Microsoft

Exam Questions AZ-101

Microsoft Azure Integration and Security

NEW QUESTION 1
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 wet) app named Appl. App1 runs in an Azure App Service plan named Plan1. Plan1 is associated to the Free pricing tier.
You discover that App1 stops each day after running continuously for 60 minutes. You need to ensure that App1 can run continuously for the entire day.
Solution: You change the pricing tier of Plan1 to Shared. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation: You should switch to the Basic Tier.
The Free Tier provides 60 CPU minutes / day. This explains why App1 is stops. The Shared Tier provides 240 CPU minutes / day. The Basic tier has no such cap.
References:
https://azure.microsoft.com/en-us/pricing/details/app-service/windows/

NEW QUESTION 2
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 Active Directory (Azure AD) tenant named Adatum and an Azure Subscript contains a resource group named Dev.
d Subscription1. Adatum contains a group named Developers. Subscription!
You need to provide the Developers group with the ability to create Azure logic apps in the; Dev, resource group.
Solution: On Dev, you assign the Logic App Contributor role to the Developers group.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation: The Logic App Contributor role lets you manage logic app, but not access to them. It provides access to view, edit, and update a logic app.
References:
https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-securing-a-logic-app

NEW QUESTION 3
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 Active Directory (Azure AD) tenant named Adatum and an Azure Subscription named Subscription1. Adatum contains a group named Developers. Subscription1 contains a resource group named Dev.
You need to provide the Developers group with the ability to create Azure logic apps in the Dev resource group.
Solution: On Subscription1, you assign the Logic App Operator role to the Developers group. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation: The Logic App Operator role only lets you read, enable and disable logic app. With it you can view the logic app and run history, and enable/disable. Cannot edit or update the definition.
You would need the Logic App Contributor role. References:
https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-securing-a-logic-app

NEW QUESTION 4
Note This question is part of a series of questions that present the same seer 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 manage a virtual network named VNet1 that is hosted in the West US Azure region.
VNet1 hosts two virtual machines named VM1 and VM2 that run Windows Server. You need to inspect all the network traffic from VM1 to VM2 for a period of three hours.
Solution: From Performance Monitor, you create a Data Collector Set (DCS) Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation: You should use Azure Network Watcher. References:
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview

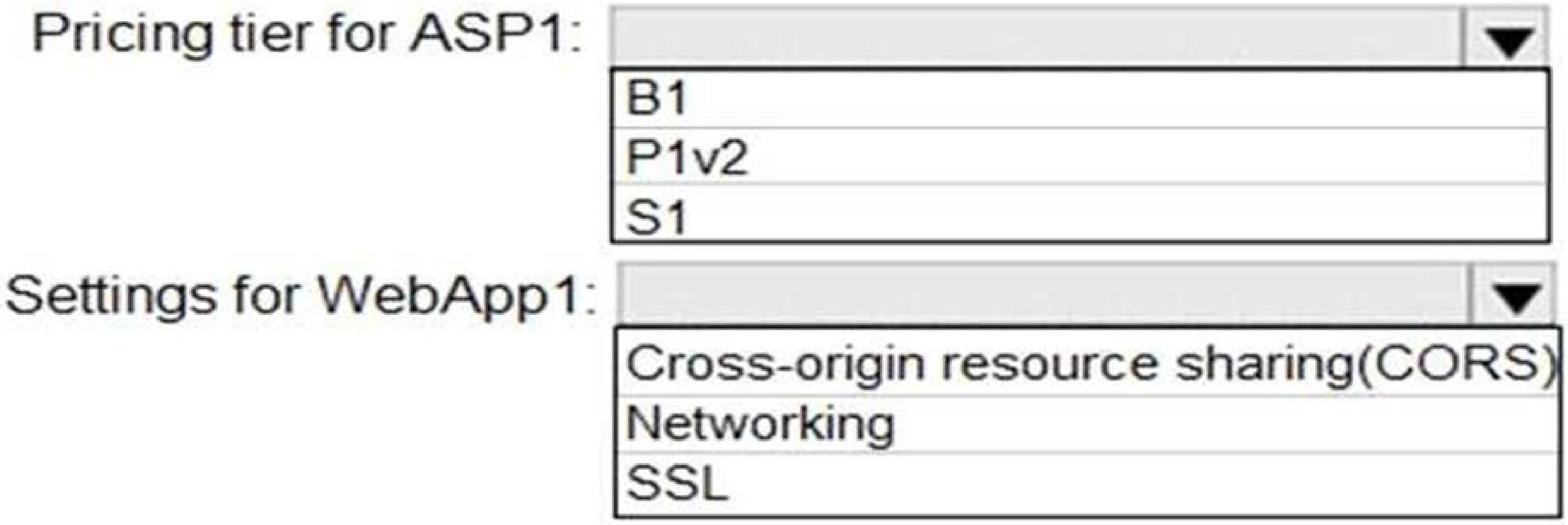
NEW QUESTION 5
A web developer creates a web application that you plan to deploy as an Azure web app.
Users must enter credentials to access the web application.
You create a new web app named WebAppl1 and deploy the web application to WebApp1.
You need to disable anonymous access to WebApp1. What should you configure?

A. Advanced Tools
B. Authentication/ Authorization
C. Access control (IAM)
D. Deployment credentials

Answer: B

Explanation: Anonymous access is an authentication method. It allows users to establish an anonymous connection.
References:
https://docs.microsoft.com/en-us/biztalk/core/guidelines-for-resolving-iis-permissions-problems

NEW QUESTION 6
HOTSPOT
You have an Azure web app named WebApp1 that runs in an Azure App Service plan named ASP1. ASP1 is based on the D1 pricing tier.
You need to ensure that WebApp1 can be accessed only from computers on your on-premises network. The solution must minimize costs.
What should you configure? To answer, select the appropriate options in the answer are a.
NOTE: Each correct selection is worth one point.



Pricing tier for ASP1:
B1
P1v2
S1

Settings for WebApp1:
Cross-origin resource sharing(CORS)
Networking
SSL

Answer:

Explanation: Box 1: B1
B1 (Basic) would minimize cost compared P1v2 (premium) and S1 (standard). Box 2: Cross Origin Resource Sharing (CORS)
Once you set the CORS rules for the service, then a properly authenticated request made against the service from a different domain will be evaluated to determine whether it is allowed according to the
rules you have specified.
Note: CORS (Cross Origin Resource Sharing) is an HTTP feature that enables a web application running under one domain to access resources in another domain. In order to reduce the possibility of cross-site scripting attacks, all modern web browsers implement a security restriction known as same-origin policy. This prevents a web page from calling APIs in a different domain. CORS provides a secure way to allow one origin (the origin domain) to call APIs in another origin.
References:
https://azure.microsoft.com/en-us/pricing/details/app-service/windows/ https://docs.microsoft.com/en-us/azure/cdn/cdn-cors

NEW QUESTION 7
You have an Azure Service Bus.
You need to implement a Service Bus queue that guarantees first in first-out (FIFO) delivery of messages.
What should you do?

A. Set the Lock Duration setting to 10 seconds.
B. Enable duplicate detection.
C. Set the Max Size setting of the queue to 5 GB.
D. Enable partitioning.
E. Enable sessions.

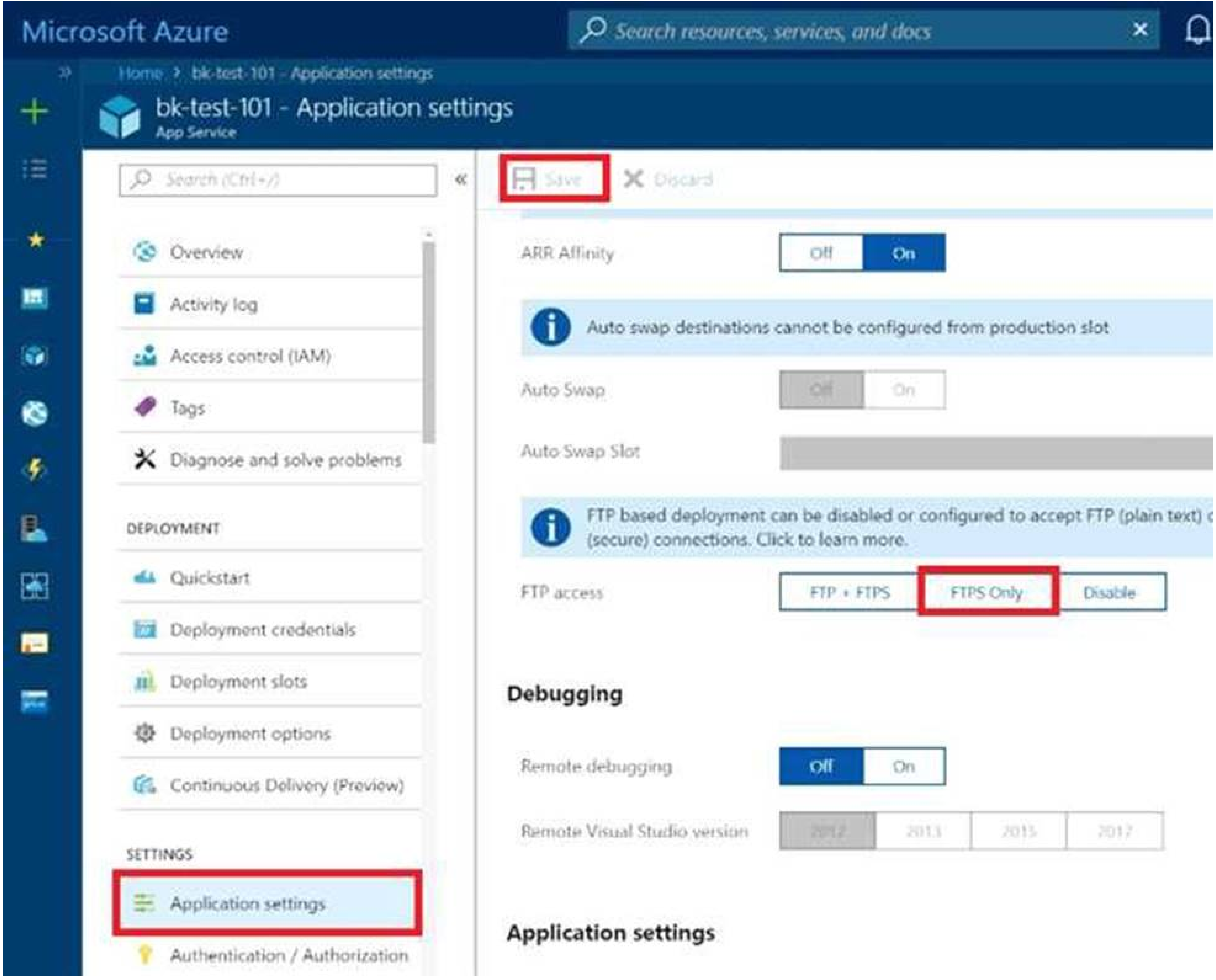
Answer: E

Explanation: Through the use of messaging sessions you can guarantee ordering of messages, that is first-in-first- out (FIFO) delivery of messages.
References:
https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-azure-and-service-bus- queues-compared-contrasted

NEW QUESTION 8
You need to prevent remote users from publishing via FTP to a function app named FunctionApplod7509087fa. Remote users must be able to publish via FTPS.
What should you do from the Azure portal?

Answer:

Explanation: Step 1:
Locate and select the function app FunctionApplod7509087fa.
Step 2:
Select Application Settings > FTP Access, change FTP access to FTPS Only, and click Save.



ARR Affinity: Off [✓ On]

Auto swap destinations cannot be configured from production slot

Auto Swap: [✓ Off] On

Auto Swap Slot

FTP based deployment can be disabled or configured to accept FTP (plain text) c (secure) connections. Click to learn more.

