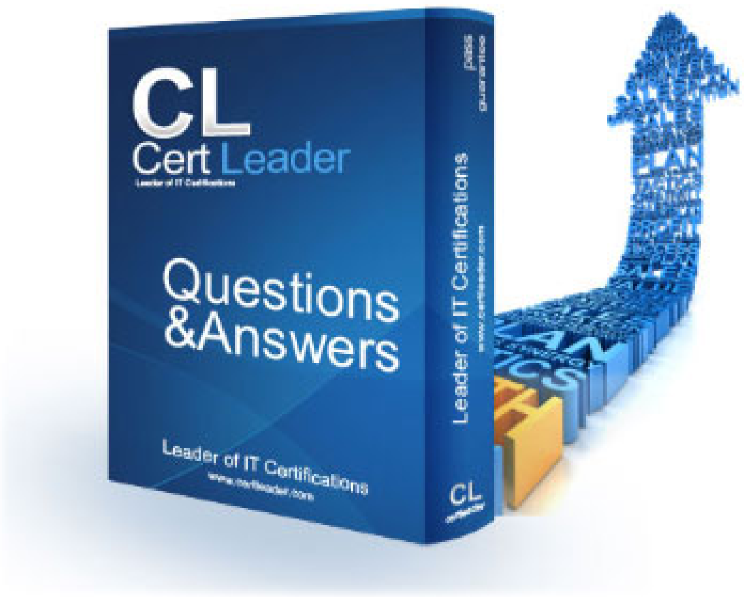
AZ-101 Dumps

Microsoft Azure Integration and Security

https://www.certleader.com/AZ-101-dumps.html



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 web 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 Basic. Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation: The Free Tier provides 60 CPU minutes / day. This explains why App1 is stops. 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 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 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 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 4
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

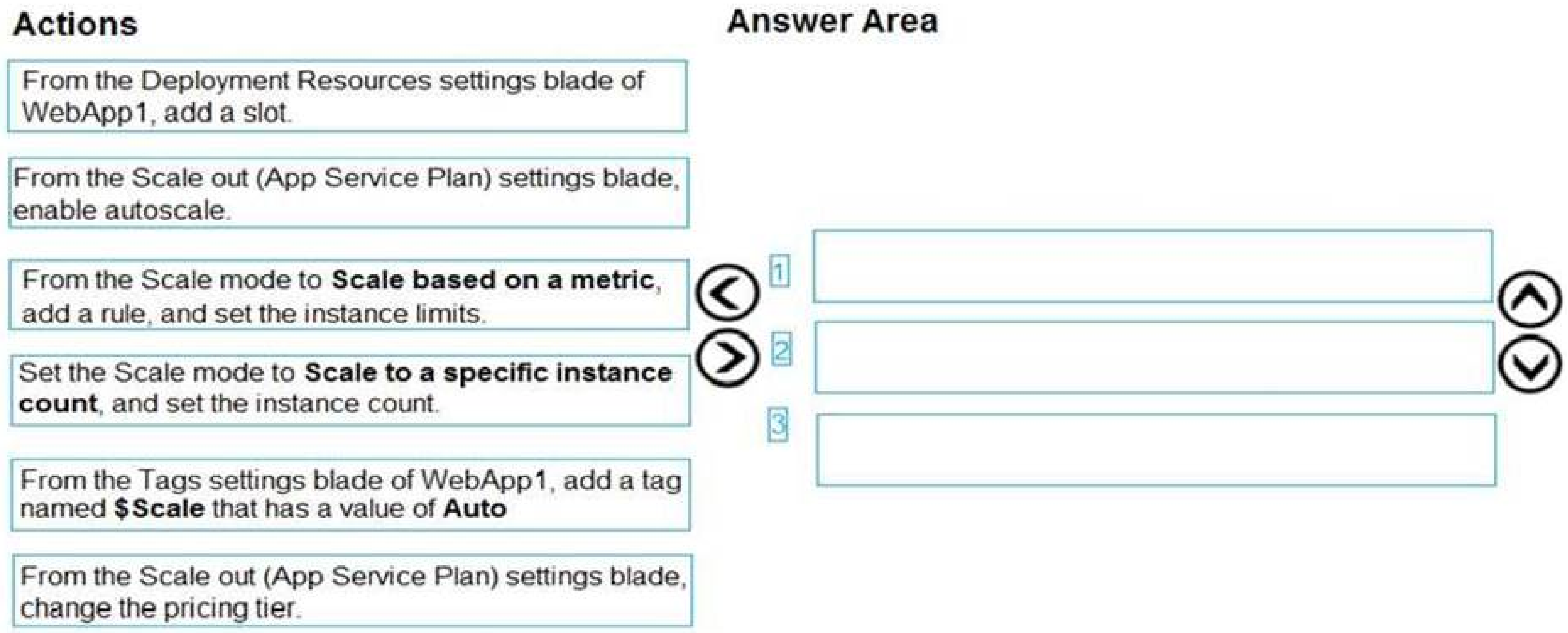
NEW QUESTION 5
Note This question is part of a series of questions that present the same seer Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these 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 6
DRAG DROP
You are developing an Azure web app named WebApp1. WebApp1 uses an Azure App Service plan named Plan1 that uses the B1 pricing tier.
You need to configure WebApp1 to add additional instances of the app when CPU usage exceeds 70 percent for 10 minutes.
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

From the Deployment Resources settings blade of WebApp1, add a slot.

From the Scale out (App Service Plan) settings blade, enable autoscale.

From the Scale mode to **Scale based on a metric**, add a rule, and set the instance limits.

Set the Scale mode to **Scale to a specific instance count**, and set the instance count.

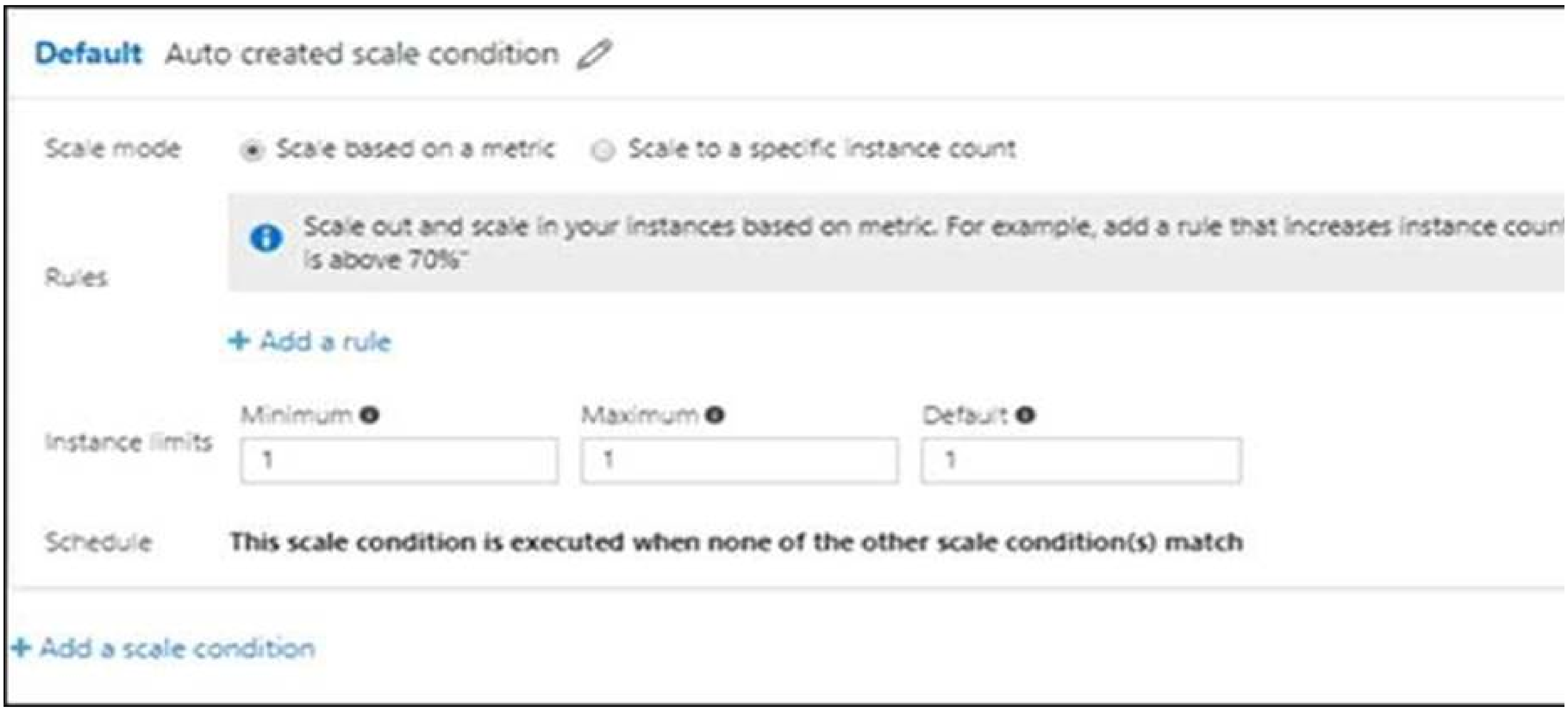
From the Tags settings blade of WebApp1, add a tag named **$Scale** that has a value of **Auto**

From the Scale out (App Service Plan) settings blade, change the pricing tier.

Answer Area

Answer:

Explanation: Box 1: From the Scale out (App Service Plan) settings blade, change the pricing tier The B1 pricing tier only allows for 1 core. We must choose another pricing tier.
Box 2: From the Scale out (App Service Plan) settings blade, enable autoscale
?Log in to the Azure portal at http://portal.azure.com
?Navigate to the App Service you would like to autoscale.
?Select Scale out (App Service plan) from the menu
?Click on Enable autoscale. This activates the editor for scaling rules.



Default Auto created scale condition

Scale mode ● Scale based on a metric ○ Scale to a specific instance count

Rules

Scale out and scale in your instances based on metric. For example, add a rule that increases instance coun
is above 70%"

+ Add a rule

Instance limits

Minimum	Maximum	Default
1	1	1

Schedule **This scale condition is executed when none of the other scale condition(s) match**

+ Add a scale condition

Box 3: From the Scale mode to Scale based on metric, add a rule, and set the instance limits.
Click on Add a rule. This shows a form where you can create a rule and specify details of the scaling. References:
https://azure.microsoft.com/en-us/pricing/details/app-service/windows/ https://blogs.msdn.microsoft.com/hsirtl/2017/07/03/autoscaling-azure-web-apps/

NEW QUESTION 7
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 8
You are building a custom Azure function app to connect to Azure Event Grid.
You need to ensure that resources are allocated dynamically to the function app. Billing must be based on the executions of the app.
What should you configure when you create the function app?

A. the Windows operating system and the Consumption plan hosting plan
B. the Windows operating system and the App Service plan hosting plan
C. the Docker container and an App Service plan that uses the Bl1 pricing tier
D. the Docker container and an App Service plan that uses the SI pricing

Answer: A

Explanation: Azure Functions runs in two different modes: Consumption plan and Azure App Service plan. The Consumption plan automatically allocates compute power when your code is running. Your app is scaled out when needed to handle load, and scaled down when code is not running.
Incorrect Answers:
B: When you run in an App Service plan, you must manage the scaling of your function app. References:
https://docs.microsoft.com/en-us/azure/azure-functions/functions-create-first-azure-function

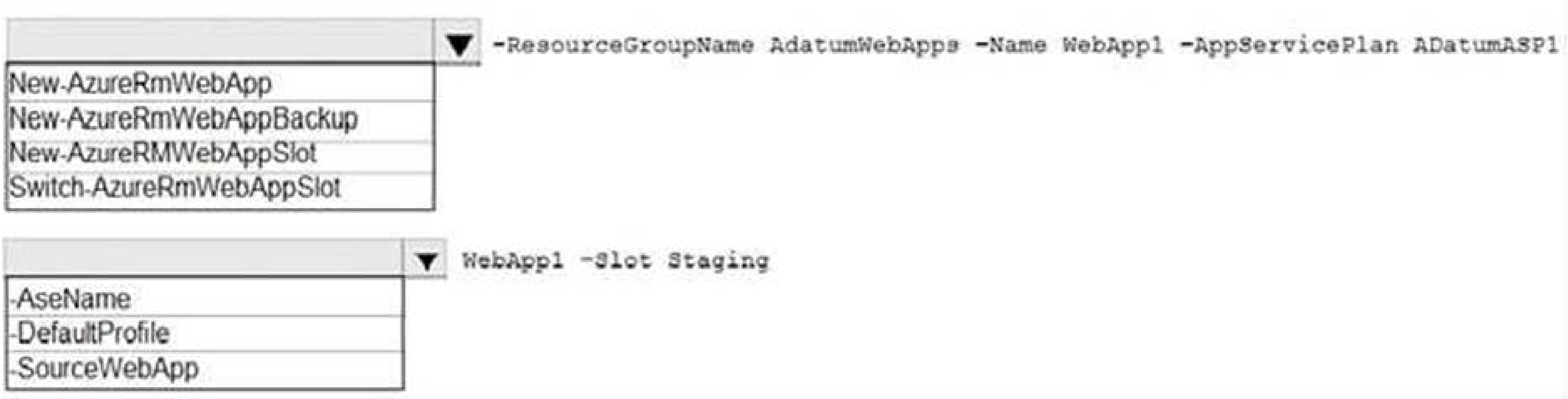
NEW QUESTION 9
You have an Azure App Service plan named AdatumASP1 that uses the P2v2 pricing tier. AdatumASP1 hosts Ml Azure web app named adatumwebapp1. You need to delegate the management of adatumwebapp1 to a group named Devs. Devs must be able to perform the following tasks:
• Add deployment slots.
• View the configuration of AdatumASP1.
• Modify the role assignment for adatumwebapp1. Which role should you assign to the Devs group?

