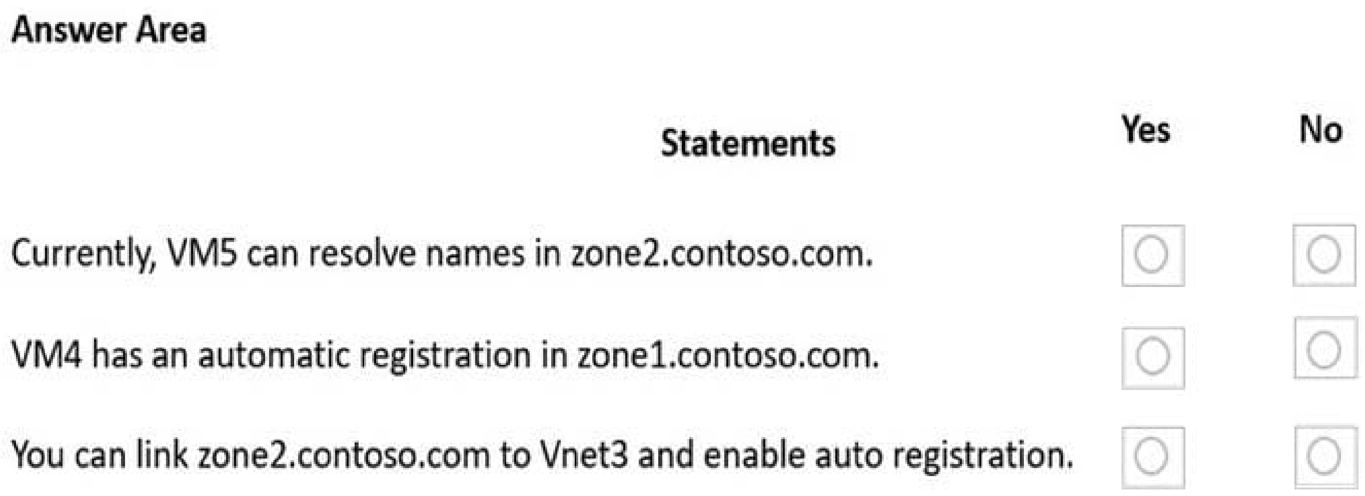
QUESTION 10

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

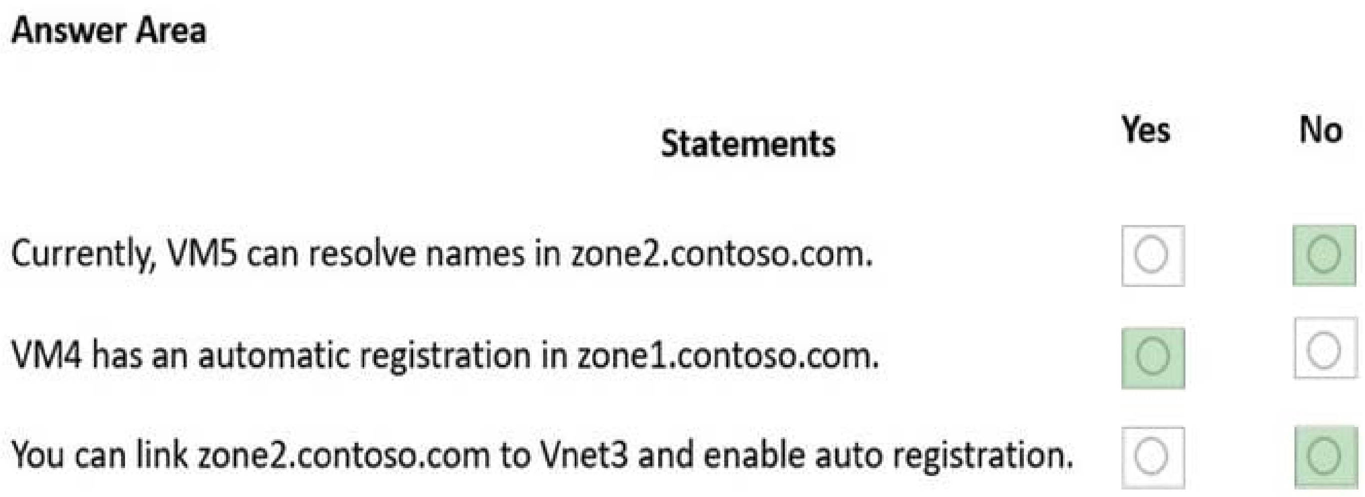
Hot Area:



Answer Area

Statements	Yes	No
Currently, VM5 can resolve names in zone2.contoso.com.	○	○
VM4 has an automatic registration in zone1.contoso.com.	○	○
You can link zone2.contoso.com to Vnet3 and enable auto registration.	○	○

Correct Answer:



Answer Area

Statements	Yes	No
Currently, VM5 can resolve names in zone2.contoso.com.	○	●
VM4 has an automatic registration in zone1.contoso.com.	●	○
You can link zone2.contoso.com to Vnet3 and enable auto registration.	○	●

Box 1: No

Zone2.contoso.com is not linked to any virtual networks. Therefore, no VMs are able to resolve names in the zone.

Box 2: Yes

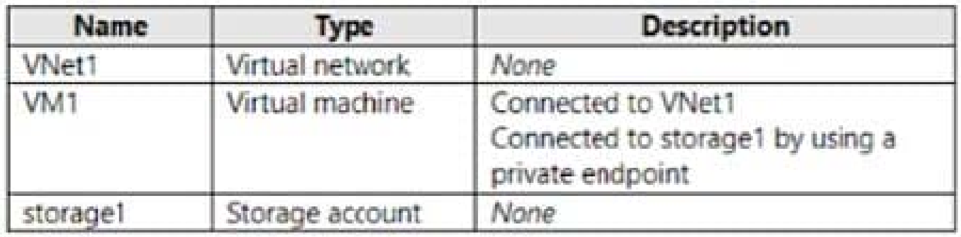
VM4 is in VNet3. Zone1.contoso.com has a link to VNet3 and auto-registration is enabled on the link.

Box3: No

VNet3 is linked to zone1.contoso.com and auto-registration is enabled on the link. A virtual network can only have one registration zone. You can link zone2.contoso.com to VNet3 but you won\\'t be able to enable auto-registration on the link.

QUESTION 11

Your on-premises network contains a DNS server named Server1.



Name	Type	Description
VNet1	Virtual network	*None*
VM1	Virtual machine	Connected to VNet1 Connected to storage1 by using a private endpoint
storage1	Storage account	*None*

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

The on-premises network is connected to VNet1 by using a Site-to-Site (S2S) VPN.

You need to ensure that Server1 can resolve the DNS name of storage1. The solution must minimize costs and administrative effort.

What should you use?

A. Azure DNS Private Resolver

B. an Azure public DNS zone

C. an Azure Private DNS zone

D. an Azure virtual machine that hosts a DNS service

Correct Answer: A

Azure DNS Private Resolver is a new service that enables you to query Azure DNS private zones from an on-premises environment and vice versa without deploying VM based DNS servers. https://learn.microsoft.com/en-us/azure/dns/dns-private-resolver-overview

QUESTION 12

You are planning the IP addressing for the subnets in Azure virtual networks. Which type of resource requires IP addresses in the subnets?

A. Azure DDoS Protection for virtual networks

B. private endpoints

C. Azure Virtual Network NAT

D. service endpoint policies

Correct Answer: B

A private endpoint is a network interface that uses a private IP address from your virtual network. This network interface connects you privately and securely to a service that\\'s powered by Azure Private Link. By enabling a private endpoint,

you\\'re bringing the service into your virtual network.

Private endpoint properties

A private endpoint specifies the following properties:

*

Name

*

Subnet

The subnet to deploy, where the private IP address is assigned.

*

Etc.

A read-only network interface is automatically created for the lifecycle of the private endpoint. The interface is assigned a dynamic private IP address from the subnet that maps to the private-link resource. The value of the private IP address remains unchanged for the entire lifecycle of the private endpoint. Reference: https://learn.microsoft.com/en-us/azure/private-link/private-endpoint-overview

QUESTION 13

HOTSPOT

Your company has an Azure virtual network named Vnet1 that uses an IP address space of 192.168.0.0/20. Vnet1 contains a subnet named Subnet1 that uses an IP address space of 192.168.0.0/24.