FTP access: FTP + FTPS [✓ FTPS Only] Disable

Remote debugging: [✓ Off] On

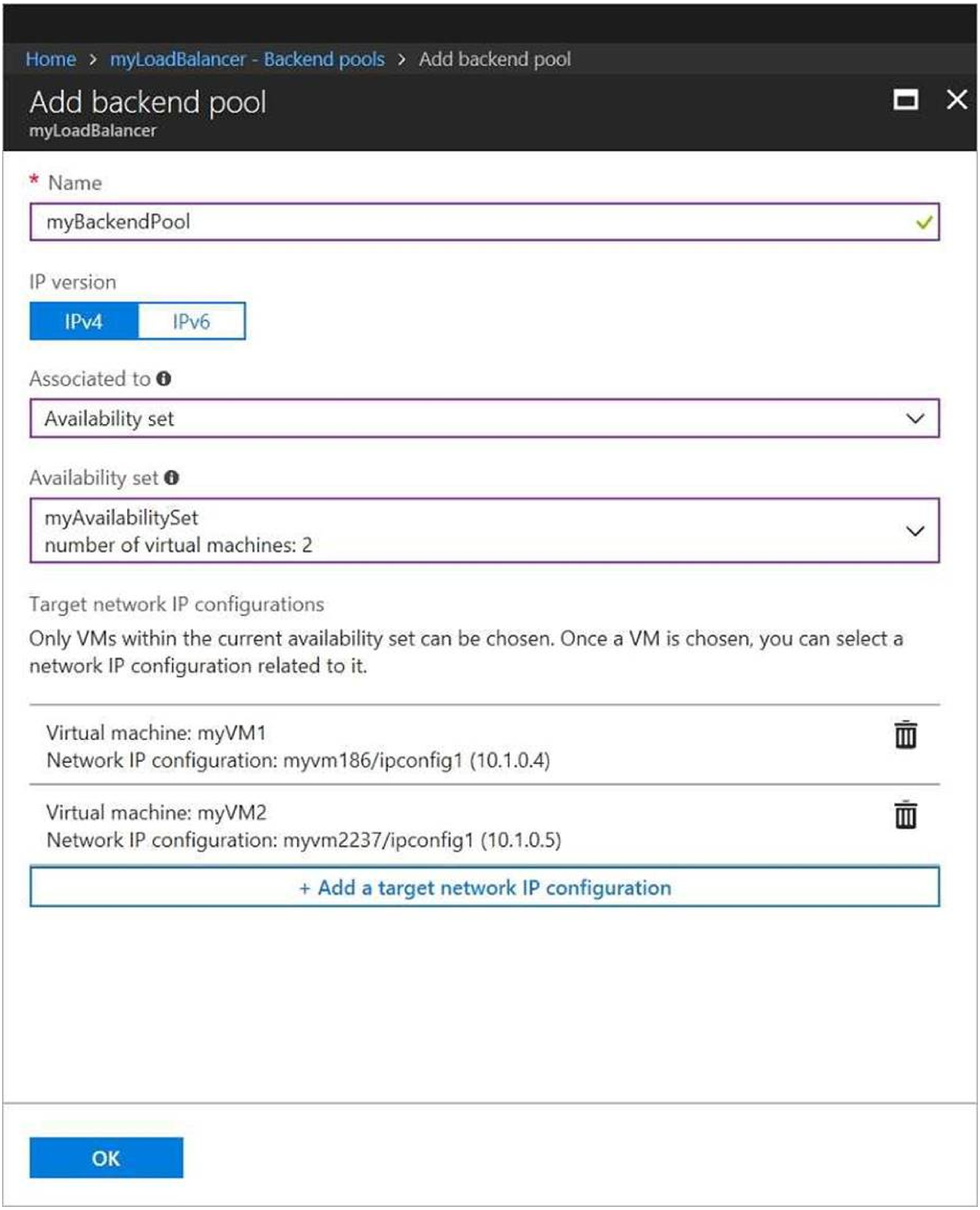
Remote Visual Studio version: [✓ 2012] 2013 2015 2017

References:
https://blogs.msdn.microsoft.com/appserviceteam/2018/05/08/web-apps-making-changes-to-ftp- deployments/

NEW QUESTION 9
Your marketing team creates a new website that you must load balance for 99.99
percent availability.
You need to deploy and configure a solution for both machines in the Web-AS availability set to load balance the website over HTTP. The solution must use the load balancer your resource group.
What should you do from the Azure portal?

Answer:

Explanation: To distribute traffic to the VMs in the availability set, a back-end address pool contains the IP addresses of the virtual NICs that are connected to the load balancer. Create the back-end address pool to include the VMs in the availability set.
Step 1:
Select All resources on the left menu, and then select LoadBalancer from the resource list. Step 2:
Under Settings, select Backend pools, and then select Add. Step 3:
On the Add a backend pool page, select the Web-AS availability set, and then select OK:



Home > myLoadBalancer - Backend pools > Add backend pool

Add backend pool

myLoadBalancer

* Name

myBackendPool

IP version

IPv4 | IPv6

Associated to

Availability set

Availability set

myAvailabilitySet
number of virtual machines: 2

Target network IP configurations

Only VMs within the current availability set can be chosen. Once a VM is chosen, you can select a network IP configuration related to it.

Virtual machine: myVM1
Network IP configuration: myvm186/ipconfig1 (10.1.0.4)

Virtual machine: myVM2
Network IP configuration: myvm2237/ipconfig1 (10.1.0.5)

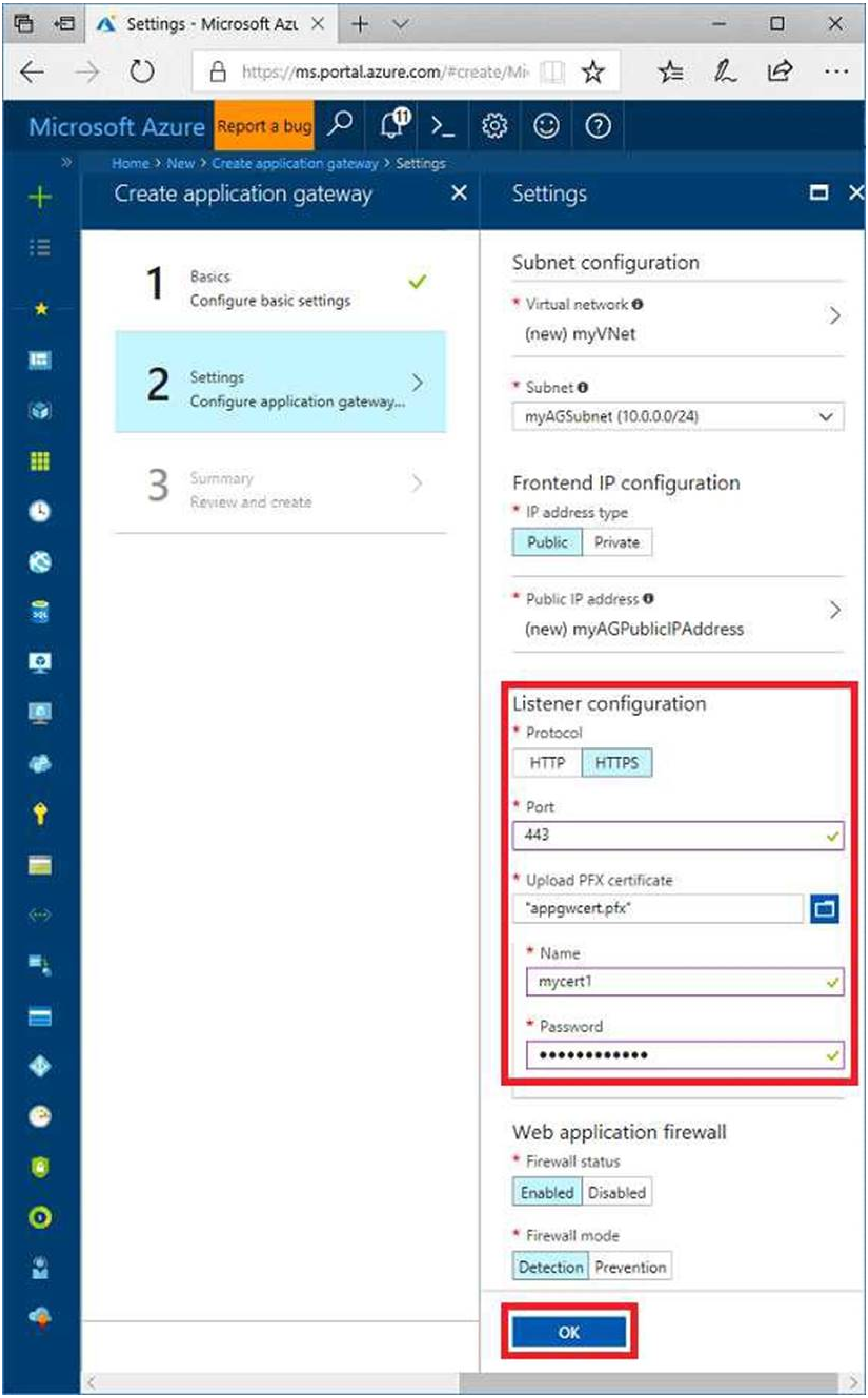
References:
https://docs.microsoft.com/en-us/azure/load-balancer/quickstart-create-basic-load-balancer-portal

NEW QUESTION 10

Your Azure environment contains an application gateway and custom apps.
Another administrator modifies the application gateway and the apps to use HTTP over TCP port 8080.
Users report that they can no longer connect to the apps.
You suspect that the cause of the issue is a change in the configuration of the application gateway.
You need to modify the application gateway to resolve the issue. What should you do from the Azure portal?

Answer:

Explanation: Step 1:
Select Networking and then select Application Gateway in the Featured list, and select the application gateway, and select the settings.
Step 2:
Click HTTP for the protocol of the listener and make sure that the port is defined as 443.


Settings - Microsoft Azu
https://ms.portal.azure.com/#create/Mi
Microsoft Azure
Report a bug
Home > New > Create application gateway > Settings

Create application gateway

1 Basics
Configure basic settings

2 Settings
Configure application gateway...

3 Summary
Review and create

Settings

Subnet configuration

* Virtual network
(new) myVNet

* Subnet
myAGSubnet (10.0.0.0/24)

Frontend IP configuration

* IP address type
Public | Private

* Public IP address
(new) myAGPublicIPAddress

Listener configuration

* Protocol
HTTP | HTTPS

* Port
443

* Upload PFX certificate
"appgwcert.pfx"

* Name
mycert1

* Password
•••••••••••••

Web application firewall

* Firewall status
Enabled | Disabled

* Firewall mode
Detection | Prevention

OK

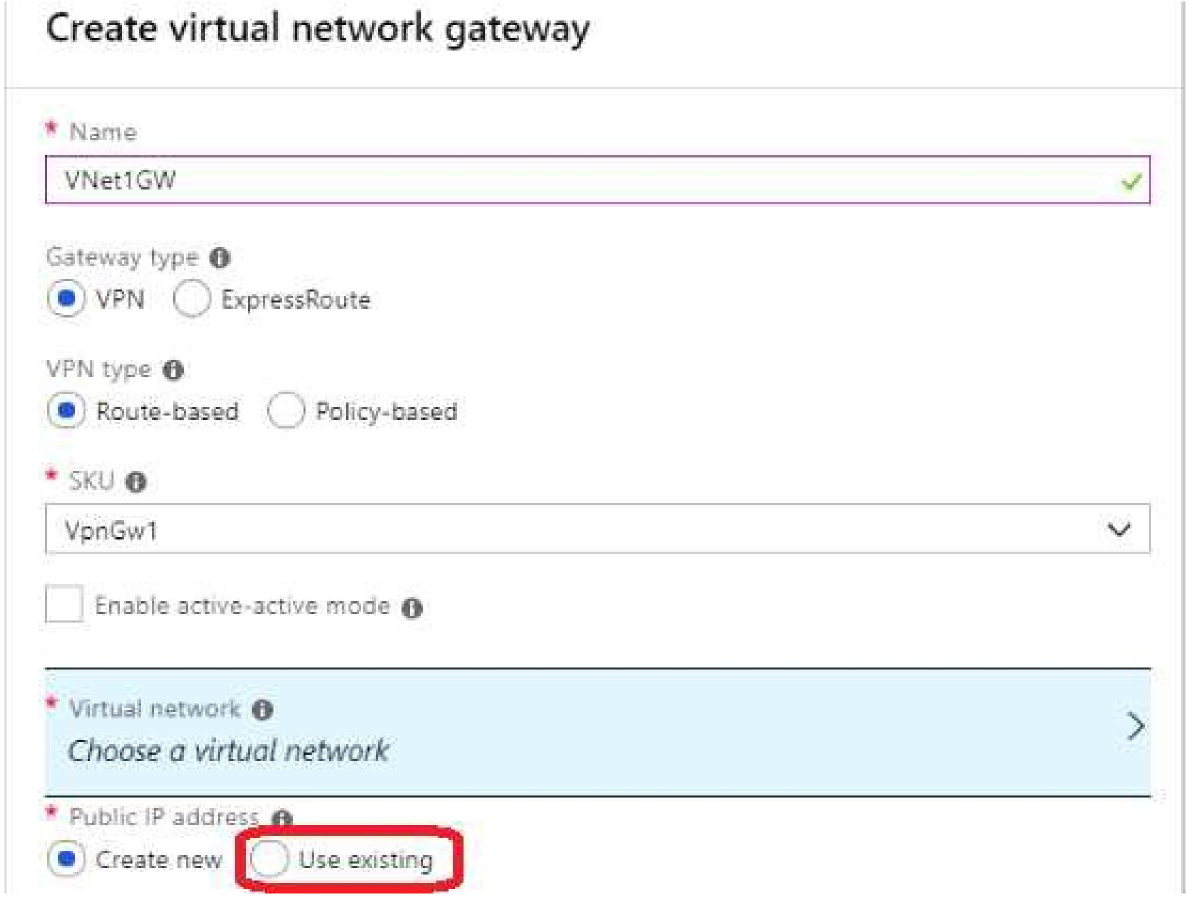
References:
https://docs.microsoft.com/en-us/azure/application-gateway/create-ssl-portal

NEW QUESTION 10

You plan to deploy a site-to-site VPN connection from on-premises network to your
Azure environment. The VPN connection will be established to the VNET01-USEA2 virtual network.
You need to create the required resources in Azure for the planned site-to-site VPN. The solution must minimize costs.
What should you do from the Azure portal?
NOTE: This task may a very long time to complete. You do NOT need to wait for the deployment to complete this task successfully.