A. Owner
B. Contributor
C. Web Plan Contributor
D. Website Contributor

Answer: B

Explanation: The Contributor role lets you manage everything except access to resources. Incorrect Answers:
A: The Owner role lets you manage everything, including access to resources.
C: The Web Plan Contributor role lets you manage the web plans for websites, but not access to them.
D: The Website Contributor role lets you manage websites (not web plans), but not access to them. References:
https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

NEW QUESTION 10
HOTSPOT
You have an Azure web app named WebApp1.
You need to provide developers with a copy of WebApp1 that they can modify without affecting the production WebApp1. When the developers finish testing their changes, you must be able to switch the current line version of WebApp1 to the new version.
Which command should you run prepare the environment? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



```
[▼] -ResourceGroupName AdatumWebApps -Name WebApp1 -AppServicePlan ADatumASP1
```

- New-AzureRmWebApp
- New-AzureRmWebAppBackup
- New-AzureRMWebAppSlot
- Switch-AzureRmWebAppSlot

```
[▼] WebApp1 -Slot Staging
```

- -AseName
- -DefaultProfile
- -SourceWebApp

Answer:

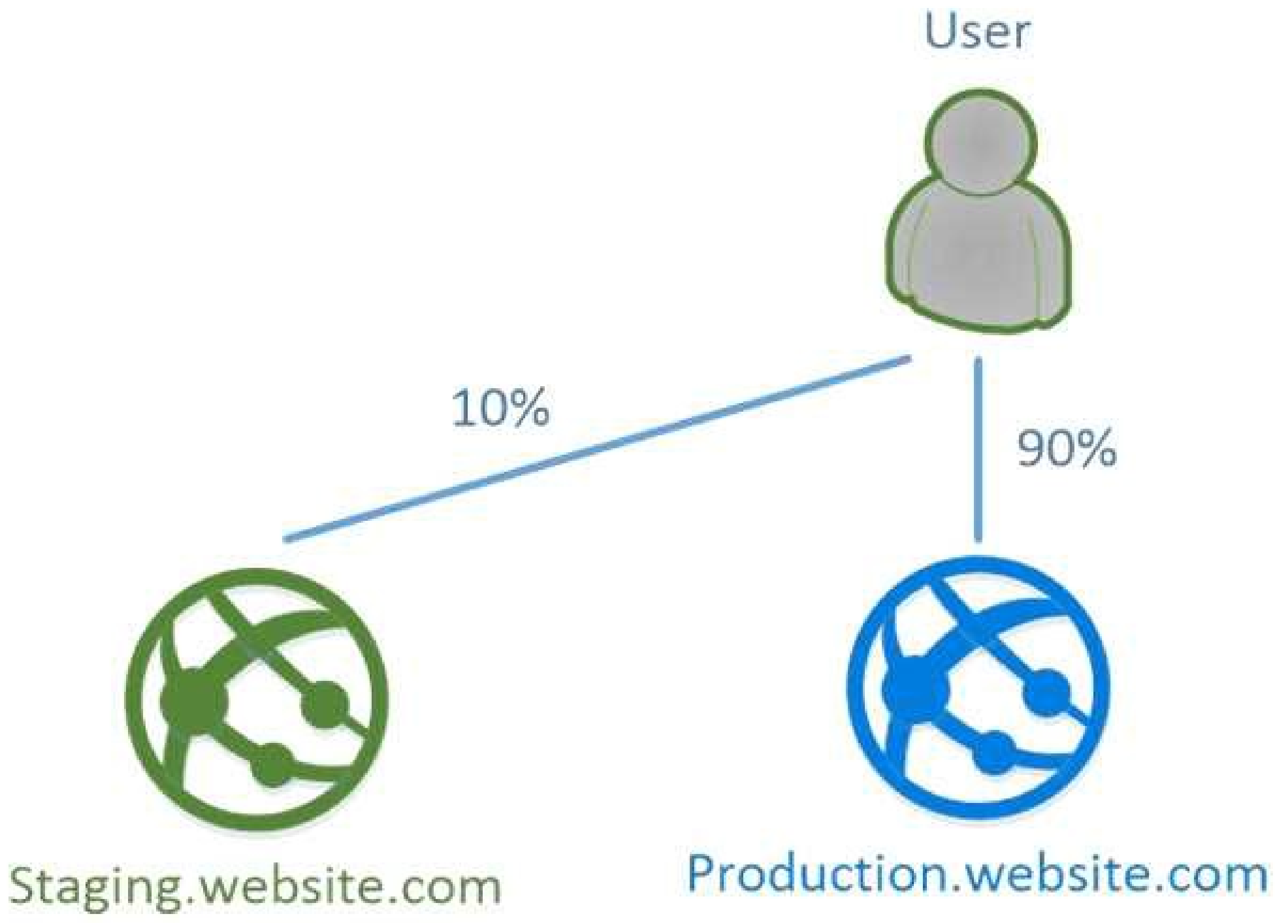
Explanation: Box 1: New-AzureRmWebAppSlot
The New-AzureRmWebAppSlot cmdlet creates an Azure Web App Slot in a given a resource group that uses the specified App Service plan and data center.
Box 2: -SourceWebApp References:
https://docs.microsoft.com/en-us/powershell/module/azurerm.websites/new-azurermwebappslot

NEW QUESTION 10
You have an Azure App Service plan that hosts an Azure App Service named App1. You configure one production slot and four staging slots for App1.
You need to allocate 10 percent of the traffic to each staging slot and 60 percent of the traffic to the production slot.
What should you add to Appl1?

A. slots to the Testing in production blade
B. a performance test
C. a WebJob
D. templates to the Automation script blade

Answer: A

Explanation: Besides swapping, deployment slots offer another killer feature: testing in production. Just like the name suggests, using this, you can actually test in production. This means that you can route a specific percentage of user traffic to one or more of your deployment slots.
Example:

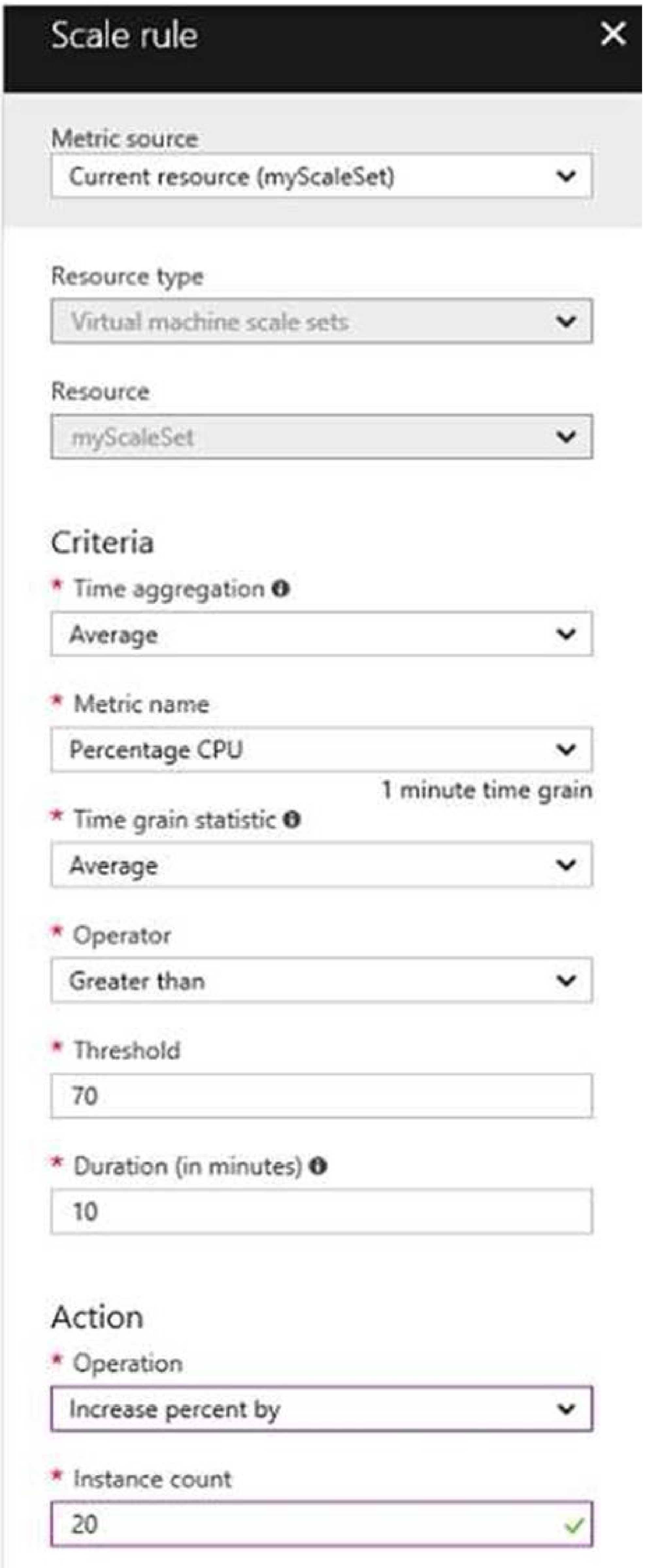


References:
https://stackify.com/azure-deployment-slots/

NEW QUESTION 13
You plan to support many connections to your company's automatically uses up to five instances when CPU utilization on the instances exceeds 70 percent for 10 minutes. When CPU utilization decreases, the solution must automatically reduce the number of instances.
What should you do from the Azure portal?

Answer:

Explanation: Step 1:
Locate the Homepage App Service plan Step 2:
below.
Click Add a rule, and enter the appropriate fields, such as below, and the click Add. Time aggregation: average
Metric Name: Percentage CPU Operator: Greater than Threshold 70
Duration: 10 minutes Operation: Increase count by Instance count: 4



Scale rule

Metric source: Current resource (myScaleSet)

Resource type: Virtual machine scale sets

Resource: myScaleSet

Criteria

* Time aggregation: Average

* Metric name: Percentage CPU

1 minute time grain

* Time grain statistic: Average

* Operator: Greater than

* Threshold: 70

* Duration (in minutes): 10

Action

* Operation: Increase percent by

* Instance count: 20 ✓

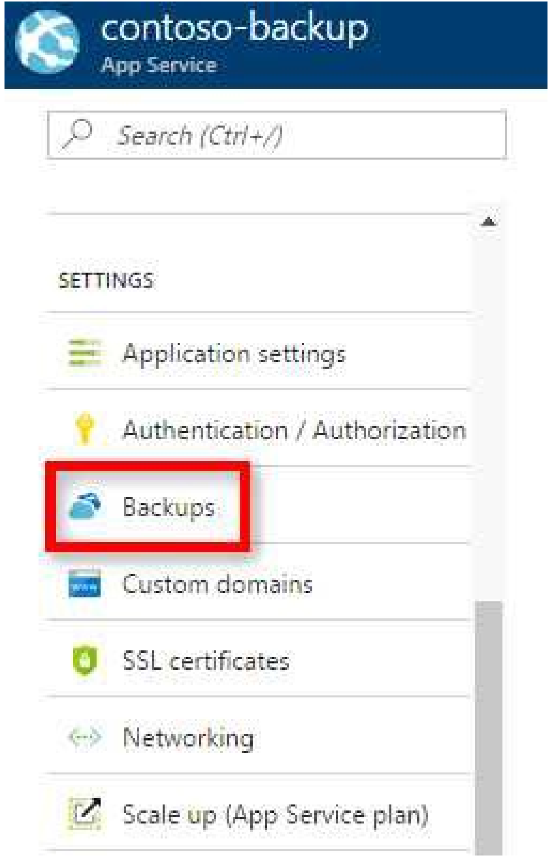
Step 3:
We must add a scale in rule as well. Click Add a rule, and enter the appropriate fields, such as below, then click Add.
Operator: Less than Threshold 70
Duration: 10 minutes Operation: Decrease count by Instance count: 4
References:
https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets- autoscale-portal
https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/insights-autoscale-best-practices

NEW QUESTION 16
You recently deployed a web app named homepagelod7509087.
You need to back up the code used for the web app and to store the code in the homepagelod7509Q87 storage account. The solution must ensure that a new backup is created daily.