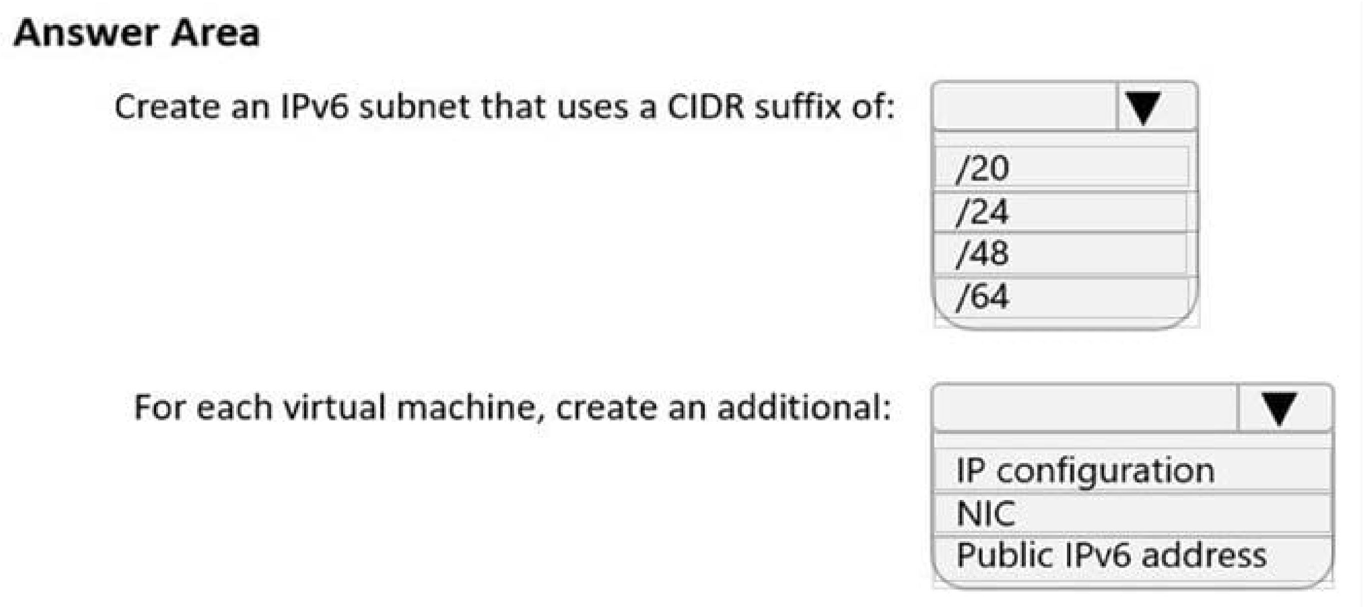
You create an IPv6 address range to Vnet1 by using a CIDR suffix of /48.

You need to enable the virtual machines on Subnet1 to communicate with each other by using IPv6 addresses assigned by the company. The solution must minimize the number of additional IPv4 addresses.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

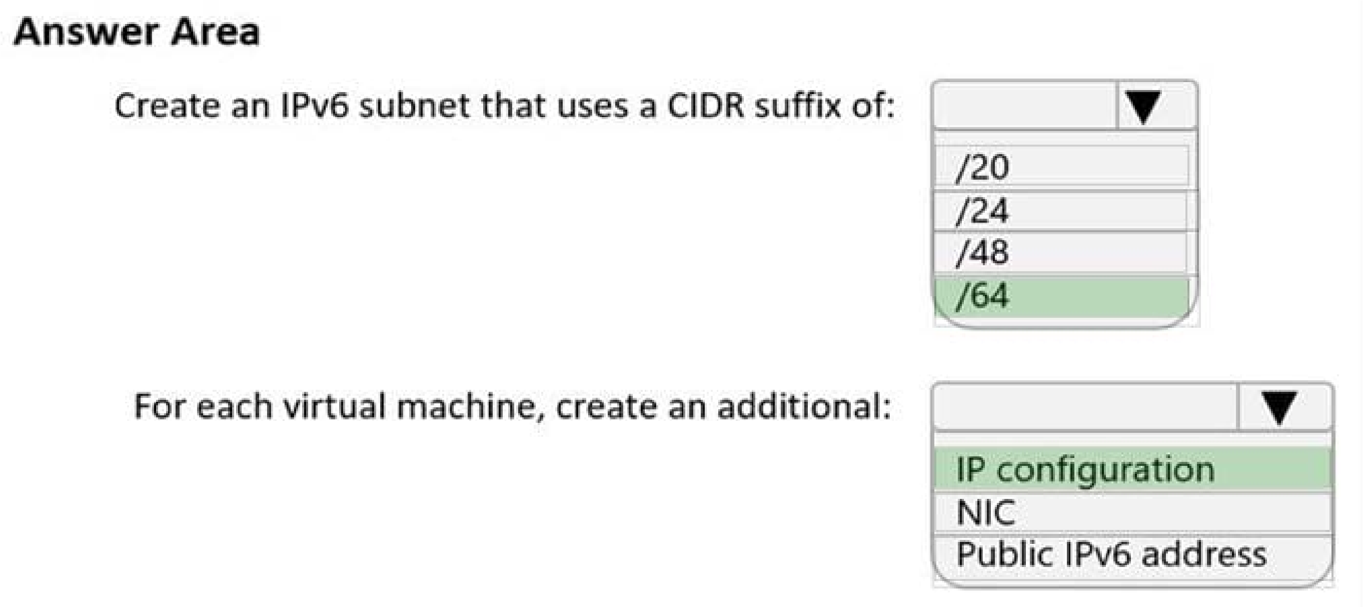
Create an IPv6 subnet that uses a CIDR suffix of:

- /20
- /24
- /48
- /64

For each virtual machine, create an additional:

- IP configuration
- NIC
- Public IPv6 address

Correct Answer:



Answer Area

Create an IPv6 subnet that uses a CIDR suffix of:

- /20
- /24
- /48
- [✓ /64]

For each virtual machine, create an additional:

- [✓ IP configuration]
- NIC
- Public IPv6 address

Reference: https://docs.microsoft.com/en-us/azure/virtual-network/ipv6-overview

https://docs.microsoft.com/en-us/azure/virtual-network/ipv6-add-to-existing-vnet-powershell

QUESTION 14

You plan to create a Point-to-Site (P2S) VPN connection for a remote user to connect to your Azure environment. Which of the following protocols should you use?

A. OpenVPN

B. IPSec

C. Secure Socket Tunneling Protocol (SSTP)

D. IKEv2 VPN

E. FTP

Correct Answer: ACD

Point-to-site VPN can use one of the following protocols:

OpenVPN?Protocol, an SSL/TLS based VPN protocol. A TLS VPN solution can penetrate firewalls, since most firewalls open TCP port 443 outbound, which TLS uses. OpenVPN can be used to connect from Android, iOS (versions 11.0 and above), Windows, Linux, and Mac devices (macOS versions 10.13 and above).

Secure Socket Tunneling Protocol (SSTP), a proprietary TLS-based VPN protocol. A TLS VPN solution can penetrate firewalls, since most firewalls open TCP port 443 outbound, which TLS uses. SSTP is only supported on Windows devices. Azure supports all versions of Windows that have SSTP and support TLS 1.2 (Windows 8.1 and later).

IKEv2 VPN, a standards-based IPsec VPN solution. IKEv2 VPN can be used to connect from Mac devices (macOS versions 10.11 and above). https://docs.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about#protocol

QUESTION 15

You have an Azure application gateway configured for a single website that is available at https://www.contoso.com.

The application gateway contains one backend pool and one rule. The backend pool contains two backend servers. Each backend server has an additional website that is available on port 8080.

You need to ensure that if port 8080 is unavailable on a backend server, all the traffic for https://www.contoso.com is redirected to the other backend server.

What should you do?

A. Create a health probe

B. Add a new rule

C. Change the port on the listener

D. Add a new listener

Correct Answer: A

By default, Azure Application Gateway probes backend servers to check their health status and to check whether they\\'re ready to serve requests. Users can also create custom probes to mention the host name, the path to be probed, and the status codes to be accepted as Healthy. In each case, if the backend server doesn\\'t respond successfully, Application Gateway marks the server as Unhealthy and stops forwarding requests to the server. After the server starts responding successfully, Application Gateway resumes forwarding the requests.

Note: The default probe request is sent in the format of ://127.0.0.1:/. For example, http://127.0.0.1:80 for an http probe on port 80. Only HTTP status codes of 200 through 399 are considered healthy. The protocol and destination port are inherited from the HTTP settings. If you want Application Gateway to probe on a different protocol, host name, or path and to recognize a different status code as Healthy, configure a custom probe and associate it with the HTTP settings.

Reference: https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-backend-healthtroubleshooting