Answer:

Explanation: We create a VPN gateway. Step 1:
On the left side of the portal page, click + and type 'Virtual Network Gateway' in search. In Results, locate and click Virtual network gateway.
Step 2:
At the bottom of the 'Virtual network gateway' page, click Create. This opens the Create virtual network gateway page.
Step 3:
On the Create virtual network gateway page, specify the values for your virtual network gateway. Gateway type: Select VPN. VPN gateways use the virtual network gateway type VPN.
Virtual network: Choose the existing virtual network VNET01-USEA2
Gateway subnet address range: You will only see this setting if you did not previously create a gateway subnet for your virtual network.
Step 4:
Select the default values for the other setting, and click create.



Create virtual network gateway

* Name
VNet1GW ✓

Gateway type
● VPN ○ ExpressRoute

VPN type
● Route-based ○ Policy-based

* SKU
VpnGw1

□ Enable active-active mode

* Virtual network
Choose a virtual network

* Public IP address
● Create new ○ Use existing

The settings are validated and you'll see the "Deploying Virtual network gateway" tile on the dashboard. Creating a gateway can take up to 45 minutes.
Note: This task may take a very long time to complete. You do NOT need to wait for the deployment to complete this task successfully.
References:
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal

Case Study: 4 Contoso Case Study
Overview
Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.
The Montreal office has 2,000 employees. The Seattle office has 1,000 employees. The New York office has 200 employees.
All the resources used by Contoso are hosted on-premises.
Contoso creates a new Azure subscription. The Azure Active Directory (Azure AD) tenant uses a domain named contoso.onmicrosoft.com. The tenant uses the P1 pricing tier.
Existing Environment
The network contains an Active Directory forest named contoso.com. All domain controllers are configured as DNS servers and host the contoso.com DNS zone.
Contoso has finance, human resources, sales, research, and information technology departments. Each department has an organizational unit (OU) that contains all the accounts of that respective department. All the user accounts have the department attribute set to their respective department. New users are added frequently.
Contoso.com contains a user named User1.
All the offices connect by using private links.
Contoso has data centers in the Montreal and Seattle offices. Each data center has a firewall that can be configured as a VPN device.
All infrastructure servers are virtualized. The virtualization environment contains the servers in the following table.

Name	Role	Contains virtual machine
Server1	VMWare vCenter server	VM1
Server2	Hyper-V-host	VM2

Contoso uses two web applications named App1 and App2. Each instance on each web application requires 1GB of memory.
The Azure subscription contains the resources in the following table.

Name	Type
VNet1	Virtual network
VM3	Virtual machine
VM4	Virtual machine

The network security team implements several network security groups (NSGs).

Planned Changes
Contoso plans to implement the following changes:
• Deploy Azure ExpressRoute to the Montreal office.
• Migrate the virtual machines hosted on Server1 and Server2 to Azure.
• Synchronize on-premises Active Directory to Azure Active Directory (Azure AD).
• Migrate App1 and App2 to two Azure web apps named webApp1 and WebApp2.
Technical requirements
Contoso must meet the following technical requirements:
• Ensure that WebApp1 can adjust the number of instances automatically based on the load and can scale up to five instance*.
• Ensure that VM3 can establish outbound connections over TCP port 8080 to the applications servers in the Montreal office.
• Ensure that routing information is exchanged automatically between Azure and the routers in the Montreal office.
• Enable Azure Multi-Factor Authentication (MFA) for the users in the finance department only.
• Ensure that webapp2.azurewebsites.net can be accessed by using the name app2.contoso.com.
• Connect the New Your office to VNet1 over the Internet by using an encrypted connection.
• Create a workflow to send an email message when the settings of VM4 are
modified.
• Cre3te a custom Azure role named Role1 that is based on the Reader role.
• Minimize costs whenever possible.

NEW QUESTION 15
You discover that VM3 does NOT meet the technical requirements. You need to verify whether the issue relates to the NSGs.
What should you use?

A. Diagram in VNet1
B. the security recommendations in Azure Advisor
C. Diagnostic settings in Azure Monitor
D. Diagnose and solve problems in Traffic Manager Profiles
E. IP flow verify in Azure Network Watcher

Answer: E

Explanation: Scenario: Contoso must meet technical requirements including:
Ensure that VM3 can establish outbound connections over TCP port 8080 to the applications servers in the Montreal office.
IP flow verify checks if a packet is allowed or denied to or from a virtual machine. The information consists of direction, protocol, local IP, remote IP, local port, and remote port. If the packet is denied by a security group, the name of the rule that denied the packet is returned. While any source or destination IP can be chosen, IP flow verify helps administrators quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment.
References:
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview

NEW QUESTION 19
You need to meet the technical requirement for VM4. What should you create and configure?

A. an Azure Notification Hub
B. an Azure Event Hub
C. an Azure Logic App
D. an Azure services Bus

Answer: B

Explanation: Scenario: Create a workflow to send an email message when the settings of VM4 are modified.
You can start an automated logic app workflow when specific events happen in Azure resources or third-party resources. These resources can publish those events to an Azure event grid. In turn, the event grid pushes those events to subscribers that have queues, webhooks, or event hubs as endpoints. As a subscriber, your logic app can wait for those events from the event grid before running automated workflows to perform tasks - without you writing any code.
References:
https://docs.microsoft.com/en-us/azure/event-grid/monitor-virtual-machine-changes-event-grid-logic- app

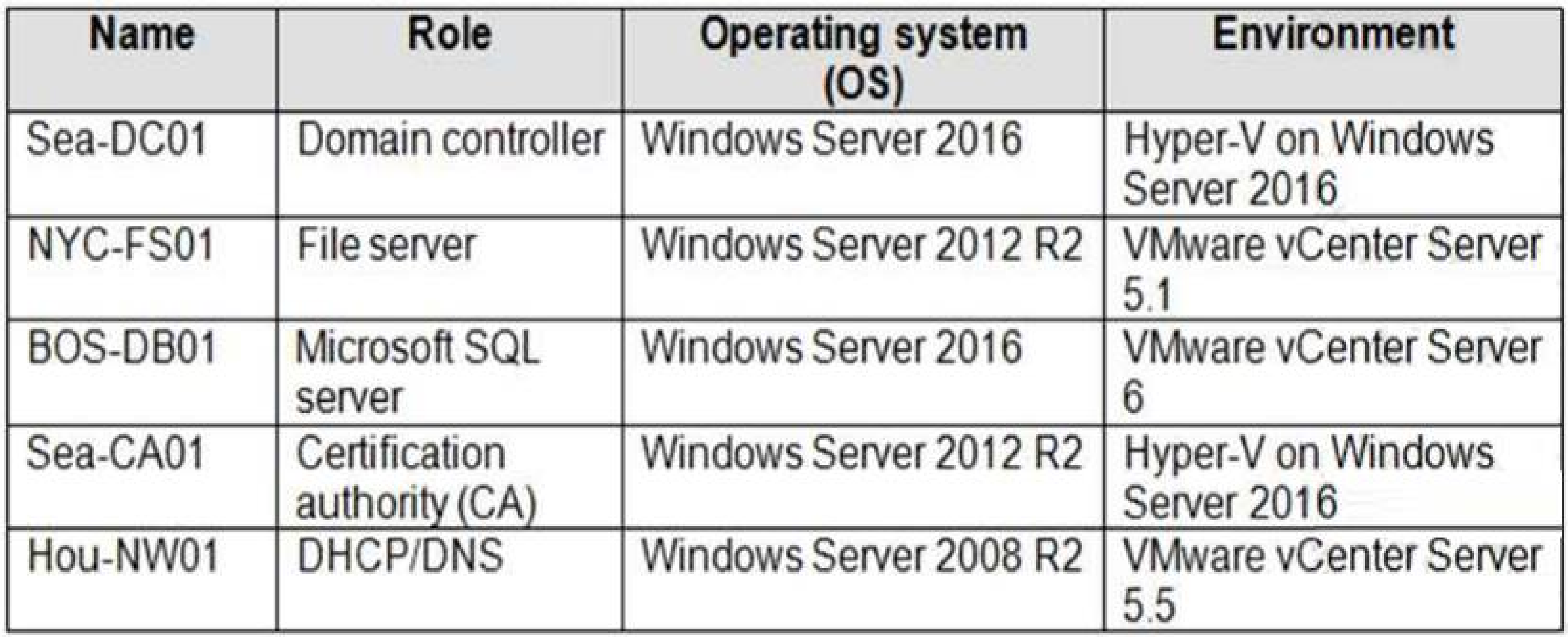
NEW QUESTION 20
You need to recommend a solution to automate the configuration for the finance department users. The solution must meet the technical requirements.
What should you include in the recommended?

A. Azure AP B2C
B. Azure AD Identity Protection
C. an Azure logic app and the Microsoft Identity Management (MIM) client
D. dynamic groups and conditional access policies

Answer: D

Explanation: Scenario: Ensure Azure Multi-Factor Authentication (MFA) for the users in the finance department only.
The recommendation is to use conditional access policies that can then be targeted to groups of users, specific applications, or other conditions.
References:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates

NEW QUESTION 22
You plan to move services from your on-premises network to Azure.
You identify several virtual machines that you believe can be hosted in Azure. The virtual machines are shown in the following table.



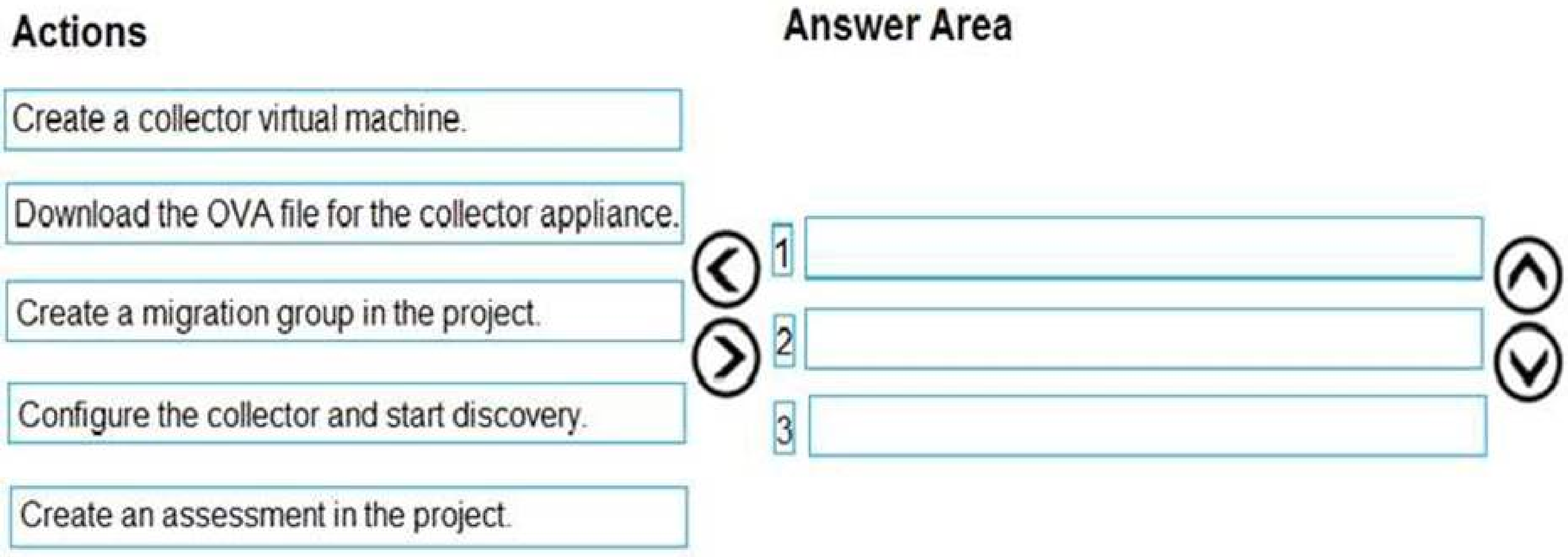
Name	Role	Operating system (OS)	Environment
Sea-DC01	Domain controller	Windows Server 2016	Hyper-V on Windows Server 2016
NYC-FS01	File server	Windows Server 2012 R2	VMware vCenter Server 5.1
BOS-DB01	Microsoft SQL server	Windows Server 2016	VMware vCenter Server 6
Sea-CA01	Certification authority (CA)	Windows Server 2012 R2	Hyper-V on Windows Server 2016
Hou-NW01	DHCP/DNS	Windows Server 2008 R2	VMware vCenter Server 5.5

Which two virtual machines can you access by using Azure migrate? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Sea-CA0l
B. Hou-NW01
C. NYC-FS01
D. Sea-DC01
E. BOS-DB01

Answer: CE

NEW QUESTION 24
DRAG DROP
You create an Azure Migrate project named TestMig in a resource group named test-migration.
You need to discover which on-premises virtual machines to assess for migration. Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Actions

Create a collector virtual machine.

Download the OVA file for the collector appliance.

Create a migration group in the project.

Configure the collector and start discovery.

Create an assessment in the project.