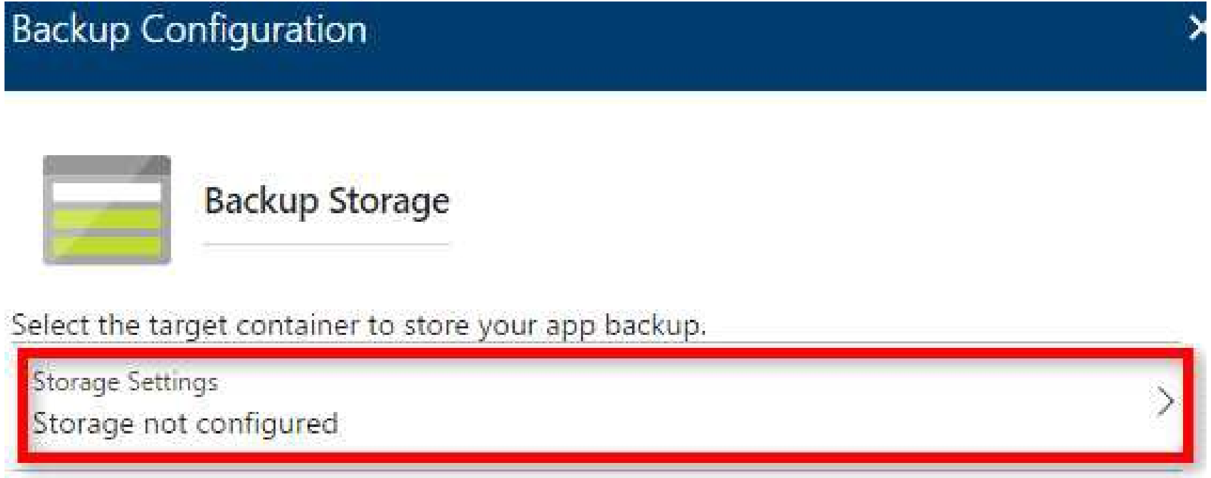
What should you do from the Azure portal?

Answer:

Explanation: Step 1:
Locate and select the web app homepagelod7509087, select Backups. The Backups page is displayed.



Step 2:
In the Backup page, Click Configure. Step 3:
In the Backup Configuration page, click Storage: Not configured to configure a storage account.



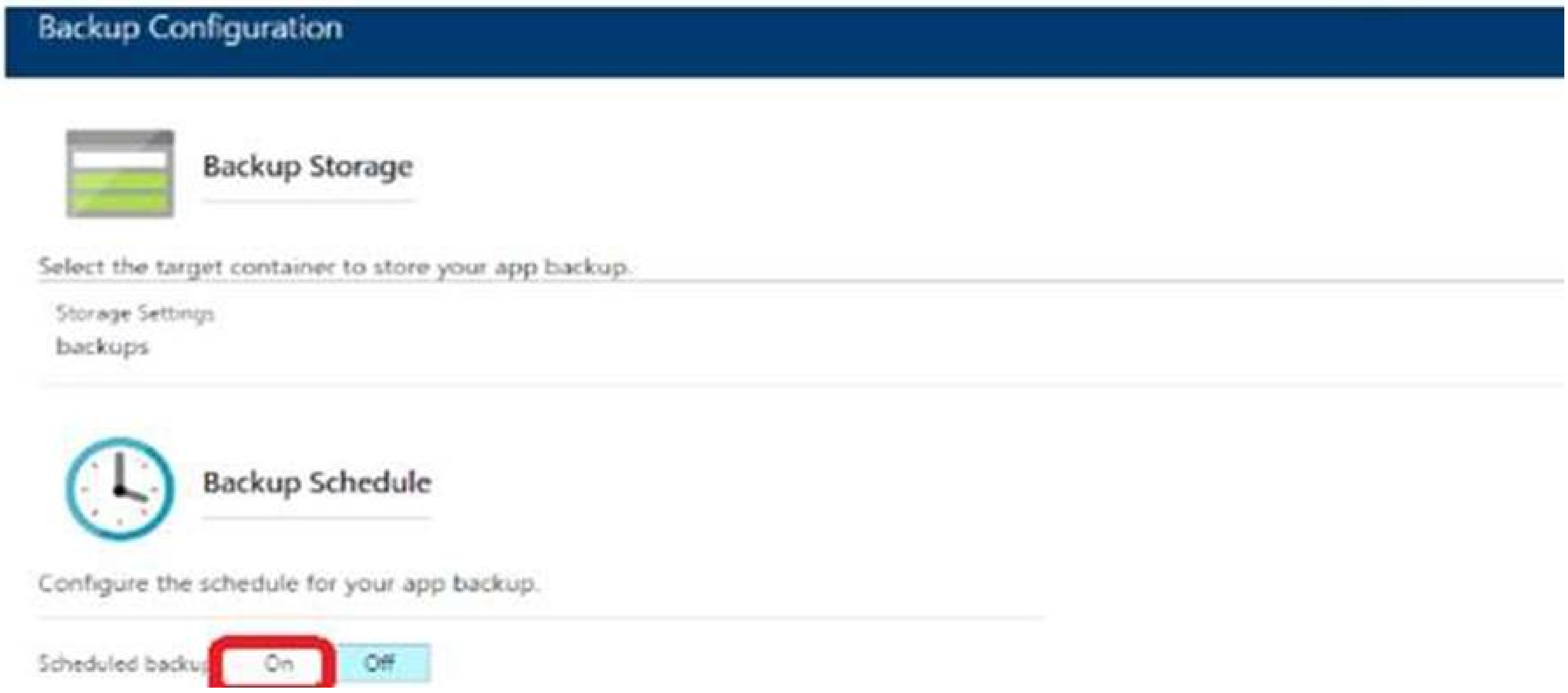
Backup Configuration

Backup Storage

Select the target container to store your app backup.

Storage Settings
Storage not configured

Step 4:
Choose your backup destination by selecting a Storage Account and Container. Select the homepagelod7509087 storage account.
Step 5:
In the Backup Configuration page that is still left open, select Scheduled backup On, and configure daily backups.



Backup Configuration

Backup Storage

Select the target container to store your app backup.

Storage Settings
backups

Backup Schedule

Configure the schedule for your app backup.

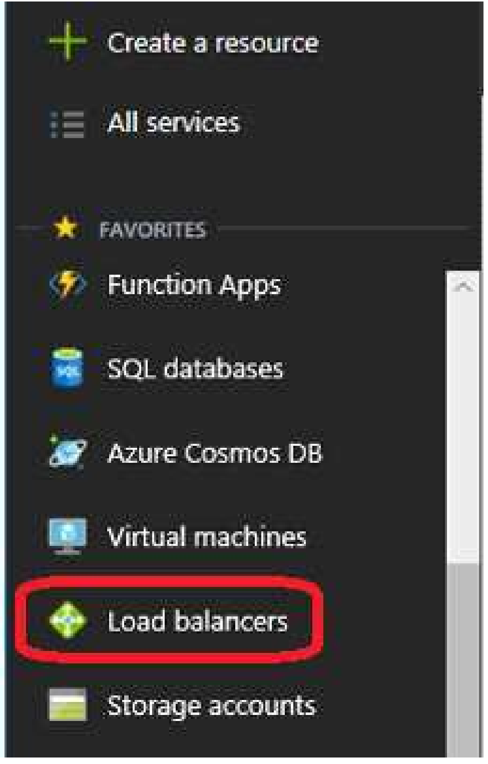
Scheduled backup On Off

Step 6:
In the Backup Configuration page, click Save. Step 7:
In the Backups page, click Backup. References:
https://docs.microsoft.com/en-us/azure/app-service/web-sites-backup

NEW QUESTION 19
Your company recently hired a user named janet-7509087@ExamUsers.com.
You need to ensure that janet-7509087@ ExamUsers.com can connect to load balancer named Web-LAB. The solution must ensure that janet-7509087@ ExamUsers.com can modify the backend pools.
What should you do from the Azure portal?

Answer:

Explanation: Step 1:
In the navigation list, choose Load Balancer.

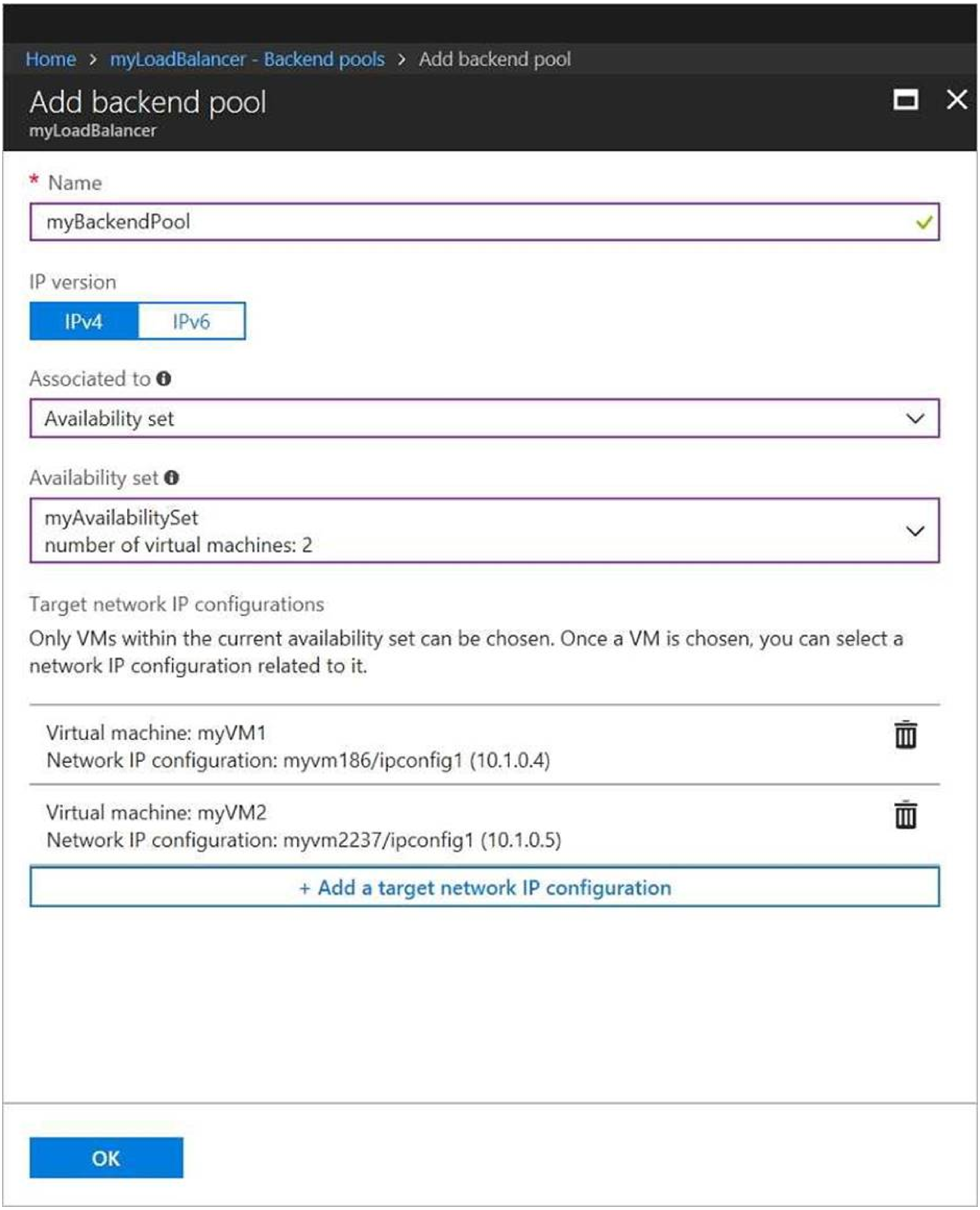


Step 2:
Locate the load balancer named Web-ALB, and click the Access icon. Step3:
In the Users blade, click Roles. In the Roles blade, click Add to add permissions for the user Janet- 7509087@ExamUsers.com.
Step 4:
Add permission to modify backend pools References:
https://docs.microsoft.com/en-us/azure/azure-stack/azure-stack-manage-permissions