Answer Area

1

2

3

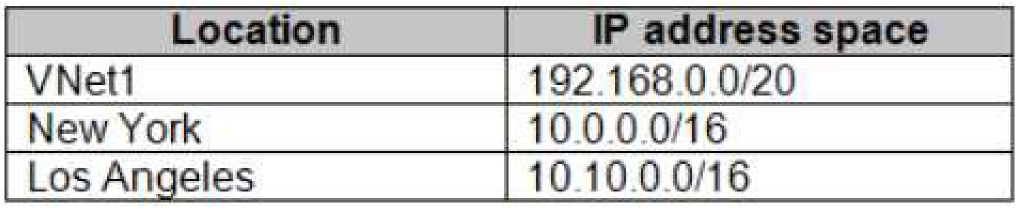
Answer:

Explanation: Step 1: Download the OVA file for the collection appliance
Azure Migrate uses an on-premises VM called the collector appliance, to discover information about your on-premises machines. To create the appliance, you download a setup file in Open Virtualization Appliance (.ova) format, and import it as a VM on your on-premises vCenter Server.
Step 2: Create a migration group in the project
For the purposes of assessment, you gather the discovered VMs into groups. For example, you might group VMs that run the same application. For more precise grouping, you can use dependency visualization to view dependencies of a specific machine, or for all machines in a group and refine the group.
Step 3: Create an assessment in the project
After a group is defined, you create an assessment for it. References:
https://docs.microsoft.com/en-us/azure/migrate/migrate-overview

Case Study: 6
Mix Questions Set D (Implement advanced networking)

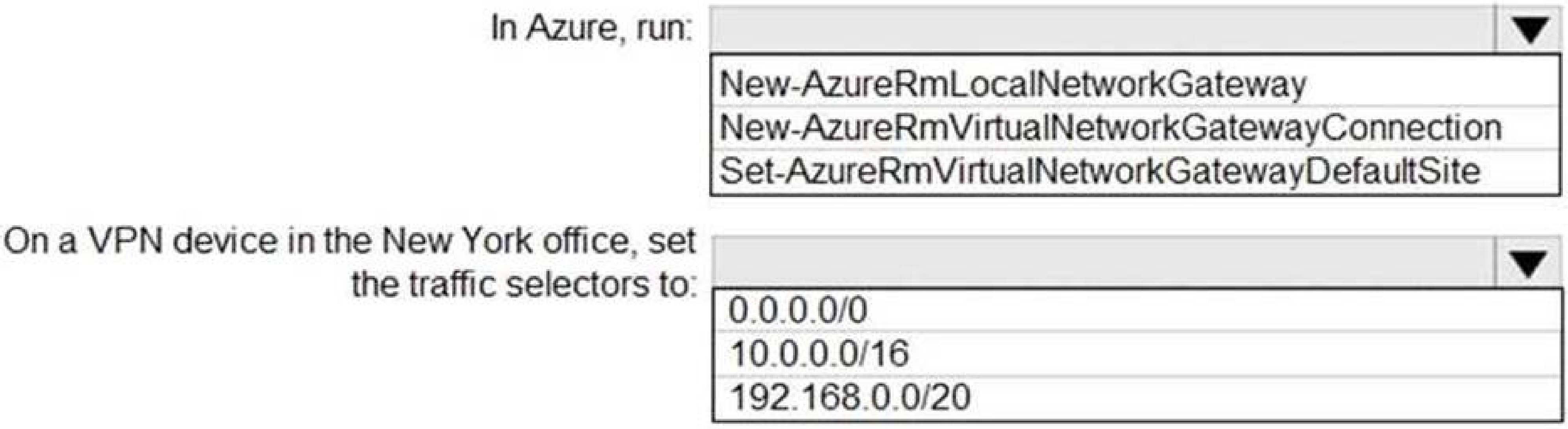
NEW QUESTION 29
HOTSPOT
Your company has offices in New York and Los Angeles.
You have an Azure subscription that contains an Azure virtual network named VNet1. Each office has a site-to-site VPN connection to VNet1.

Each network uses the address spaces shown in the following table.



Location	IP address space
VNet1	192.168.0.0/20
New York	10.0.0.0/16
Los Angeles	10.10.0.0/16

You need to ensure that all Internet-bound traffic from VNet1 is routed through the New York office.
What should you do? To answer, select the appropriate options in the answer are a.
NOTE: Each correct selection is worth one point.



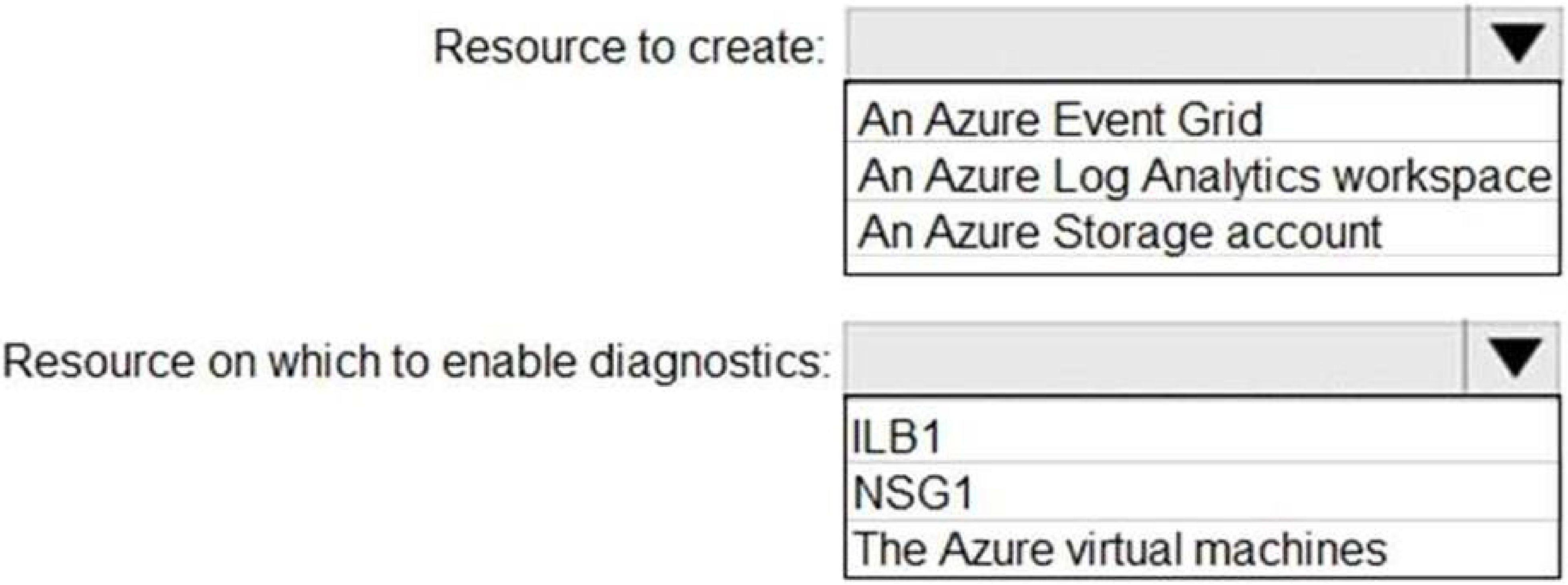
In Azure, run:
- New-AzureRmLocalNetworkGateway
- New-AzureRmVirtualNetworkGatewayConnection
- Set-AzureRmVirtualNetworkGatewayDefaultSite

On a VPN device in the New York office, set the traffic selectors to:
- 0.0.0.0/0
- 10.0.0.0/16
- 192.168.0.0/20

Answer:

Explanation: Incorrect Answers:
Not: New-AzureRmVirtualNetworkGatewayConnection
This command creates the Site-to-Site VPN connection between the virtual network gateway and the on-prem VPN device. We already have Site-to-Site VPN connections.
Box 2: 192.168.0.0/20
Specify the VNET1 address. References:
https://docs.microsoft.com/en-us/powershell/module/azurerm.network/set- azurermvirtualnetworkgatewaydefaultsite

NEW QUESTION 34
HOTSPOT
You have an Azure virtual network named VNet1 that connects to your on-premises network by using a site-to-site VPN. VMet1 contains one subnet named Subnet1.
Subnet1 is associated to a network security group (NSG) named NSG1. Subnet1 contains a basic internal load balancer named ILB1. ILB1 has three Azure virtual machines in the backend pool.
You need to collect data about the IP addresses that connects to ILB1. You must be able to run interactive queries from the Azure portal against the collected data.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Resource to create:
- An Azure Event Grid
- An Azure Log Analytics workspace
- An Azure Storage account

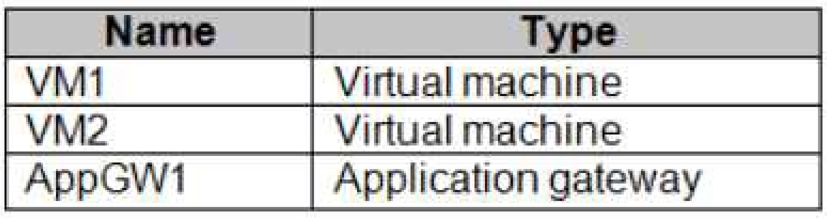
Resource on which to enable diagnostics:
- ILB1
- NSG1
- The Azure virtual machines

Answer:

Explanation: Box 1: An Azure Log Analytics workspace
In the Azure portal you can set up a Log Analytics workspace, which is a unique Log Analytics environment with its own data repository, data sources, and solutions

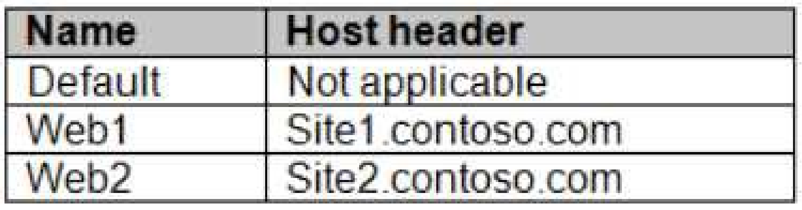
Box 2: ILB1
References:
https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-quick-create-workspace https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-standard-diagnostics

NEW QUESTION 37
HOTSPOT
You have an Azure subscription named Subscription1 that contains the resources in the following table.



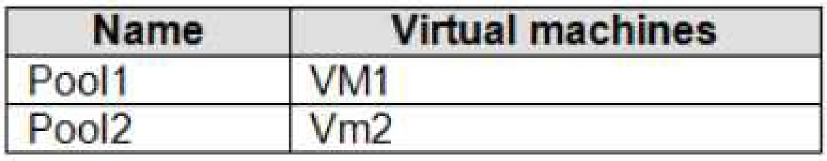
Name	Type
VM1	Virtual machine
VM2	Virtual machine
AppGW1	Application gateway

VM1 and VM2 run the websites in the following table.



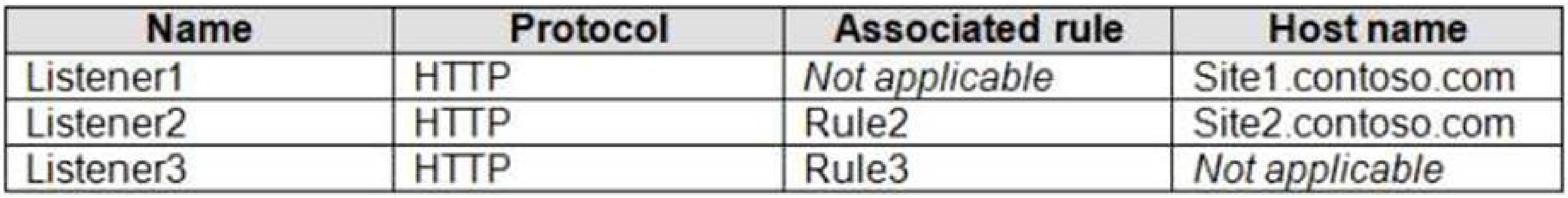
Name	Host header
Default	Not applicable
Web1	Site1.contoso.com
Web2	Site2.contoso.com

AppGW1 has the backend pools in the following table.



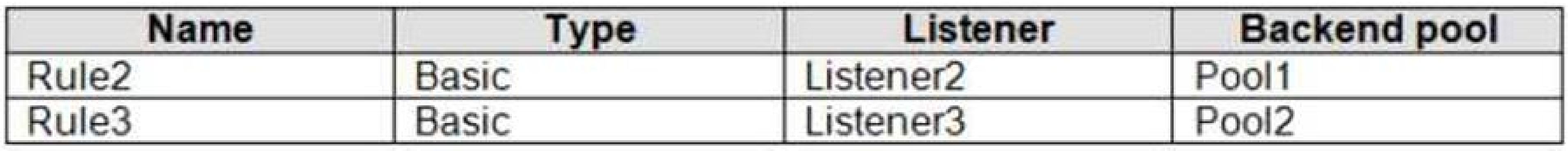
Name	Virtual machines
Pool1	VM1
Pool2	Vm2

DNS resolves site1.contoso.com, site2.contoso.com, and site3.contoso.com to the IP address of AppGW1.
AppGW1 has the listeners in the following table.