NEW QUESTION 20
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:



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)

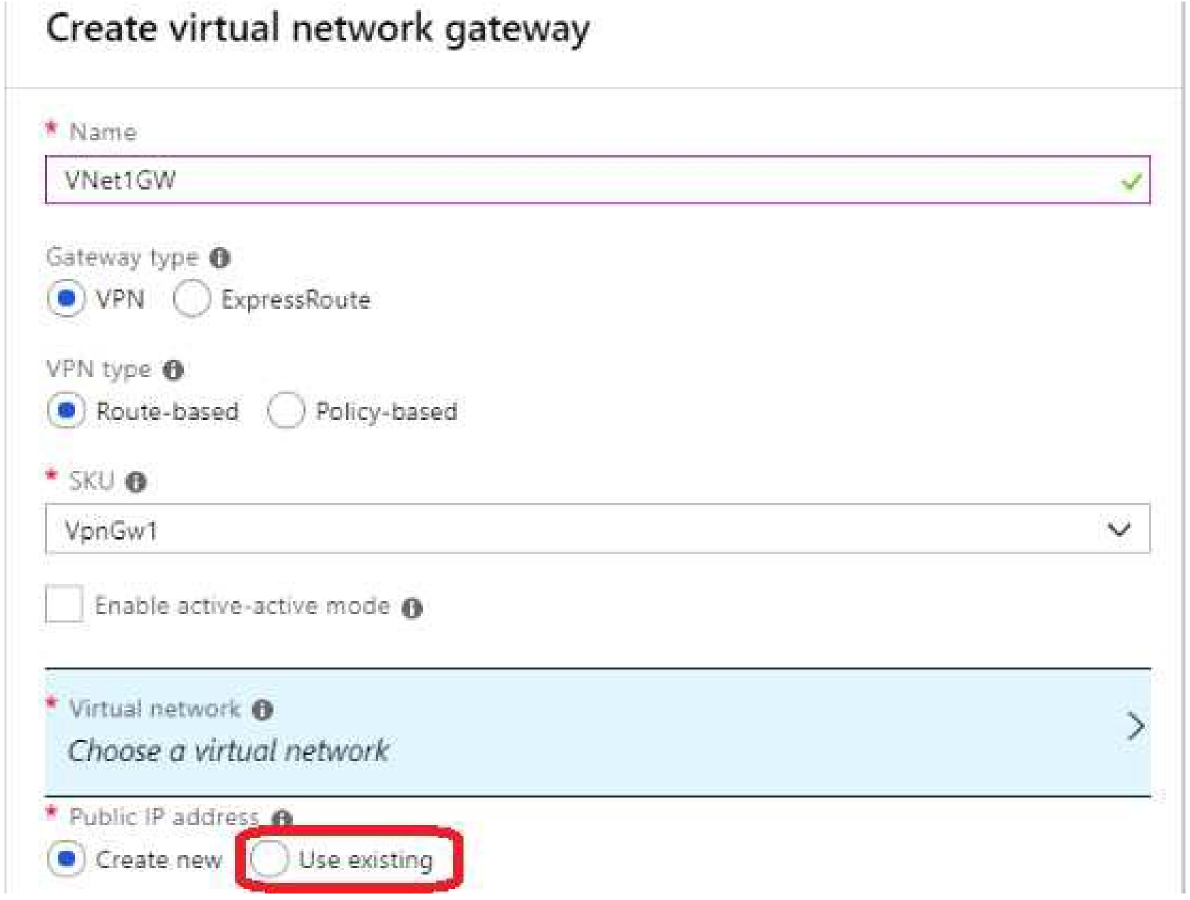
References:
https://docs.microsoft.com/en-us/azure/load-balancer/quickstart-create-basic-load-balancer-portal

NEW QUESTION 23

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.

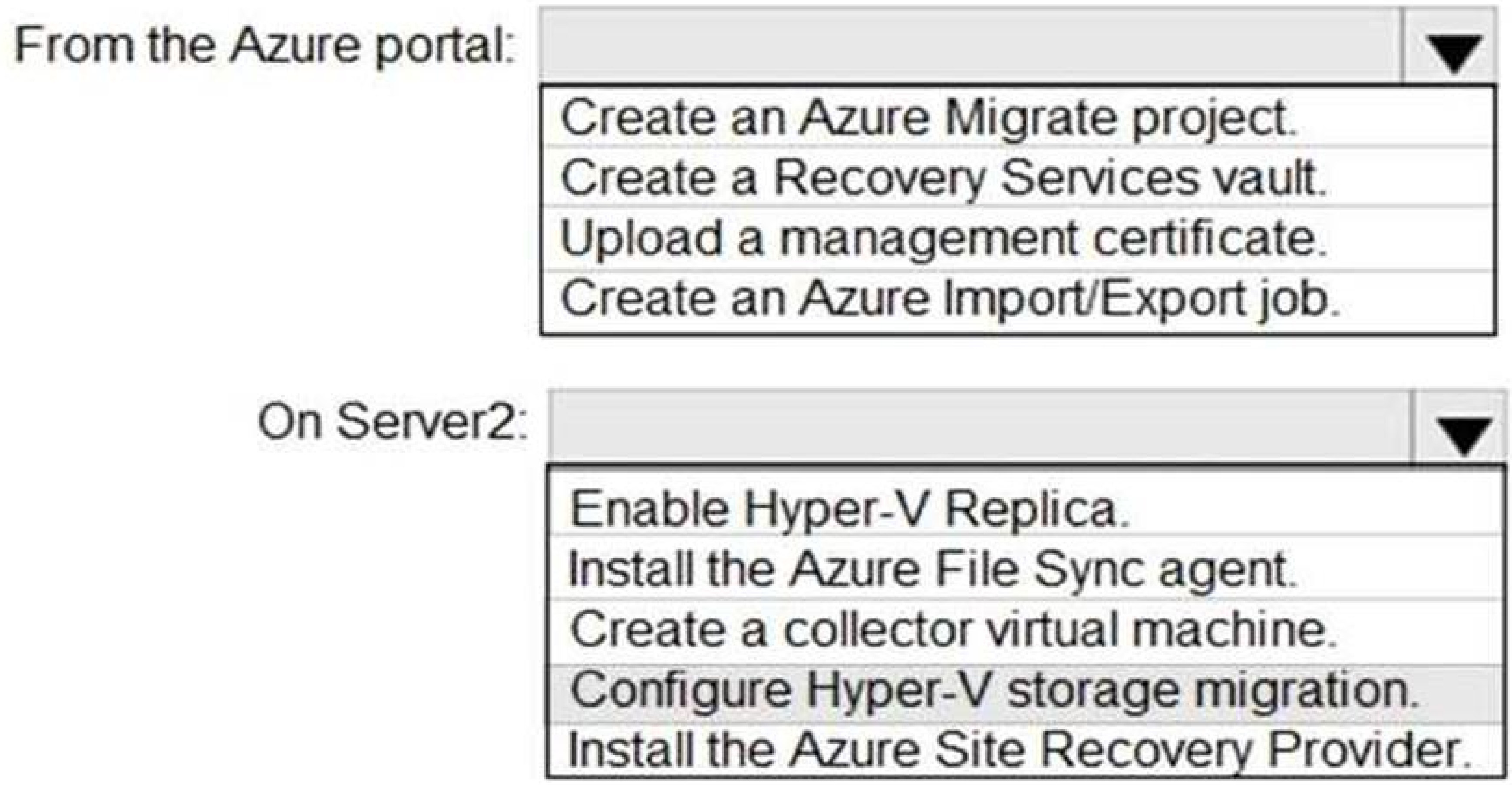
NEW QUESTION 25
You discover that VM3 does NOT meet the technical requirements. You need to verify whether the issue relates to the NSGs.
What should you use?

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 29
HOTSPOT
You need to prepare the environment to implement the planned changes for Server2.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



From the Azure portal:
- Create an Azure Migrate project.
- Create a Recovery Services vault.
- Upload a management certificate.
- Create an Azure Import/Export job.

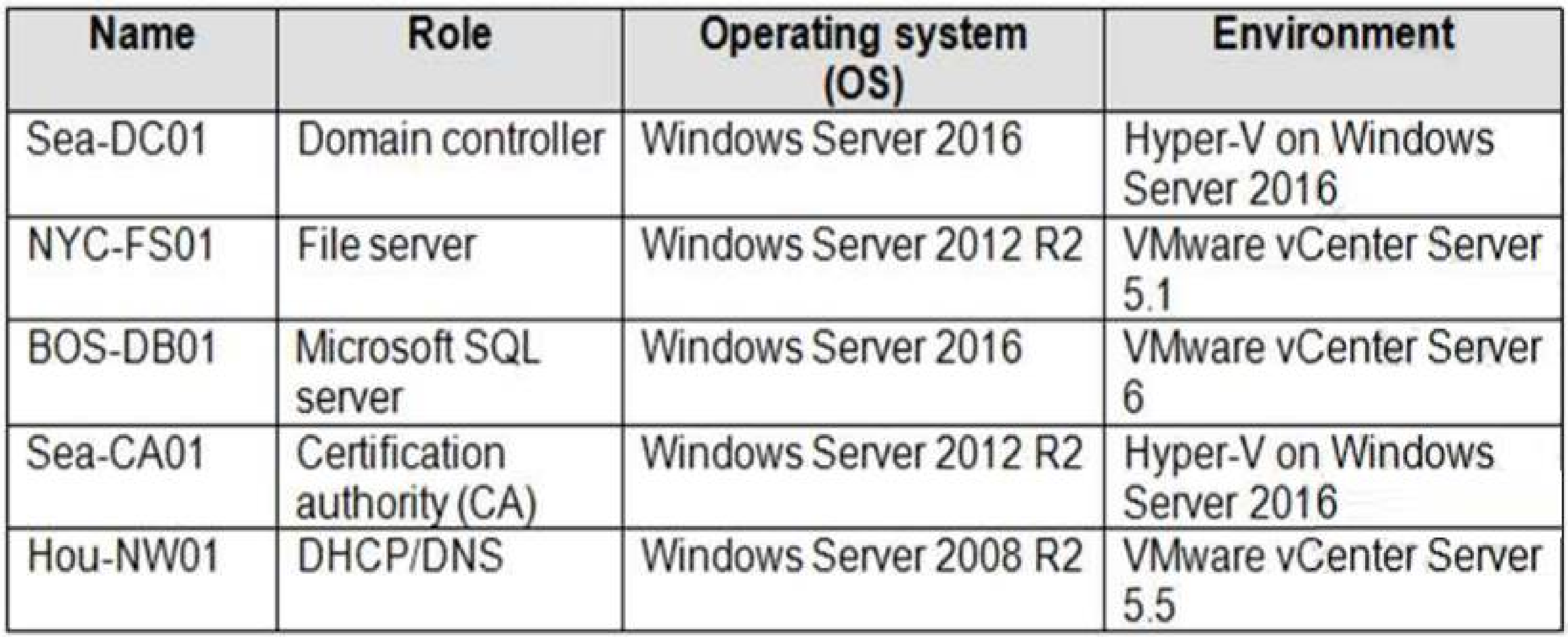
On Server2:
- Enable Hyper-V Replica.
- Install the Azure File Sync agent.
- Create a collector virtual machine.
- Configure Hyper-V storage migration.
- Install the Azure Site Recovery Provider.

Answer:

Explanation: Box 1: Create a Recovery Services vault
Create a Recovery Services vault on the Azure Portal. Box 2: Install the Azure Site Recovery Provider
Azure Site Recovery can be used to manage migration of on-premises machines to Azure. Scenario: Migrate the virtual machines hosted on Server1 and Server2 to Azure.
Server2 has the Hyper-V host role. References:
https://docs.microsoft.com/en-us/azure/site-recovery/migrate-tutorial-on-premises-azure

Case Study: 5
Mix Questions Set C (Evaluate and perform server migration to Azure)

NEW QUESTION 31
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.



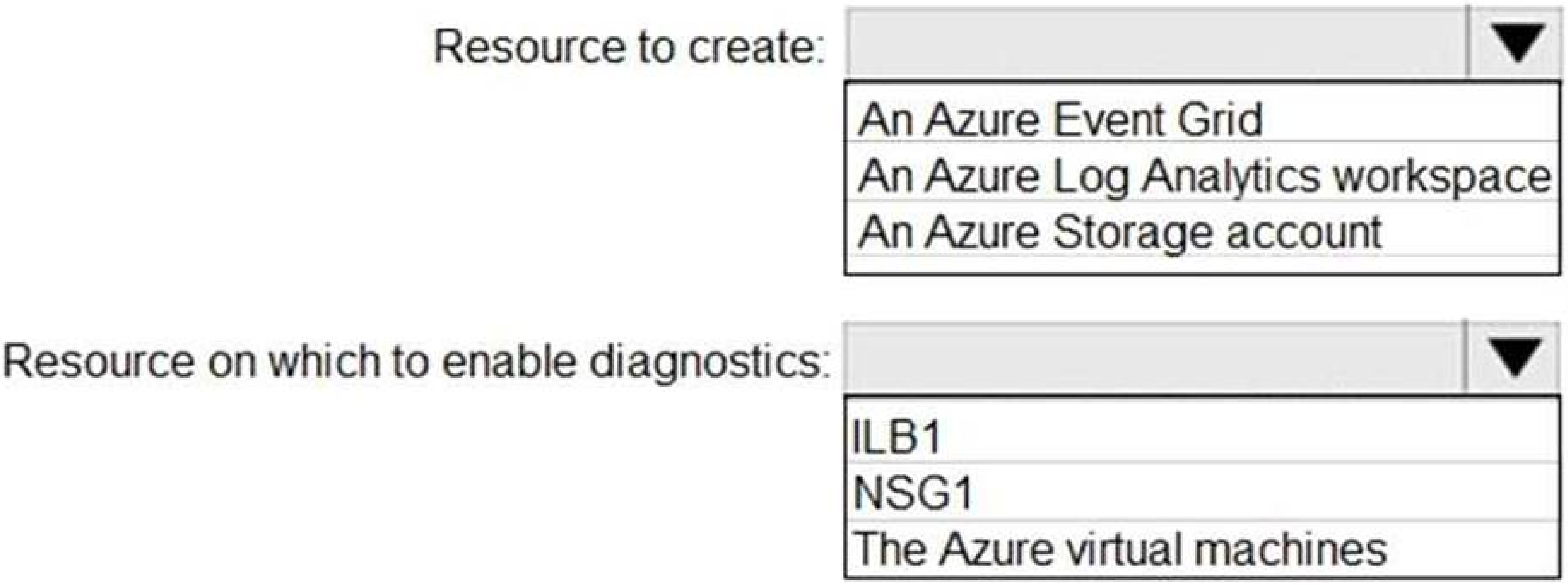
Name	Role	Operating system (OS)	Environment
Sea-DC01	Domain controller	Windows Server 2016	Hyper-V on Windows Server 2016
NYC-FS01	File server	Windows Server 2012 R2	VMware vCenter Server 5.1
BOS-DB01	Microsoft SQL server	Windows Server 2016	VMware vCenter Server 6
Sea-CA01	Certification authority (CA)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

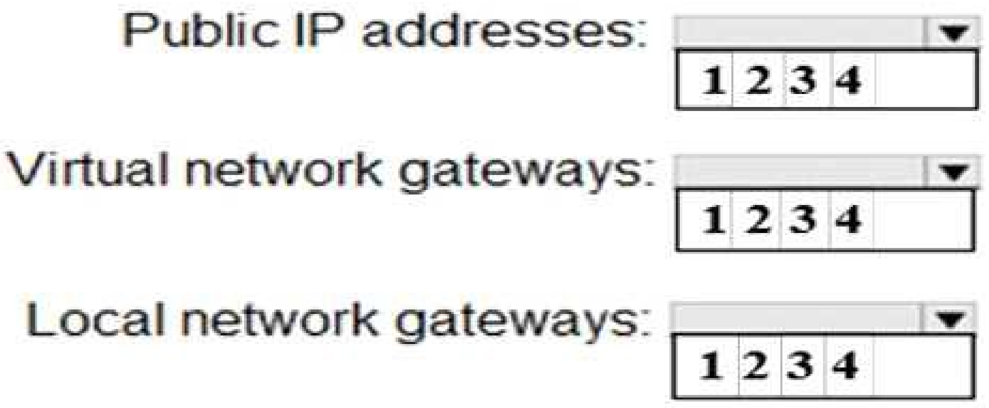
Resource on which to enable diagnostics:
- ILB1
- NSG1
- The Azure virtual machines

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 36
HOTSPOT
You have an on-premises data center and an Azure subscription. The data center contains two VPN devices. The subscription contains an Azure virtual network

named VNet1. VNet1 contains a gateway subnet.
You need to create a site-to-site VPN. The solution must ensure that is a single instance of an Azure VPN gateway fails, or a single on-premises VPN device fails, the failure will not cause an interruption that is longer than two minutes.
What is the minimum number of public IP addresses, virtual network gateways, and local network gateways required in Azure? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



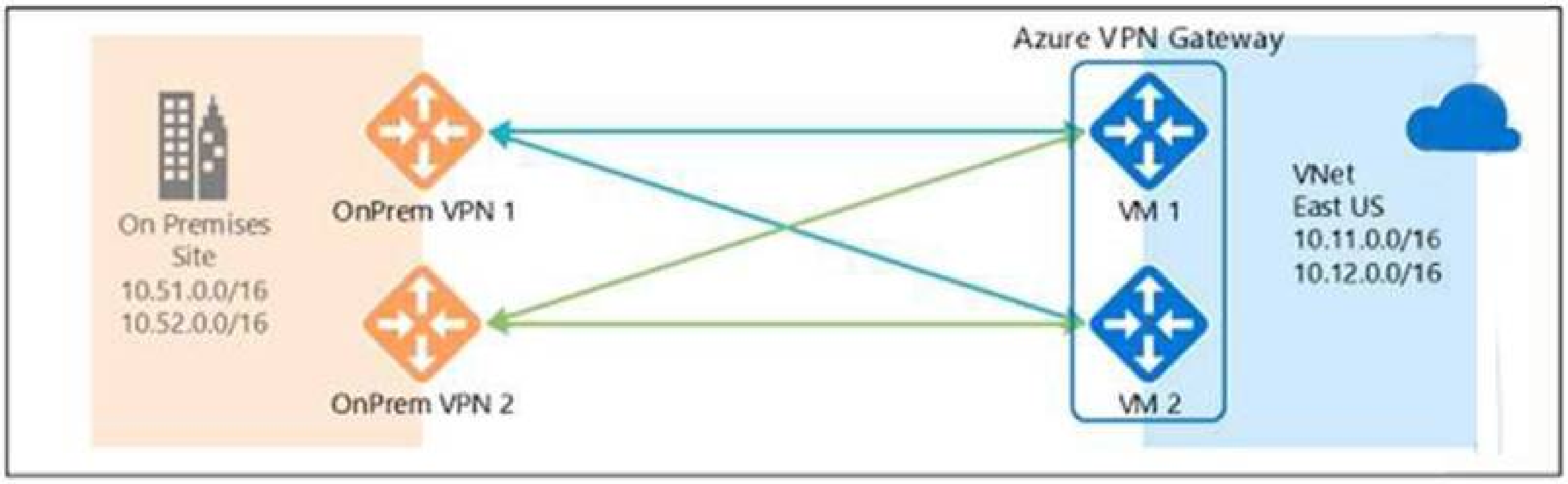
Public IP addresses: 1 2 3 4

Virtual network gateways: 1 2 3 4

Local network gateways: 1 2 3 4

Answer:

Explanation: Box 1: 4
Two public IP addresses in the on-premises data center, and two public IP addresses in the VNET. The most reliable option is to combine the active-active gateways on both your network and Azure, as shown in the diagram below.



Box 2: 2
Every Azure VPN gateway consists of two instances in an active-standby configuration. For any planned maintenance or unplanned disruption that happens to the active instance, the standby instance would take over (failover) automatically, and resume the S2S VPN or VNet-to-VNet connections.
Box 3: 2
Dual-redundancy: active-active VPN gateways for both Azure and on-premises networks References:
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-highlyavailable

NEW QUESTION 39
You have an Azure virtual network named VNet1 that contains a subnet named Subnet1. Subnet1 contains three Azure virtual machines. Each virtual machine has a public IP address.
The virtual machines host several applications that are accessible over port 443 to user on the Internet.
Your on-premises network has a site-to-site VPN connection to VNet1.
You discover that the virtual machines can be accessed by using the Remote Desktop Protocol (RDP) from the Internet and from the on-premises network.
You need to prevent RDP access to the virtual machines from the Internet, unless the RDP connection is established from the on-premises network. The solution must ensure that all the applications can still be accesses by the Internet users.
What should you do?

A. Modify the address space of the local network gateway.
B. Remove the public IP addresses from the virtual machines.
C. Modify the address space of Subnet1.
D. Create a deny rule in a network security group (NSG) that is linked to Subnet1.

Answer: D

Explanation: You can filter network traffic to and from Azure resources in an Azure virtual network with a network security group. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources.
References:
https://docs.microsoft.com/en-us/azure/virtual-network/security-overview

NEW QUESTION 44
You have a public load balancer that balancer ports 80 and 443 across three virtual machines.
You need to direct all the Remote Desktop protocol (RDP) to VM3 only. What should you configure?

A. an inbound NAT rule
B. a load public balancing rule
C. a new public load balancer for VM3
D. a new IP configuration

Answer: A

Explanation: To port forward traffic to a specific port on specific VMs use an inbound network address translation (NAT) rule.
Incorrect Answers:
B: Load-balancing rule to distribute traffic that arrives at frontend to backend pool instances. References:
https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview

NEW QUESTION 46
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/

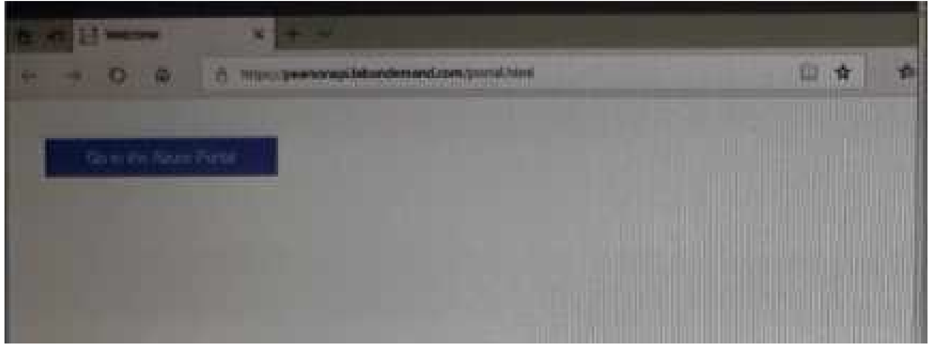
NEW QUESTION 49
You have an Azure subscription that contains a policy-based virtual network gateway named GW1 and a virtual network named VNet1. You need to ensure that you can configure a point-to-site connection from VNet1 to an on-premises computer. Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

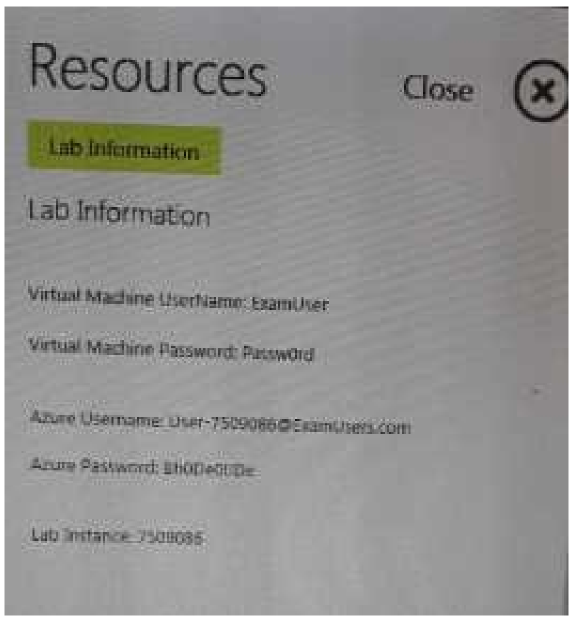
A. Reset GW1.
B. Add a service endpoint to VNet1.
C. Add a connection to GW1.
D. Add a public IP address space to VNet1.
E. Delete GWL
F. Create a route-based virtual network gateway.