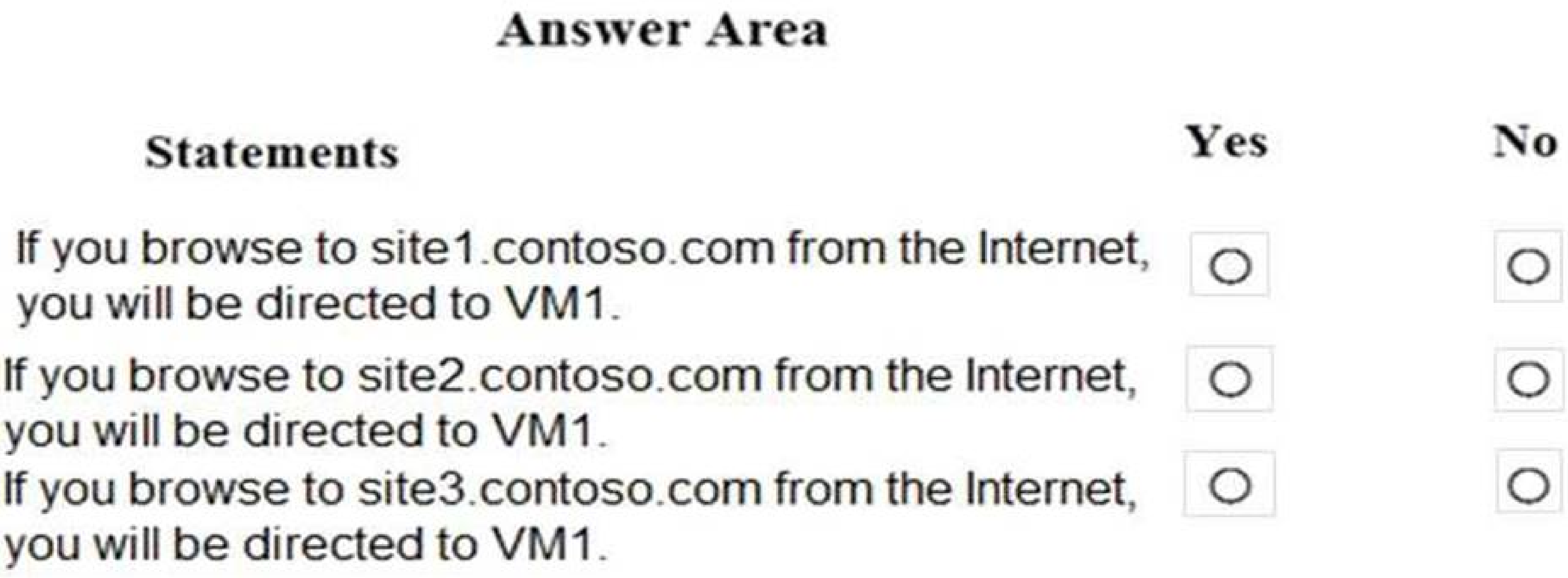
Name	Protocol	Associated rule	Host name
Listener1	HTTP	*Not applicable*	Site1.contoso.com
Listener2	HTTP	Rule2	Site2.contoso.com
Listener3	HTTP	Rule3	*Not applicable*

AppGW1 has the rules in the following table.



Name	Type	Listener	Backend pool
Rule2	Basic	Listener2	Pool1
Rule3	Basic	Listener3	Pool2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
If you browse to site1.contoso.com from the Internet, you will be directed to VM1.	○	○
If you browse to site2.contoso.com from the Internet, you will be directed to VM1.	○	○
If you browse to site3.contoso.com from the Internet, you will be directed to VM1.	○	○

Answer:

Explanation: Vm1 is in Pool1. Rule2 applies to Pool1, Listener 2, and site2.contoso.com

NEW QUESTION 40

You have an azure subscription that contain a virtual named VNet1. VNet1. contains four subnets named Gatesway, perimeter, NVA, and production.
The NVA contain two network virtual appliance (NVAs) that will network traffic inspection between the perimeter subnet and the production subnet.
You need o implement an Azure load balancer for the NVAs. The solution must meet the following requirements:
The NVAs must run in an active-active configuration that uses automatic failover.
The NVA must load balance traffic to two services on the Production subnet. The services have different IP addresses
Which three actions should you perform? Each correct answer presents parts of the solution.
NOTE: Each correct selection is worth one point.

A. Add two load balancing rules that have HA Ports enabled and Floating IP disabled.
B. Deploy a standard load balancer.
C. Add a frontend IP configuration, two backend pools, and a health prob.
D. Add a frontend IP configuration, a backend pool, and a health probe.
E. Add two load balancing rules that have HA Ports and Floating IP enabled.
F. Deploy a basic load balancer.

Answer: BCE

Explanation: A standard load balancer is required for the HA ports.
-Two backend pools are needed as there are two services with different IP addresses.
-Floating IP rule is used where backend ports are reused. Incorrect Answers:
F: HA Ports are not available for the basic load balancer. References:
https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-standard-overview https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-multivip-overview

NEW QUESTION 45
You have five Azure virtual machines that run Windows Server 2016.
You have an Azure load balancer named LB1 that provides load balancing se
You need to ensure that visitors are serviced by the same web server for each request.
What should you configure?

A. Floating IP (direct server return) to Disable
B. Session persistence to Client IP
C. a health probe
D. Session persistence to None

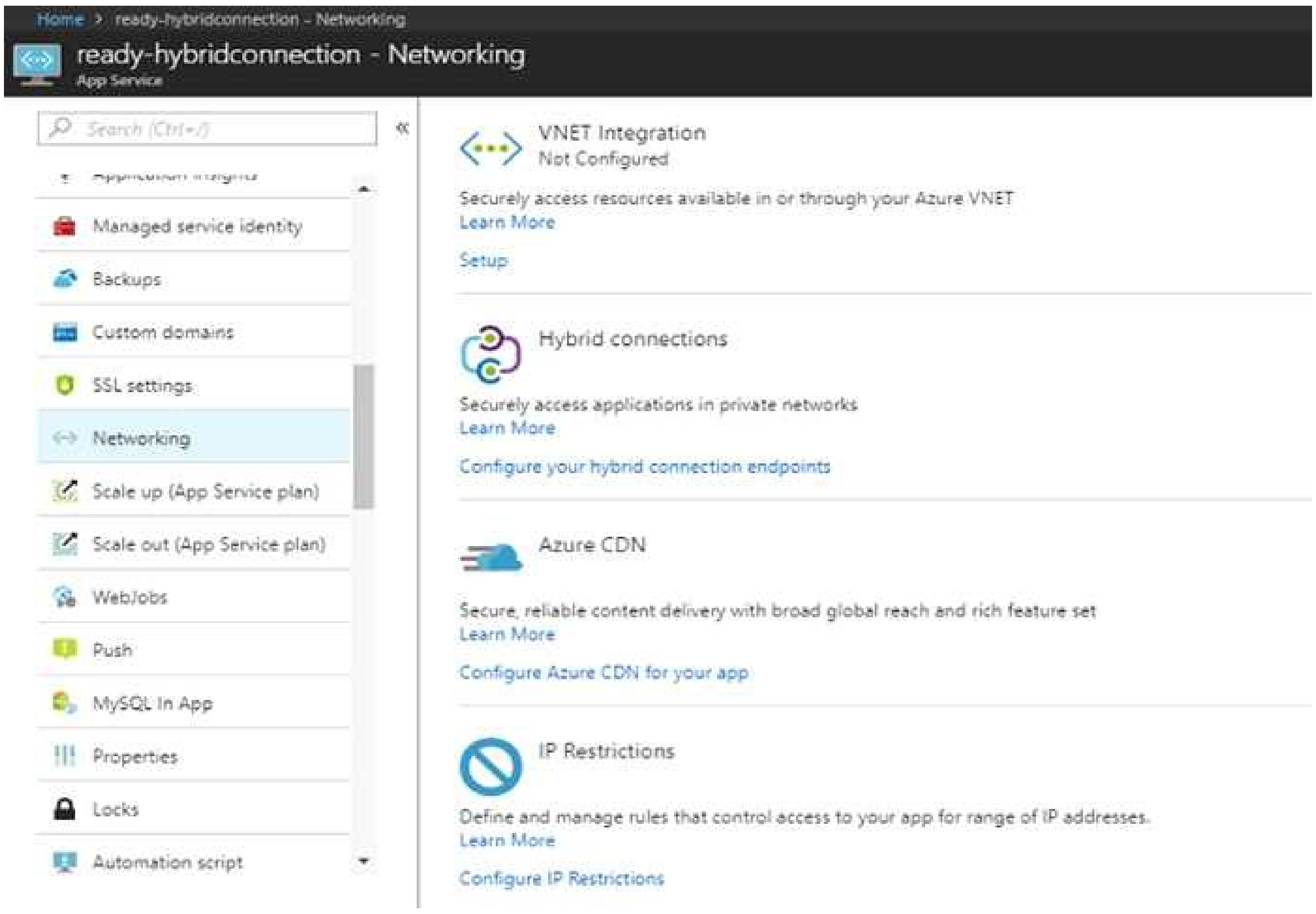
Answer: B

Explanation: You can set the sticky session in load balancer rules with setting the session persistence as the client IP.
References:
https://cloudopszone.com/configure-azure-load-balancer-for-sticky-sessions/

NEW QUESTION 49
Another administrator reports that she is unable to configure a web app named
corplod7509086n3 to prevent all connections from an IP address of 11.0.0.11.
You need to modify corplod7509086n3 to successfully prevent the connections from the IP address. The solution must minimize Azure-related costs.
What should you do from the Azure portal?

Answer:

Explanation: Step 1:
Find and select application corplod7509086n3:
1. In the Azure portal, on the left navigation panel, click Azure Active Directory.
2. In the Azure Active Directory blade, click Enterprise applications. Step 2:
To add an IP restriction rule to your app, use the menu to open Network>IP Restrictions and click on Configure IP Restrictions



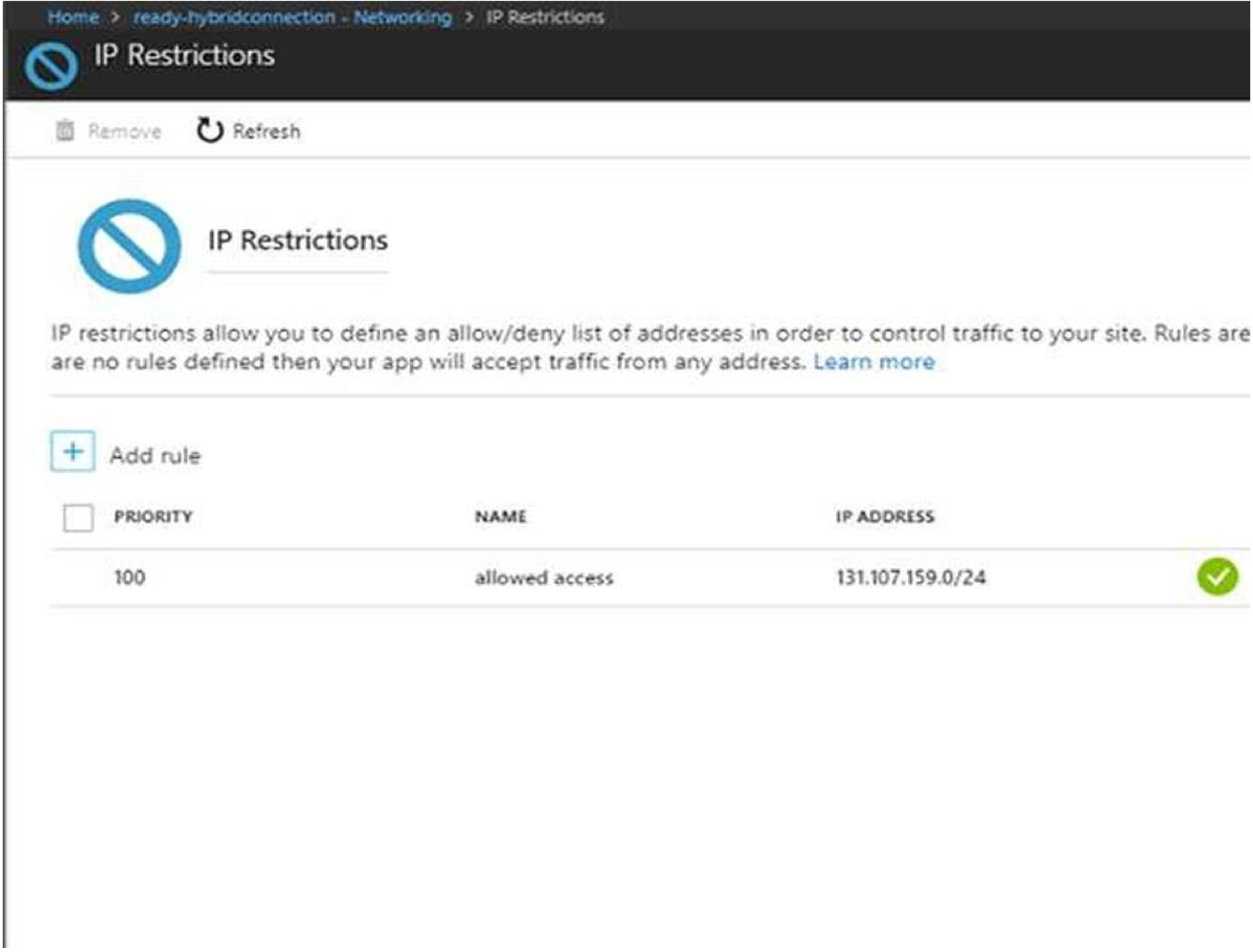
VNET Integration
Not Configured
Securely access resources available in or through your Azure VNET
Learn More
Setup

Hybrid connections
Securely access applications in private networks
Learn More
Configure your hybrid connection endpoints

Azure CDN
Secure, reliable content delivery with broad global reach and rich feature set
Learn More
Configure Azure CDN for your app

IP Restrictions
Define and manage rules that control access to your app for range of IP addresses.
Learn More
Configure IP Restrictions

Step 3:
Click Add rule
You can click on [+] Add to add a new IP restriction rule. Once you add a rule, it will become effective immediately.