Answer: EF

Explanation: E: Policy-based VPN devices use the combinations of prefixes from both networks to define how traffic is encrypted/decrypted through IPsec tunnels. It is typically built on firewall devices that perform packet filtering. IPsec tunnel encryption and decryption are added to the packet filtering and processing engine.
F: A VPN gateway is used when creating a VPN connection to your on-premises network.
Route-based VPN devices use any-to-any (wildcard) traffic selectors, and let routing/forwarding tables direct traffic to different IPsec tunnels. It is typically built on router platforms where each IPsec tunnel is modeled as a network interface or VTI (virtual tunnel interface).
Incorrect Answers:
D: Point-to-Site connections do not require a VPN device or a public-facing IP address. References:
https://docs.microsoft.com/en-us/azure/vpn-gateway/create-routebased-vpn-gateway-portal https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-connect-multiple-policybased-rm- ps

Case Study: 7
Lab 2
Overview
This is a lab or performance-based testing (PBT) section.
The following section of the exam is a lab. In this section, you will perform a set of tasks m a live environment. While most liable to you as it would be m a live environment, some functionality (e g, copy and paste, ability to having sites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the lab9s0 and all other sections of the
exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab. you will NOT be able to return to the tab.





Resources

Lab Information

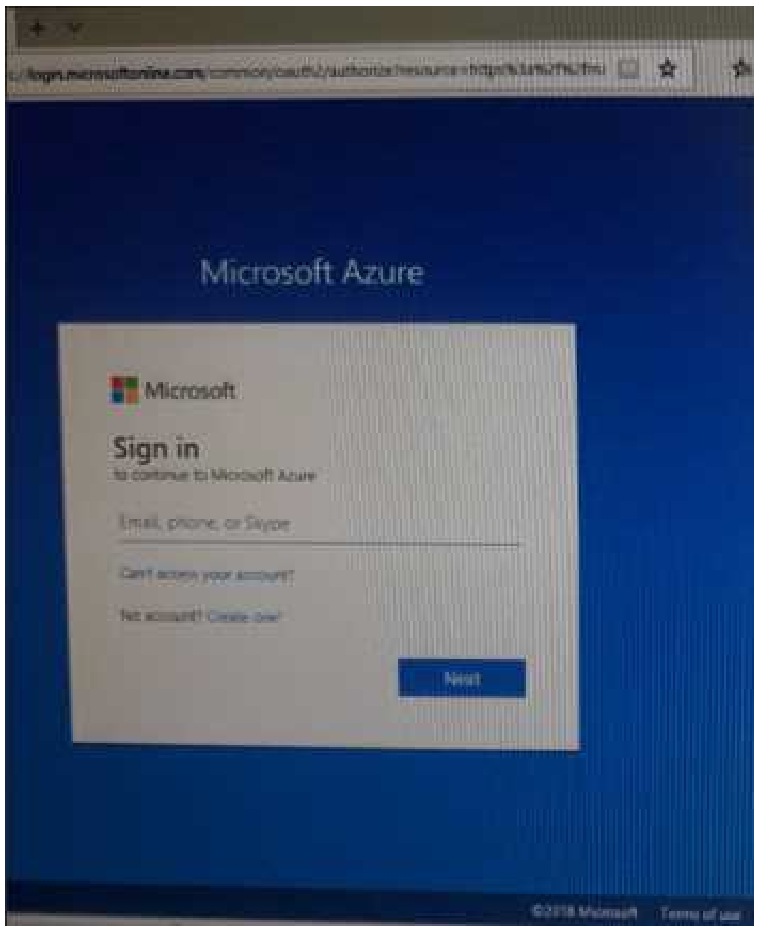
Virtual Machine UserName: ExamUser

Virtual Machine Password: Passw0rd

Azure Username: User-7509086@ExamUsers.com

Azure Password: Bh0De0tDe

Lab Instance: 7509086


login.microsoftonline.com/common/oauth2/authorize?resource=https%3a%2f%2fmi
Microsoft Azure
Microsoft
Sign in
to continue to Microsoft Azure
Email, phone, or Skype
Can't access your account?
No account? Create one!
Next
©2018 Microsoft
Terms of use

To connect to Azure portal, type https://portal.azure.com in te browser address bar.

NEW QUESTION 52
You need to create a web app named corp7509086n2 that can be scaled horizontally. The solution must use the lowest possible pricing tier for the App Service plan.
What should you do from the Azure portal?

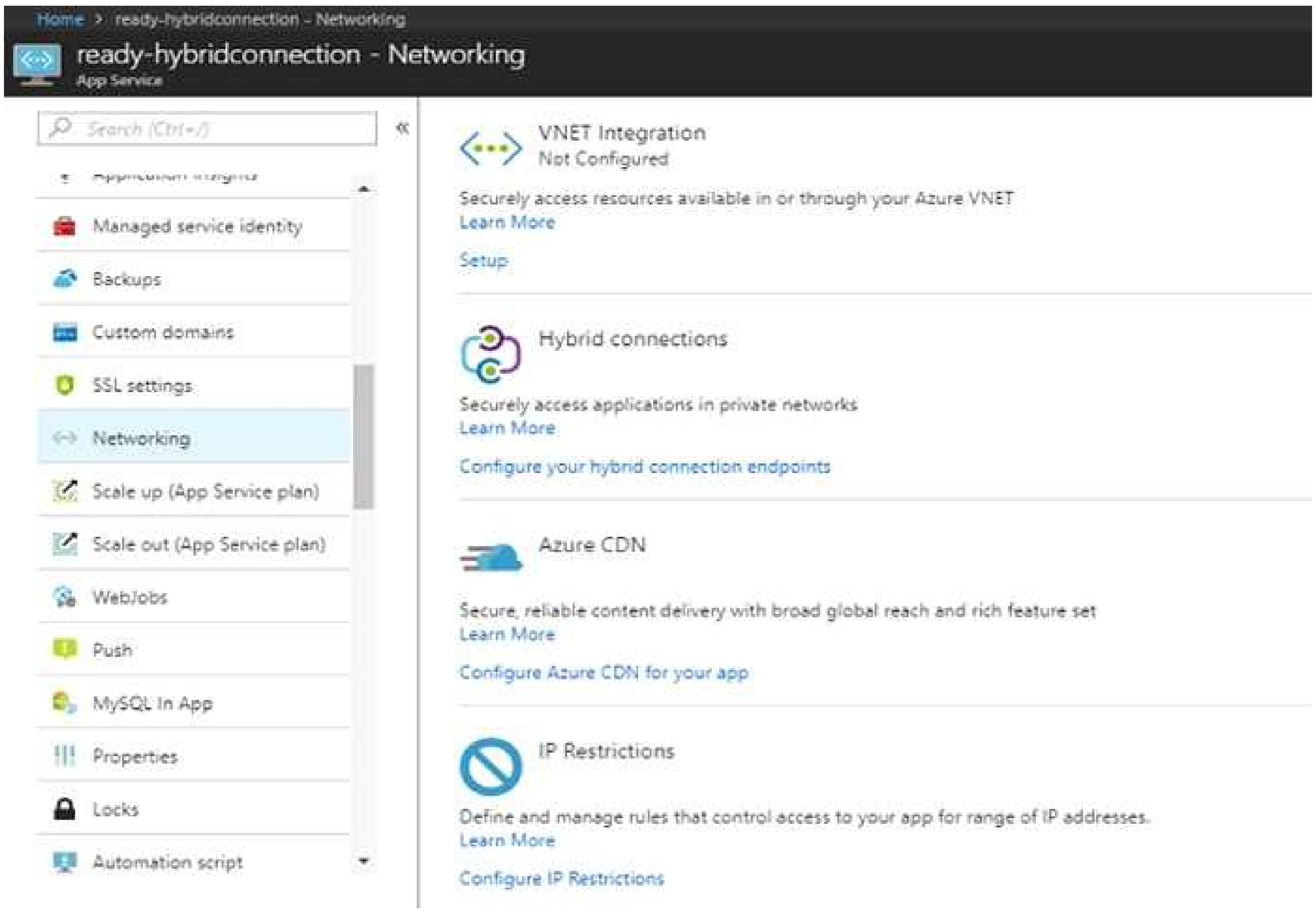
Answer:

Explanation: Step 1:
In the Azure Portal, click Create a resource > Web + Mobile > Web App. Step 2:
Use the Webb app settings as listed below. Web App name: corp7509086n2
Hosting plan: Azure App Service plan Pricing tier of the Pricing Tier: Standard
Change your hosting plan to Standard, you can't setup auto-scaling below standard tier.
Step 3:
Select Create to provision and deploy the Web app.
References:
https://docs.microsoft.com/en-us/azure/app-service/environment/app-service-web-how-to-create-a- web-app-in-an-ase
https://azure.microsoft.com/en-us/pricing/details/app-service/plans/

NEW QUESTION 57
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

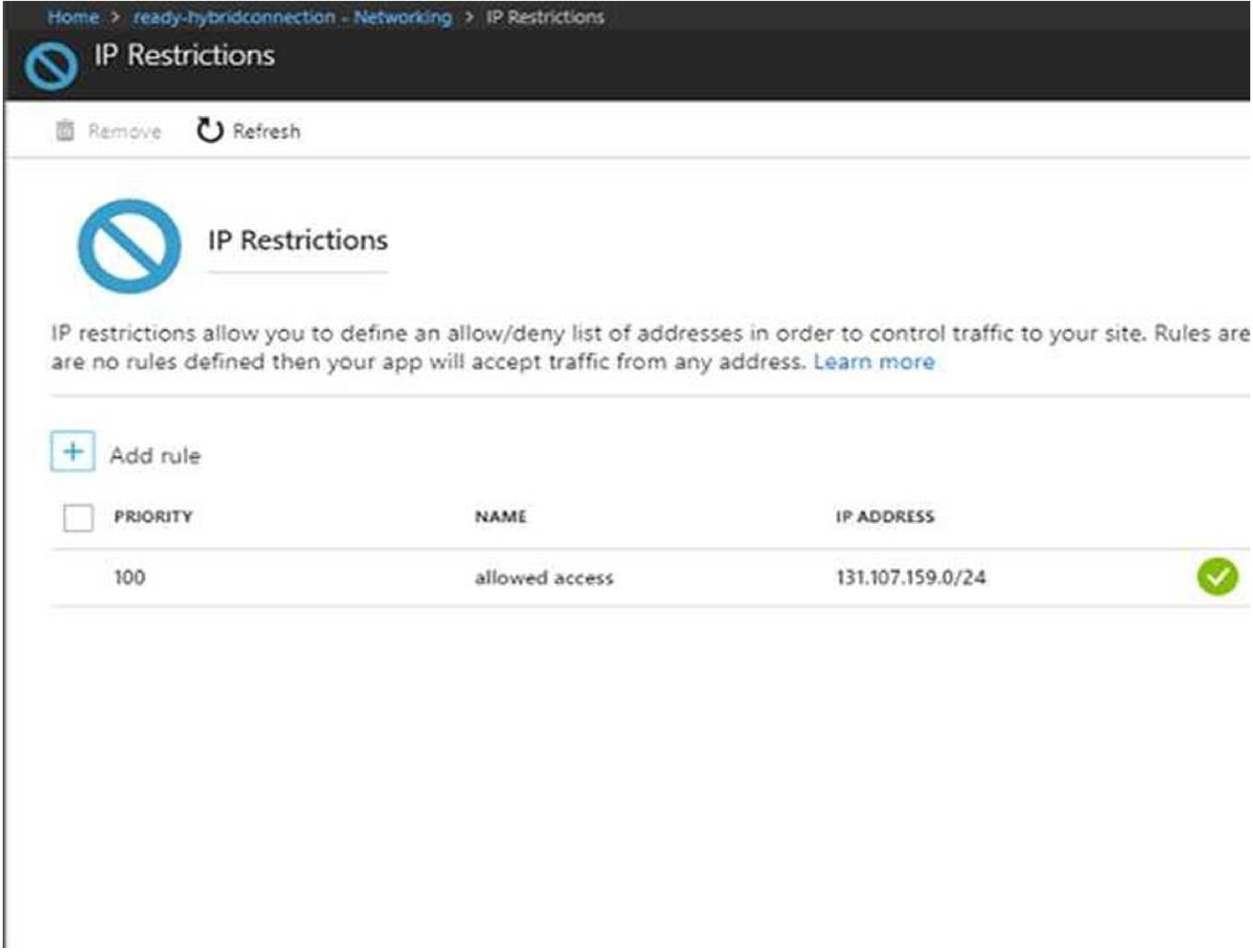
Configure Azure CDN for your app

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.