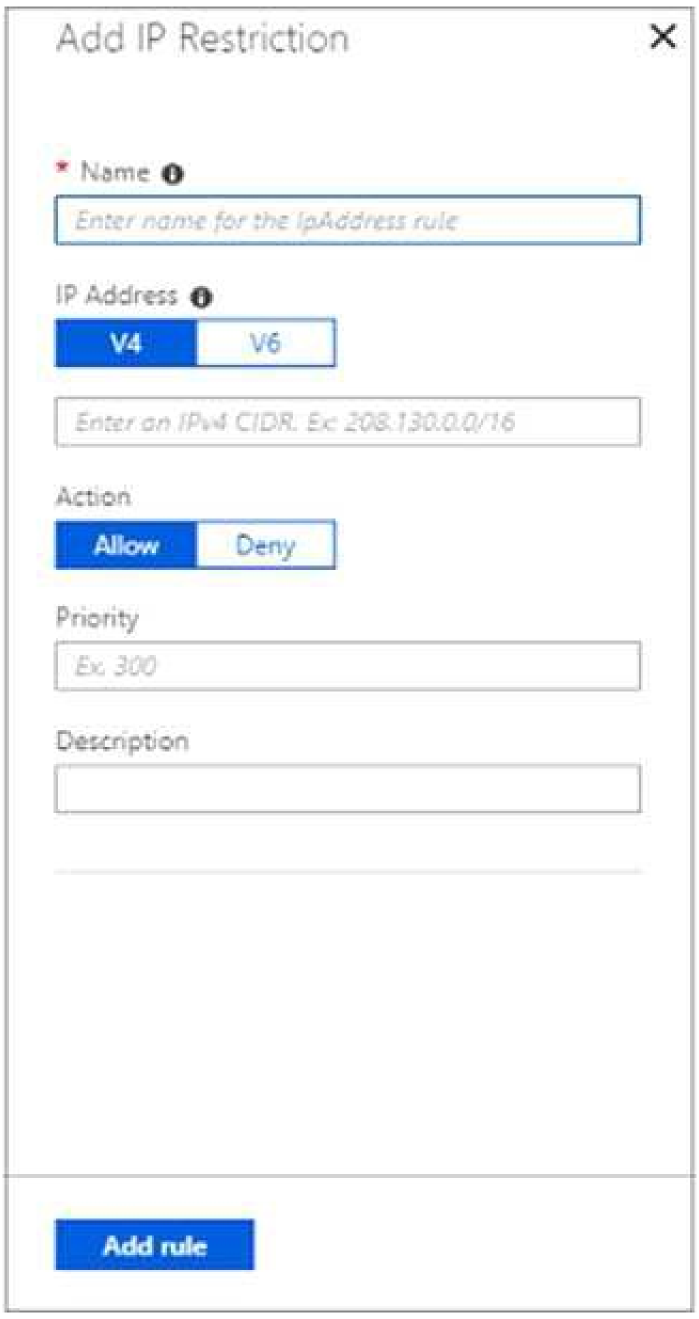

Home > ready-hybridconnection - Networking > IP Restrictions
IP Restrictions
Remove
Refresh
Add rule

IP Restrictions

IP restrictions allow you to define an allow/deny list of addresses in order to control traffic to your site. Rules are
are no rules defined then your app will accept traffic from any address. Learn more

PRIORITY	NAME	IP ADDRESS	
100	allowed access	131.107.159.0/24	✓

Step 4:
Add name, IP address of 11.0.0.11, select Deny, and click Add Rule



Add IP Restriction

* Name

Enter name for the IpAddress rule

IP Address

V4 | V6

Enter an IPv4 CIDR. Ex: 208.130.0.0/16

Action

Allow | Deny

Priority

Ex: 300

Description

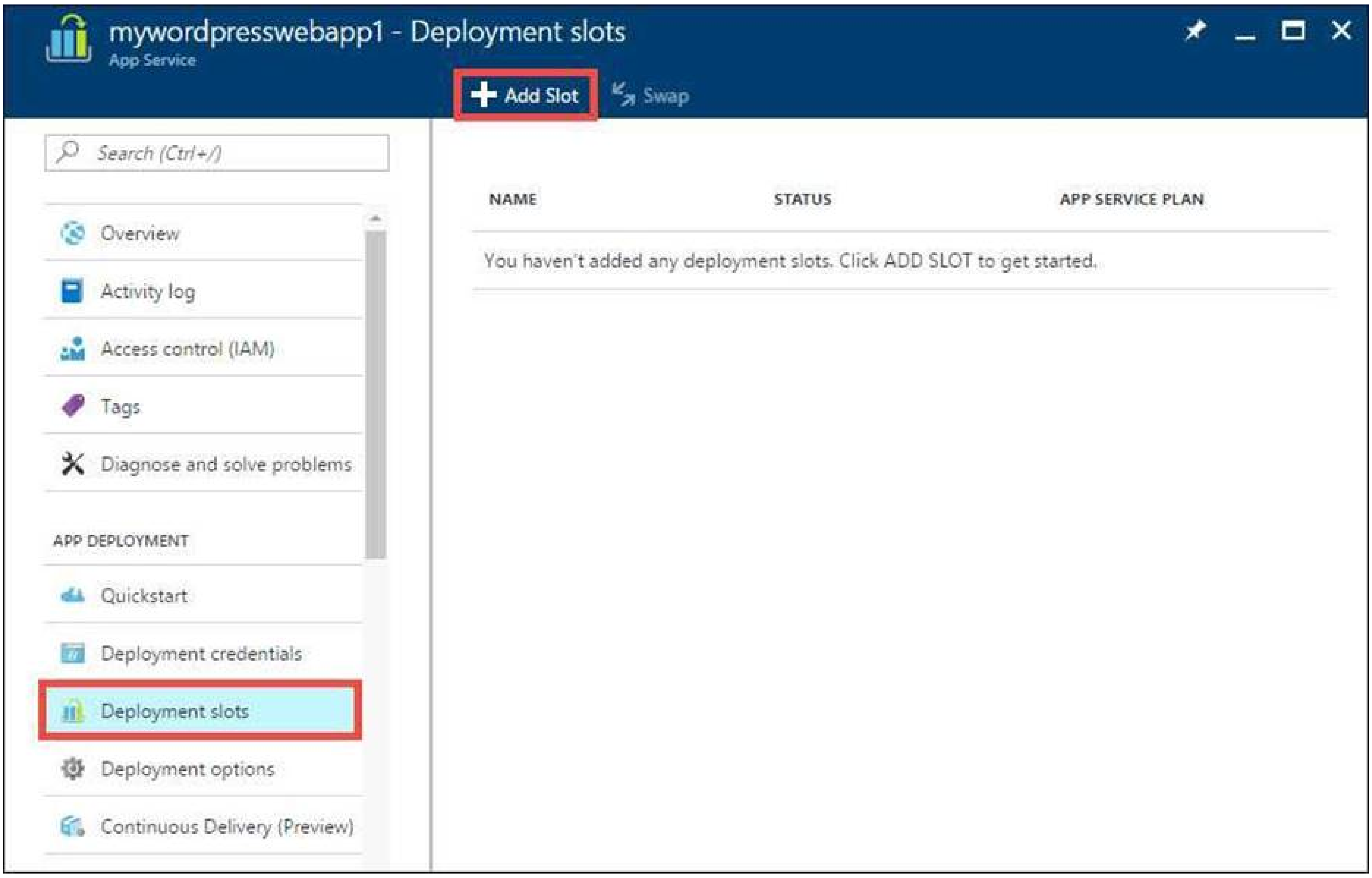
Add rule

References:
https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions

NEW QUESTION 51
You need to add a deployment slot named staging to an Azure web app named corplod@lab.LabInstance.Idn4. The solution must meet the following requirements:
When new code is deployed to staging, the code must be swapped automatically to the production slot. Azure-related costs must be minimized.
What should you do from the Azure portal?

Answer:

Explanation: Step 1:
Locate and open the corplod@lab.LabInstance.Idn4 web app.
1. In the Azure portal, on the left navigation panel, click Azure Active Directory.
2. In the Azure Active Directory blade, click Enterprise applications.
Step 2:
Open your app's resource blade and Choose the Deployment slots option, then click Add Slot.



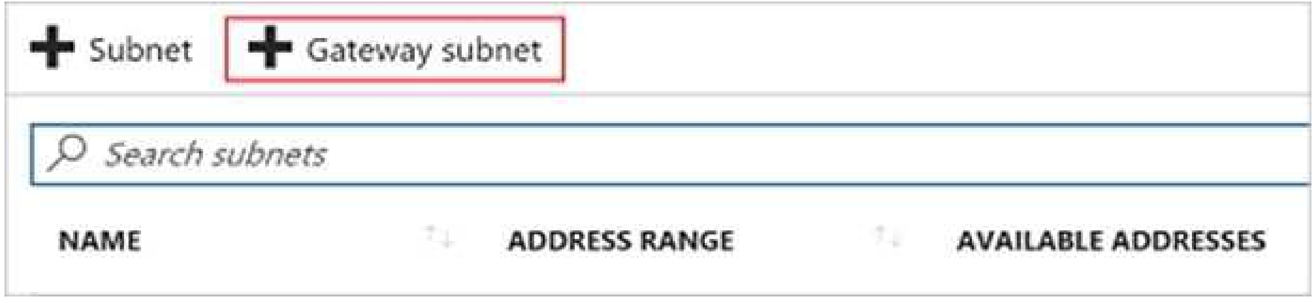
You haven't added any deployment slots. Click ADD SLOT to get started.

Step 3:
In the Add a slot blade, give the slot a name, and select whether to clone app configuration from another existing deployment slot. Click the check mark to continue.
The first time you add a slot, you only have two choices: clone configuration from the default slot in production or not at all.
References:
https://docs.microsoft.com/en-us/azure/app-service/web-sites-staged-publishing

NEW QUESTION 54
You plan to deploy an application getaway named appgw1015 to load balance IP traffic to the Azure virtual machines connected to subnet0.
You need to configure a virtual network named VNET1015 to support the planned application gateway.
What should you do from the Azure portal?

Answer:

Explanation: Step 1:
Click Networking, Virtual Network, and select VNET1015.
Step 2:
Click Subnets, and Click +Add on the VNET1015 - Subnets pane that appears.
Step 3:
On the Subnets page, click +Gateway subnet at the top to open the Add subnet page.

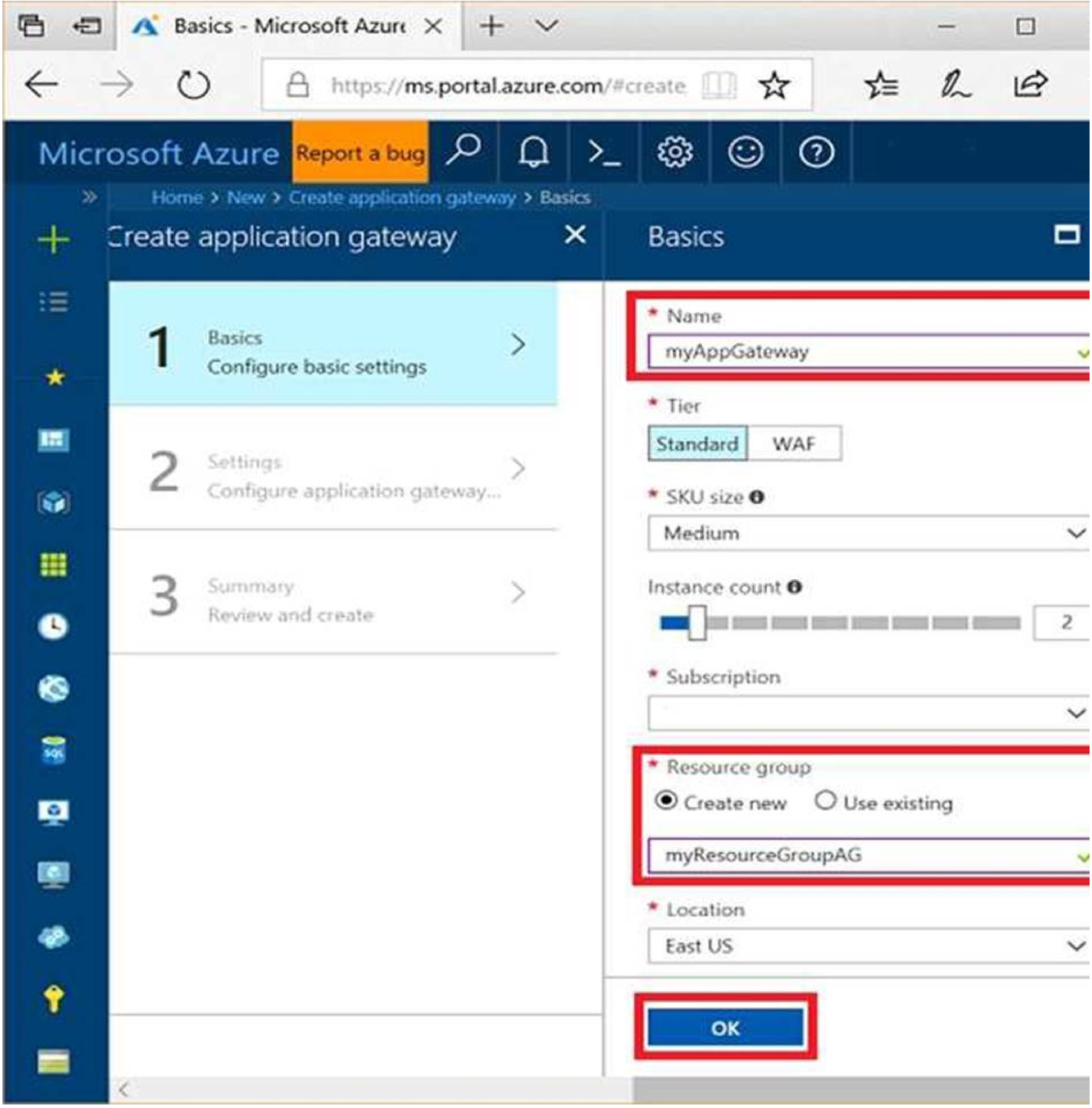


Step 4:
Locate subnet0 and add it. References:
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource- manager-portal

NEW QUESTION 55
You need to deploy an application gateway named appgwl015 to meet the following requirements: Load balance internal IP traffic to the Azure virtual machines connected to subnet0.
Provide a Service Level Agreement (SLA) of 99.99 percent availability for the Azure virtual machines.
What should you do from the Azure portal?

Answer:

Explanation: Step 1:
Click New found on the upper left-hand corner of the Azure portal.
Step 2:
Select Networking and then select Application Gateway in the Featured list.
Step 3:
Enter these values for the application gateway: appgw1015 - for the name of the application gateway. SKU Size: Standard_V2
The new SKU [Standard_V2] offers autoscaling and other critical performance enhancements.


Basics - Microsoft Azure
https://ms.portal.azure.com/#create
Microsoft Azure
Report a bug
Home > New > Create application gateway > Basics
OK

Create application gateway

1 Basics
Configure basic settings

2 Settings
Configure application gateway...

3 Summary
Review and create

Basics

* Name
myAppGateway

* Tier
Standard WAF

* SKU size
Medium

Instance count
2

* Subscription

* Resource group
● Create new ○ Use existing
myResourceGroupAG

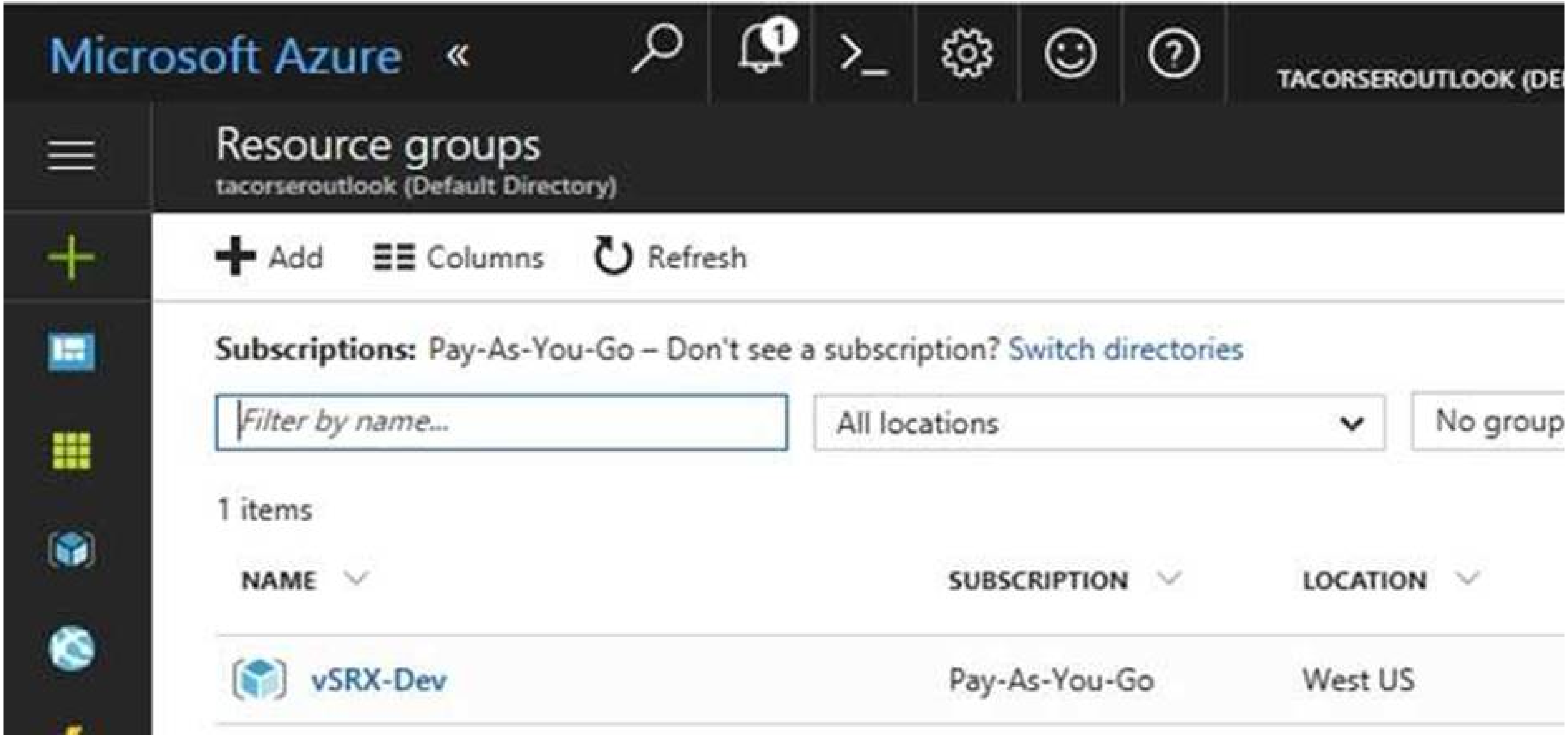
* Location
East US

Step 4:
Accept the default values for the other settings and then click OK.
Step 5:
Click Choose a virtual network, and select subnet0. References:
https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-create-gateway- portal

NEW QUESTION 60
You plan to grant the member of a new Azure AD group named crop 75099086 the right to delegate administrative access to any resource in the resource group named 7509086.
You need to create the Azure AD group and then to assign the correct to e to the group. The solution must use the principle of least privilege and minimize the number of role assignments.
What should you do from the Azure portal?

Answer:

Explanation: Step 1:
Click Resource groups from the menu of services to access the Resource Groups blade



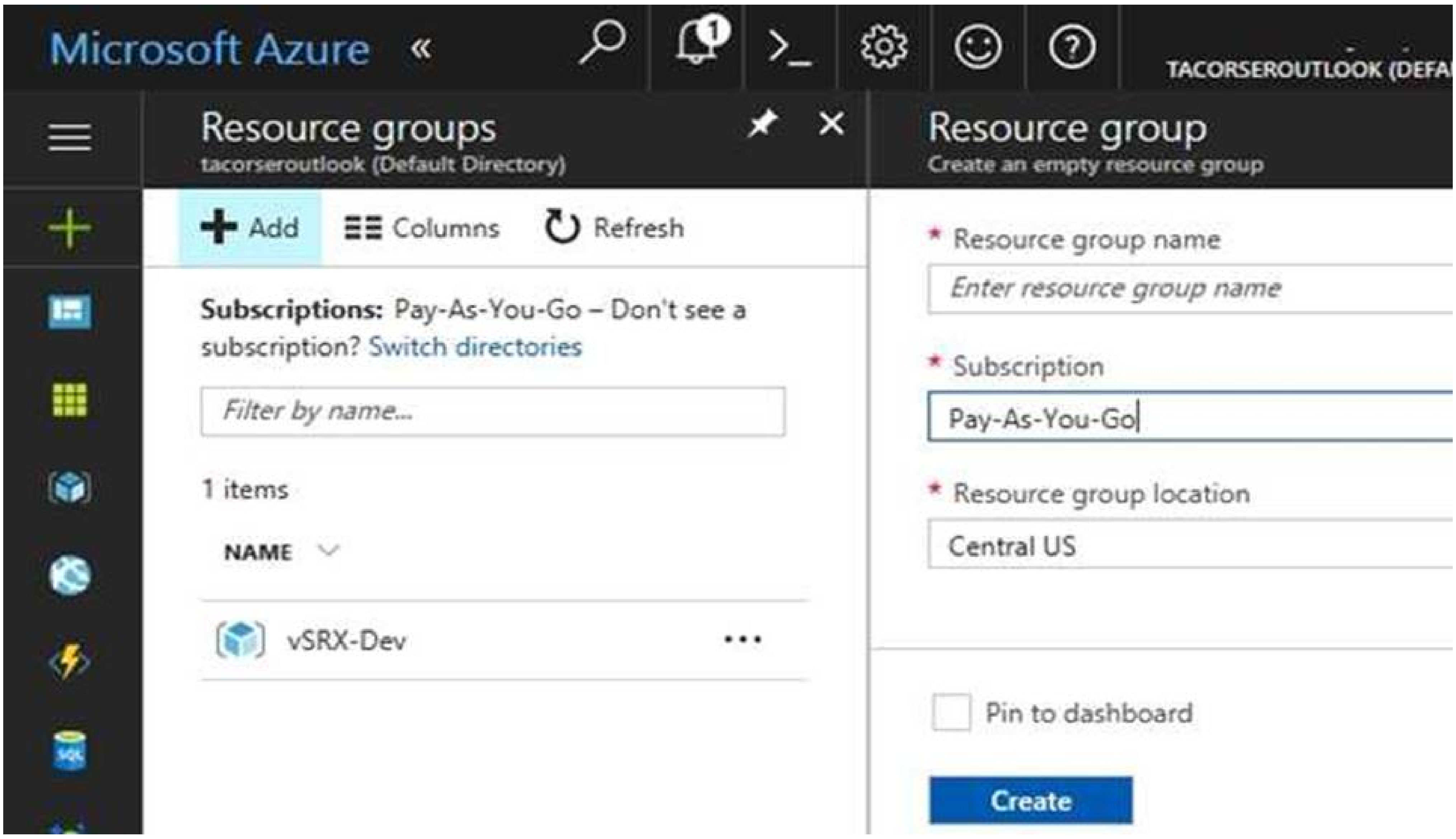
Subscriptions: Pay-As-You-Go – Don't see a subscription? Switch directories

Filter by name...

1 items

NAME	SUBSCRIPTION	LOCATION
vSRX-Dev	Pay-As-You-Go	West US

Step 2:
Click Add (+) to create a new resource group. The Create Resource Group blade appears. Enter corp7509086 as the Resource group name, and click the Create button.



Subscriptions: Pay-As-You-Go – Don't see a subscription? Switch directories

Filter by name...

1 items

* Resource group name

Enter resource group name

* Subscription

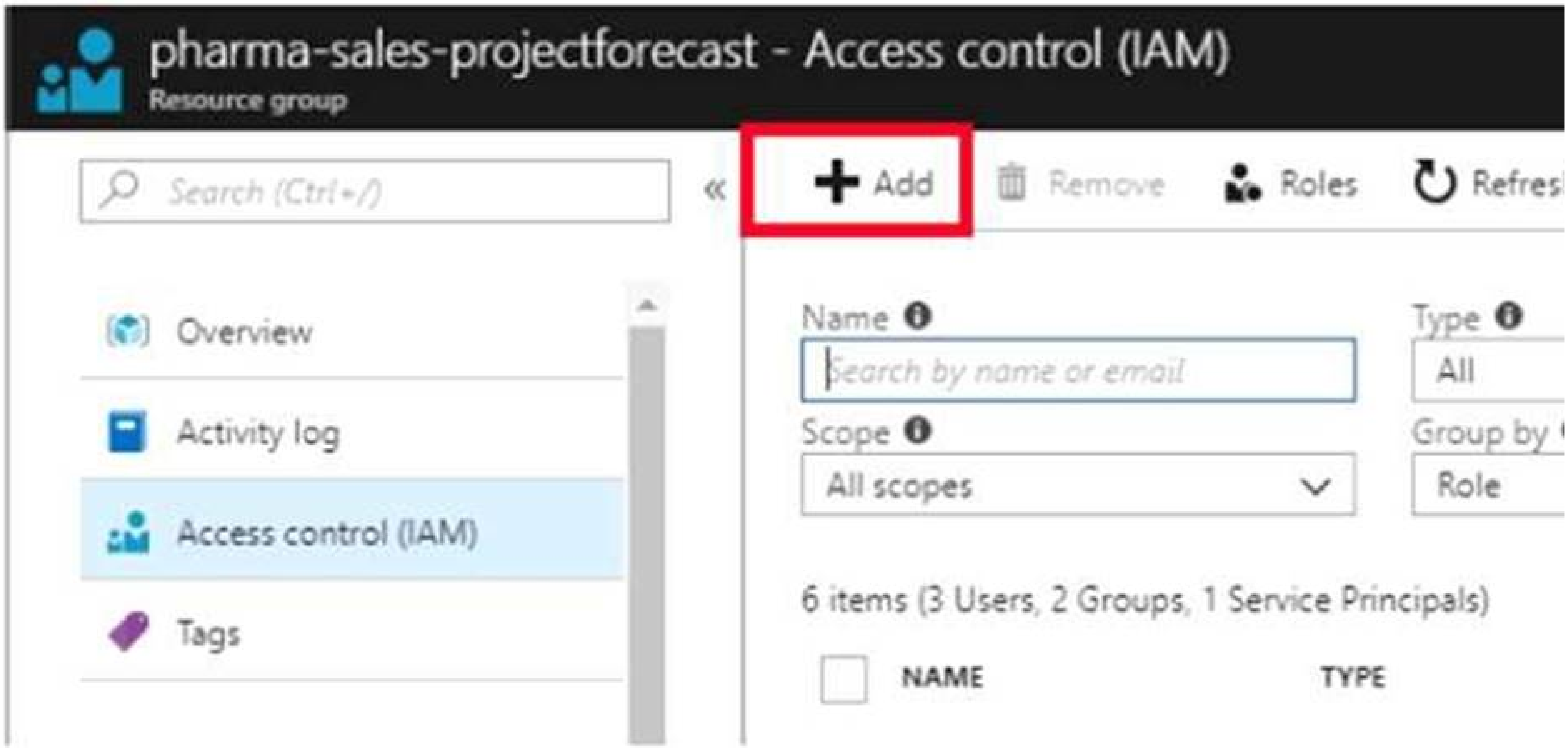
Pay-As-You-Go

* Resource group location

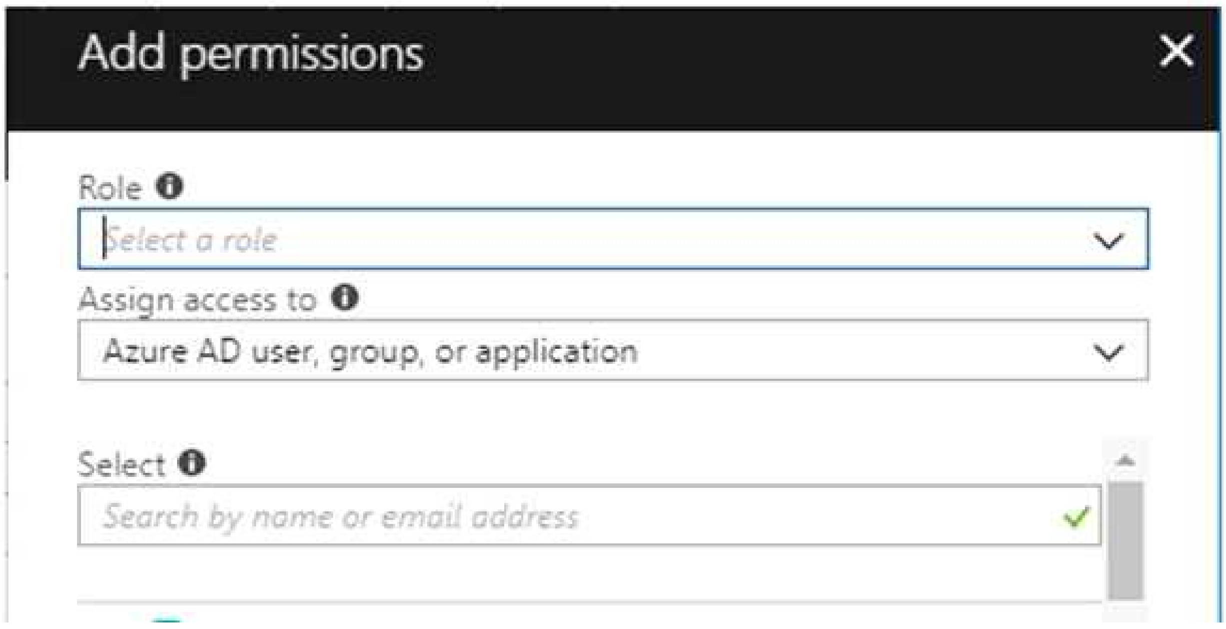
Central US

□ Pin to dashboard

Step 3:
Select Create.
Your group is created and ready for you to add members. Now we need to assign a role to this resource group scope. Step 4:
Choose the newly created Resource group, and Access control (IAM) to see the current list of role assignments at the resource group scope. Click +Add to open the Add permissions pane.



Step 5:
In the Role drop-down list, select a role Delegate administration, and select Assign access to: resource group corp7509086


Add permissions
Role
Select a role
Assign access to
Azure AD user, group, or application
Select
Search by name or email address

References:
https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal https://www.juniper.net/documentation/en_US/vsrx/topics/task/multi-task/security-vsrx-azure- marketplace-resource-group.html

Case Study: 8
Mix Questions Set E (Security Identities)

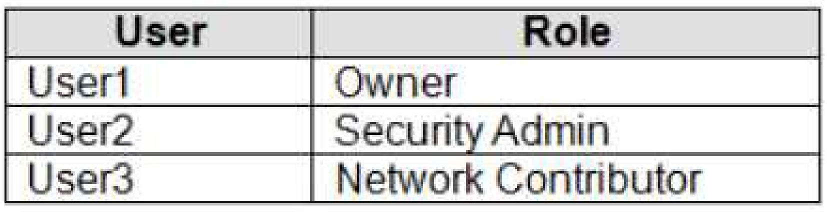
NEW QUESTION 65
You are the global administrator for an Azure Active Directory (Azure AD) tenet named adatum.com. You need to enable two-step verification for Azure users.
What should you do?

A. Create a sign-in risk policy in Azure AD Identity Protection
B. Enable Azure AD Privileged Identity Management.
C. Create and configure the Identity Hub.
D. Configure a security policy in Azure Security Center.

Answer: A

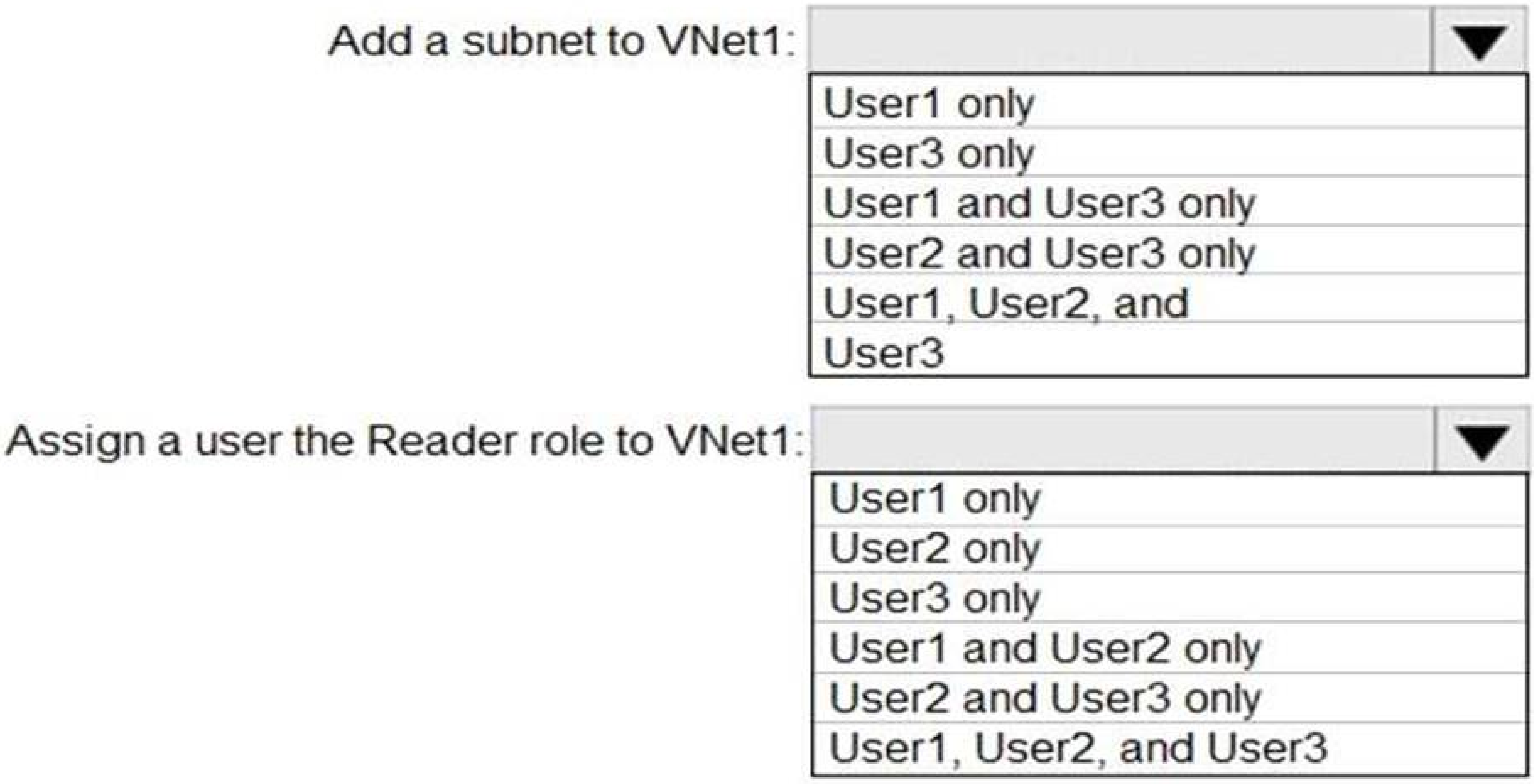
Explanation: With Azure Active Directory Identity Protection, you can:
?require users to register for multi-factor authentication
?handle risky sign-ins and compromised users References:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/flows

NEW QUESTION 67
HOTSPOT
You have an Azure subscription named Subscription1 that contains a virtual network named VNet1. You add the users in the following table.



User	Role
User1	Owner
User2	Security Admin
User3	Network Contributor

Which user can perform each configuration? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Add a subnet to VNet1:
- User1 only
- User3 only
- User1 and User3 only
- User2 and User3 only
- User1, User2, and User3

Assign a user the Reader role to VNet1:
- User1 only
- User2 only
- User3 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

Answer:

Explanation: Box 1: User1 and User3 only.
The Owner Role lets you manage everything, including access to resources.
The Network Contributor role lets you manage networks, but not access to them. Box 2: User1 and User2 only
The Security Admin role: In Security Center only: Can view security policies, view security states, edit security policies, view alerts and recommendations, dismiss alerts and recommendations.
References:
https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

NEW QUESTION 70
You have an Azure subscription named Subscnption1 that contains an Azure virtual machine named VM1. VM1 is in a resource group named RG1.
VM1 runs services that will be used to deploy resources to RG1.
You need to ensure that a service running on VM1 can manage the resources in RG1 by using the identity of VM1. What should you do fit -

A. From the Azure portal modify the Access control (1AM) settings of VM1.
B. From the Azure portal, modify the Policies settings of RG1.
C. From the Azure portal, modify the value of the Managed Service Identity option for VM1.
D. From the Azure portal, modify the Access control (IAM) settings of RG1.

Answer: C

Explanation: A managed identity from Azure Active Directory allows your app to easily access other AAD-protected resources such as Azure Key Vault. The identity is managed by the Azure platform and does not require you to provision or rotate any secrets.
User assigned managed identities can be used on Virtual Machines and Virtual Machine Scale Sets. References:
https://docs.microsoft.com/en-us/azure/app-service/app-service-managed-service-identity

NEW QUESTION 72
You are configuring Azure Active Directory (AD) Privileged Identity Management.
You need to provide a user named Admm1 with read access to a resource group named RG1 for only one month.
The user role must be assigned immediately.
What should you do?

A. Assign an active role.
B. Assign an eligible role.
C. Assign a permanently active role.
D. Create a custom role and a conditional access policy.

Answer: B

Explanation: Azure AD Privileged Identity Management introduces the concept of an eligible admin. Eligible admins should be users that need privileged access now and then, but not all-day, every day. The role is inactive until the user needs access, then they complete an activation process and become an active admin for a predetermined amount of time.
References:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

NEW QUESTION 73
You have an Azure Active Directory (Azure AD) tenant named Tenant1 and an Azure subscription named You enable Azure AD Privileged Identity Management.
You need to secure the members of the Lab Creator role. The solution must ensure that the lab creators request access when they create labs.
What should you do first?

A. From Azure AD Privileged Identity Management, edit the role settings for Lab Creator.
B. From Subscription1 edit the members of the Lab Creator role.
C. From Azure AD Identity Protection, creates a user risk policy.
D. From Azure AD Privileged Identity Management, discover the Azure resources of Conscription.

Answer: A

Explanation: As a Privileged Role Administrator you can:
?Enable approval for specific roles
?Specify approver users and/or groups to approve requests
?View request and approval history for all privileged roles References:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

NEW QUESTION 77
You have an Azure subscription named Subscription1 and two Azure Active Directory (Azure AD) tenants named Tenant1 and Tenant2.
Subscnption1 is associated to Tenant1 Multi-factor authentication (MFA) is enabled for all the users in Tenant1.
You need to enable MFA for the users in Tenant2. The solution must maintain MFA forTenant1. What should you do first?

A. Transfer the administration of Subscription1 to a global administrator of Tenants.
B. Configure the MFA Server setting in Tenant1.
C. Create and link a subscription to Tenant2.
D. Change the directory for Subscription1.

Answer: C

NEW QUESTION 78
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

AZ-101 Practice Exam Features:

* AZ-101 Questions and Answers Updated Frequently

* AZ-101 Practice Questions Verified by Expert Senior Certified Staff

* AZ-101 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* AZ-101 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The AZ-101 Practice Test Here