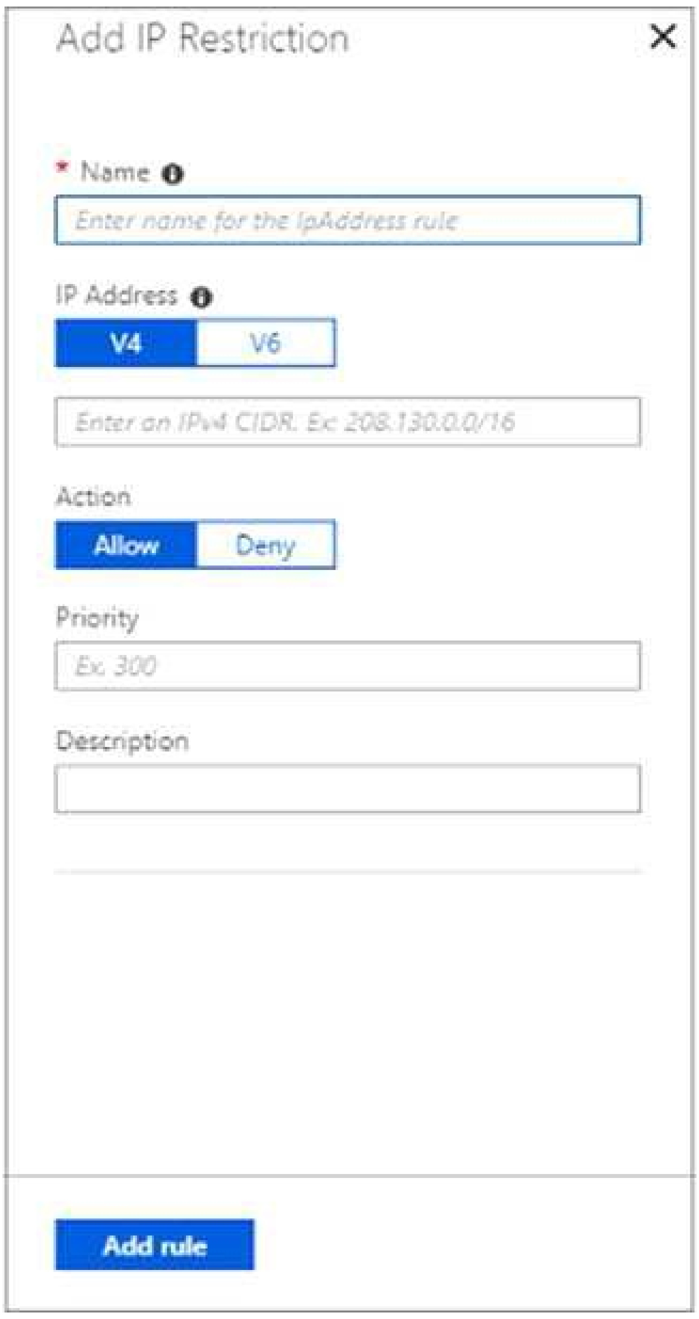


Home > ready-hybridconnection - Networking > IP Restrictions
IP Restrictions
Remove
Refresh
IP Restrictions

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

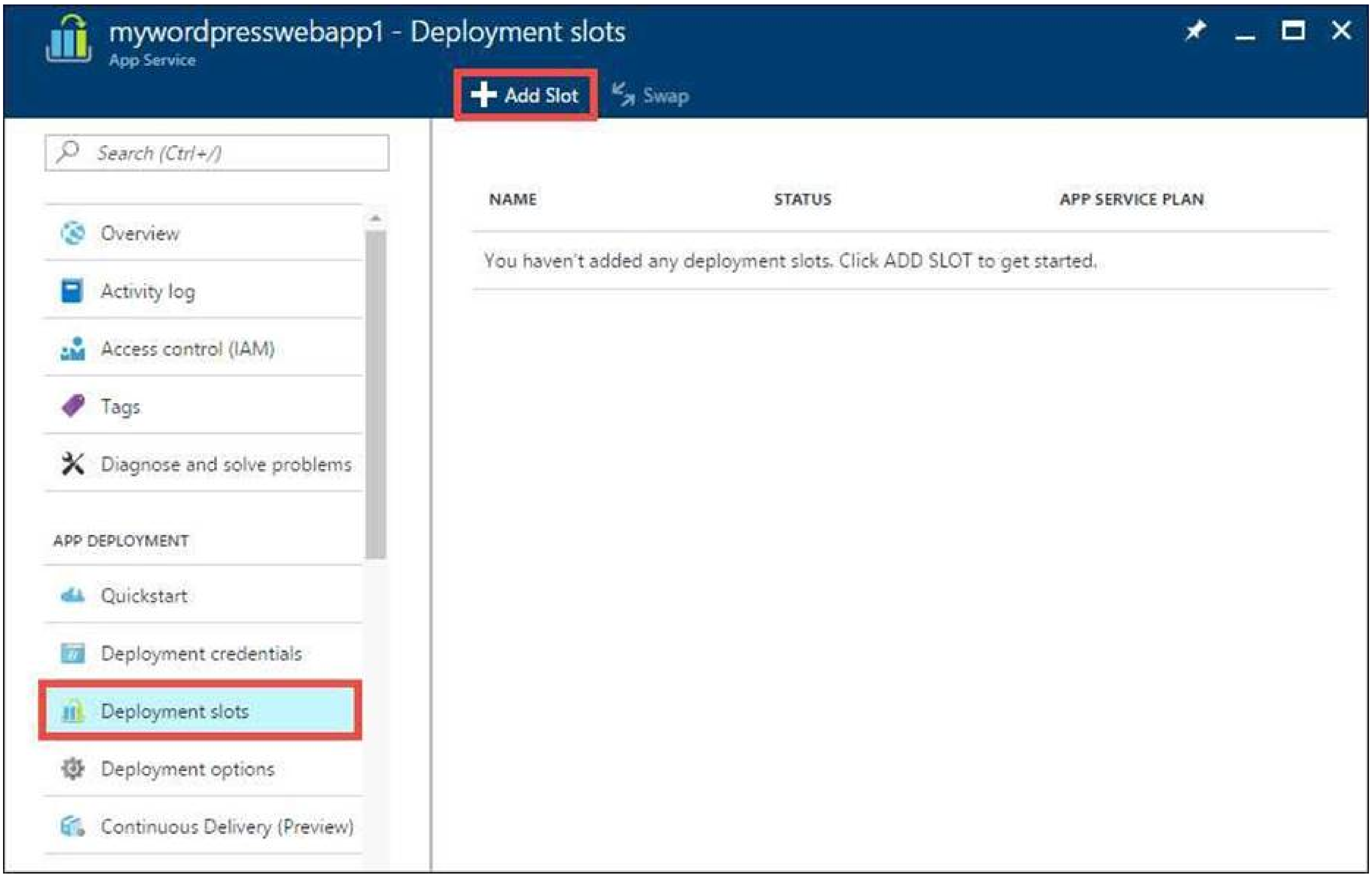
Description

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

NEW QUESTION 59
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.



mywordpresswebapp1 - Deployment slots
App Service

NAME	STATUS	APP SERVICE PLAN

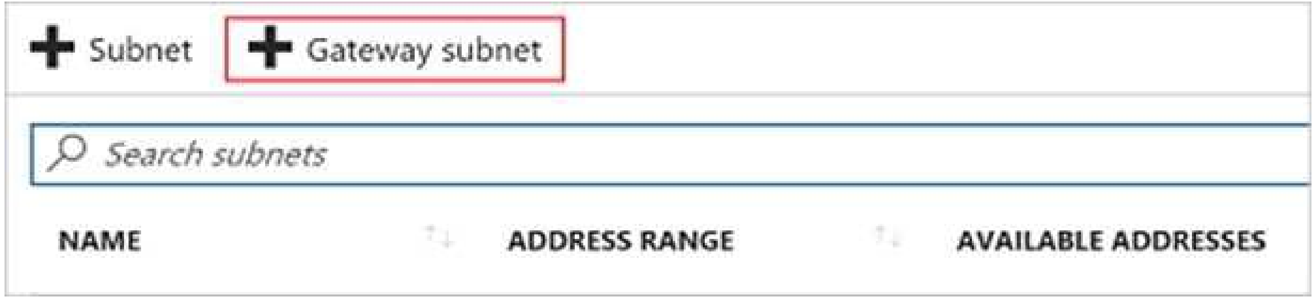
You haven't added any deployment slots. Click ADD SLOT to get started.

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 60
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.



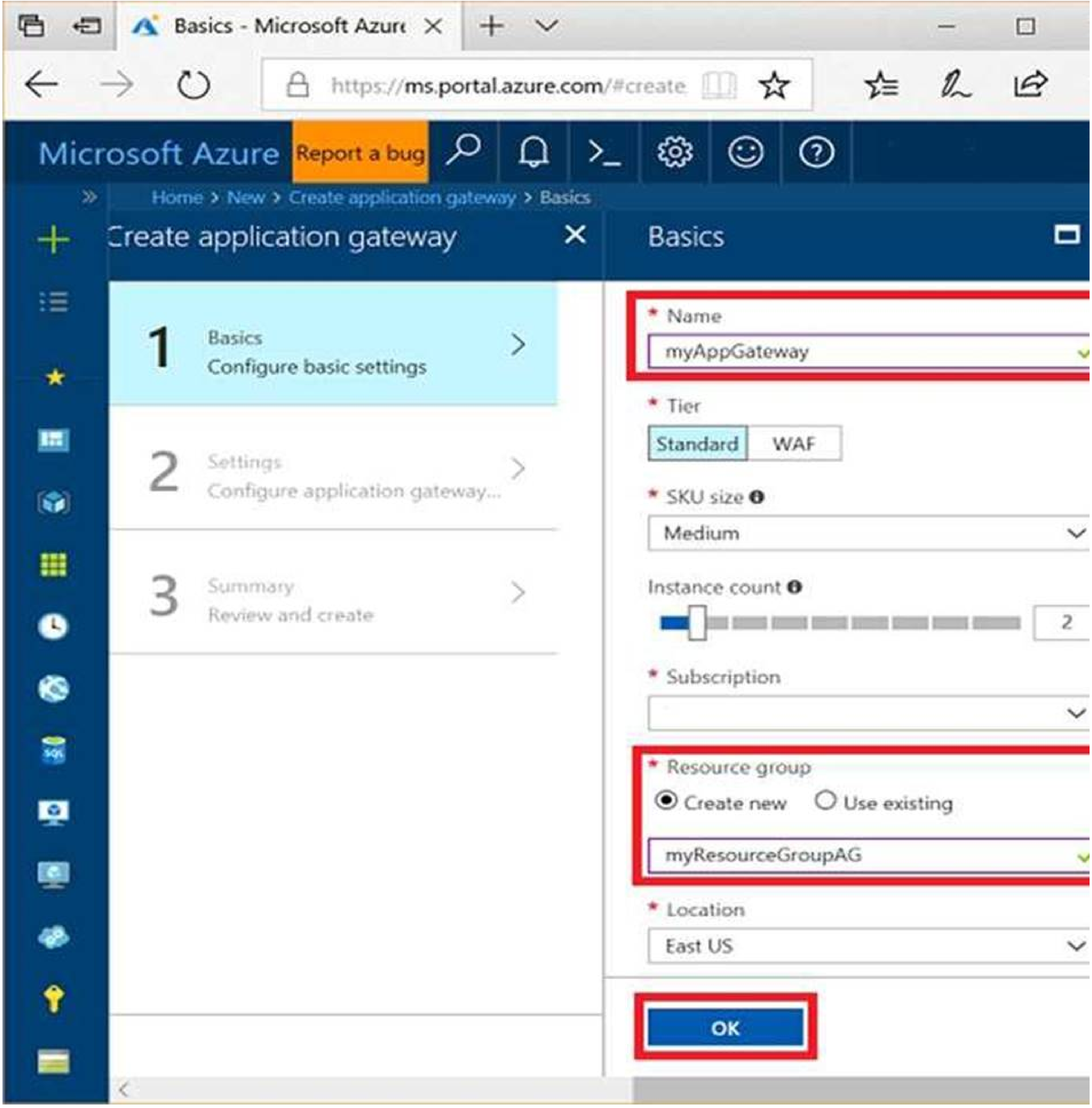
NAME	ADDRESS RANGE	AVAILABLE ADDRESSES

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 61
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
Create application gateway
1 Basics
Configure basic settings
2 Settings
Configure application gateway...
3 Summary
Review and create
Basics
OK

* Name: myAppGateway

* Tier: Standard WAF

* SKU size: Medium

Instance count: 2

* Subscription:

* Resource group: ● Create new ○ Use existing

myResourceGroupAG

* Location: East US

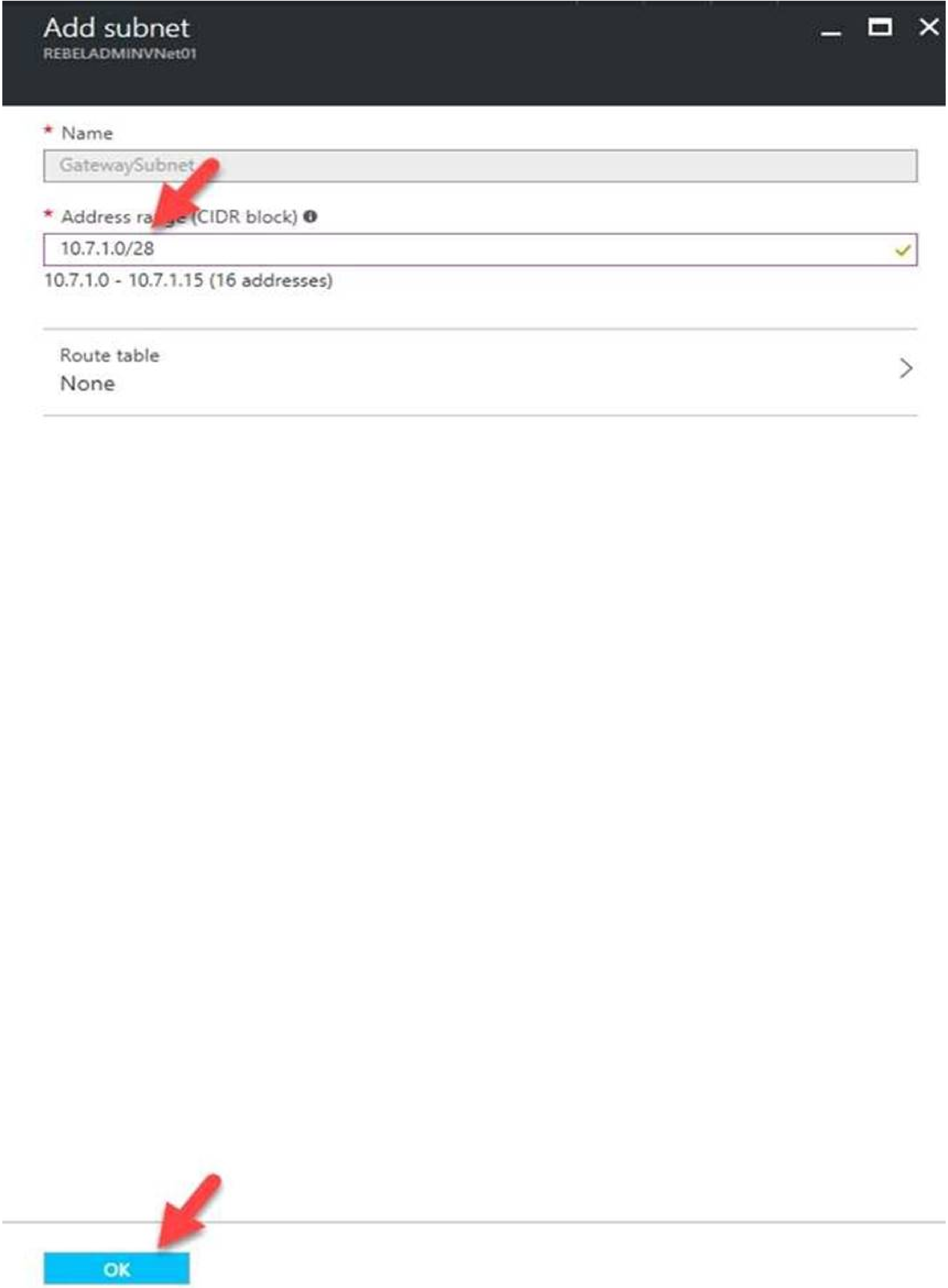
Step 4:
Accept the default values for the other settings and then click OK.
Step 5:
Click Choose a virtual network, and select subnet0. References:
https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-create-gateway- portal

NEW QUESTION 62
You plan to connect a virtual network named VNET1017 to your on-premises network by using both an Azure ExpressRoute and a site-to-site VPN connection.
You need to prepare the Azure environment for the planned deployment. The solution must maximize the IP address space available to Azure virtual machines.
What should you do from the Azure portal before you create the ExpressRoute are the VPN gateway?

Answer:

Explanation: We need to create a Gateway subnet Step 1:

Go to More Services > Virtual Networks Step 2:
Then click on the VNET1017, and click on subnets. Then click on gateway subnet.
Step 3:
In the next window define the subnet for the gateway and click OK



Add subnet
REBELADMINVNet01

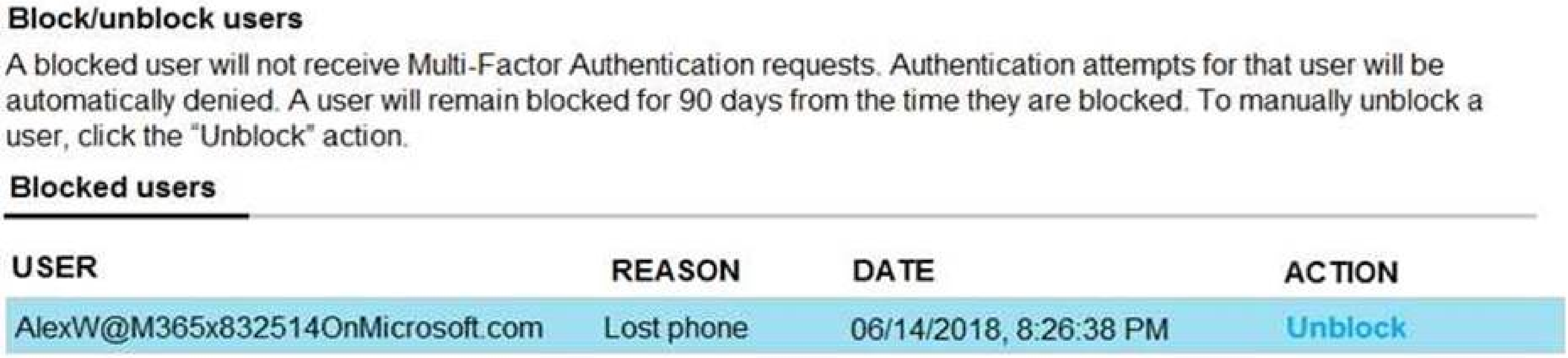
* Name
GatewaySubnet

* Address range (CIDR block)
10.7.1.0/28
10.7.1.0 - 10.7.1.15 (16 addresses)

Route table
None

It is recommended to use /28 or /27 for gateway subnet.
As we want to maximize the IP address space we should use /27. References:
https://blogs.technet.microsoft.com/canitpro/2017/06/28/step-by-step-configuring-a-site-to-site-vpn- gateway-between-azure-and-on-premise/

NEW QUESTION 65
From the MFA Server blade, you open the Block/unblock users blade as shown in the exhibit.



Block/unblock users

A blocked user will not receive Multi-Factor Authentication requests. Authentication attempts for that user will be automatically denied. A user will remain blocked for 90 days from the time they are blocked. To manually unblock a user, click the "Unblock" action.

Blocked users

USER	REASON	DATE	ACTION
AlexW@M365x832514OnMicrosoft.com	Lost phone	06/14/2018, 8:26:38 PM	Unblock

What caused AlexW to be blocked?

A. An administrator manually blocked the user.
B. The user reports a fraud alert when prompted for additional authentication.
C. The user account password expired.
D. The user entered an incorrect PIN four times within 10 minutes.

Answer: B

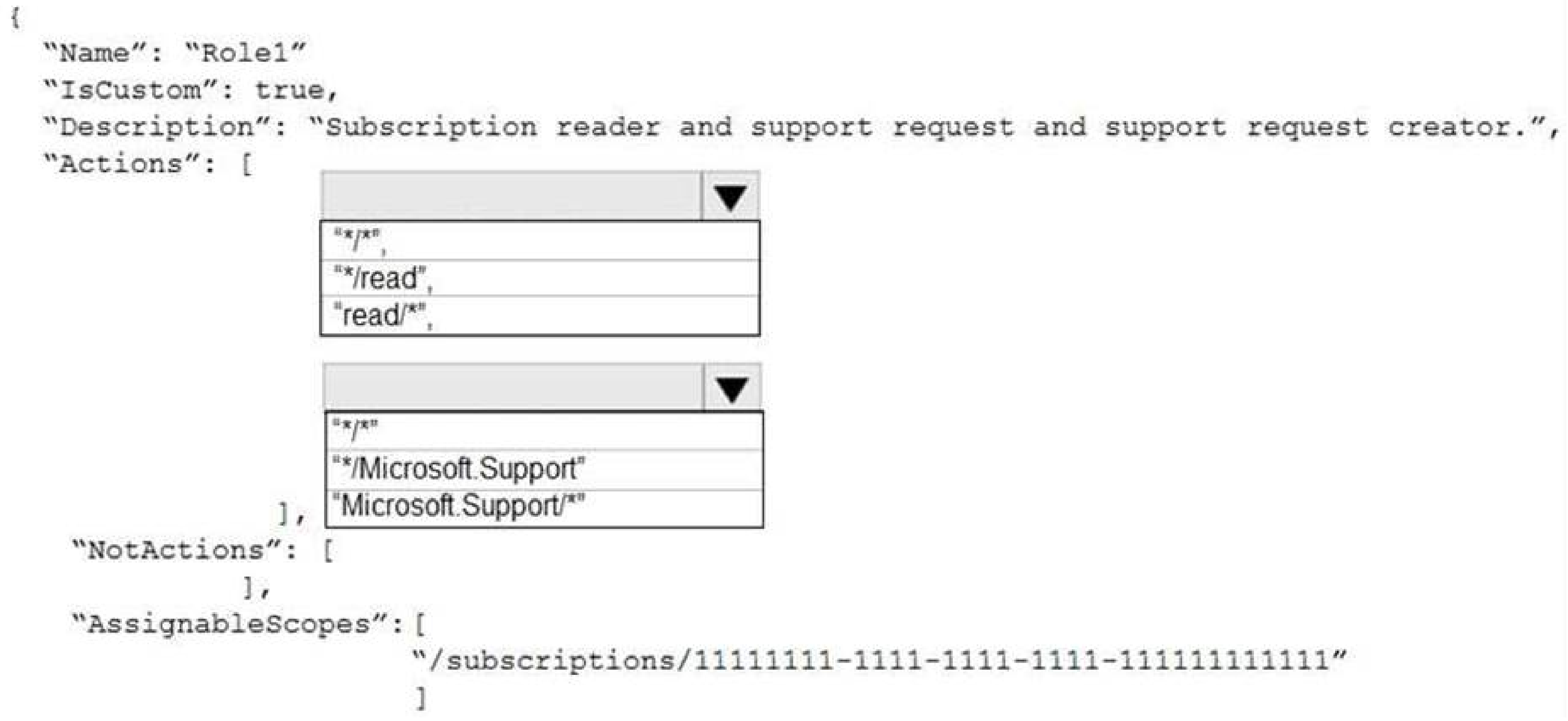
NEW QUESTION 66
You are the global administrator for an Azure Active Directory (Azure AD) tenet named adatum.com. You need to enable two-step verification for Azure users.
What should you do?

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 71
HOTSPOT
You plan to create a new Azure Active Directory (Azure AD) role.
You need to ensure that the new role can view all the resources in the Azure subscription and issue support requests to Microsoft. The solution must use the principle of least privilege.
How should you complete the JSON definition? To answer, select the appropriate options in the answer are
a.
NOTE: Each correct selection is worth one point.



```
{
   "Name": "Role1"
   "IsCustom": true,
   "Description": "Subscription reader and support request and support request creator.",
   "Actions": [
                    ▼
                    "*/*",
                    "*/read",
                    "read/*",

                    ▼
                    "*/*"
                    "*/Microsoft.Support"
                ],  "Microsoft.Support/*"
    "NotActions": [
            ],
    "AssignableScopes": [
                        "/subscriptions/11111111-1111-1111-1111-111111111111"
                        ]
```

Answer:

Explanation: Box 1: "*/read",
/read lets you view everything, but not make any changes. Box 2: " Microsoft.Support/"
The action Microsoft.Support/* enables creating and management of support tickets. References:
https://docs.microsoft.com/en-us/azure/role-based-access-control/tutorial-custom-role-powershell https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

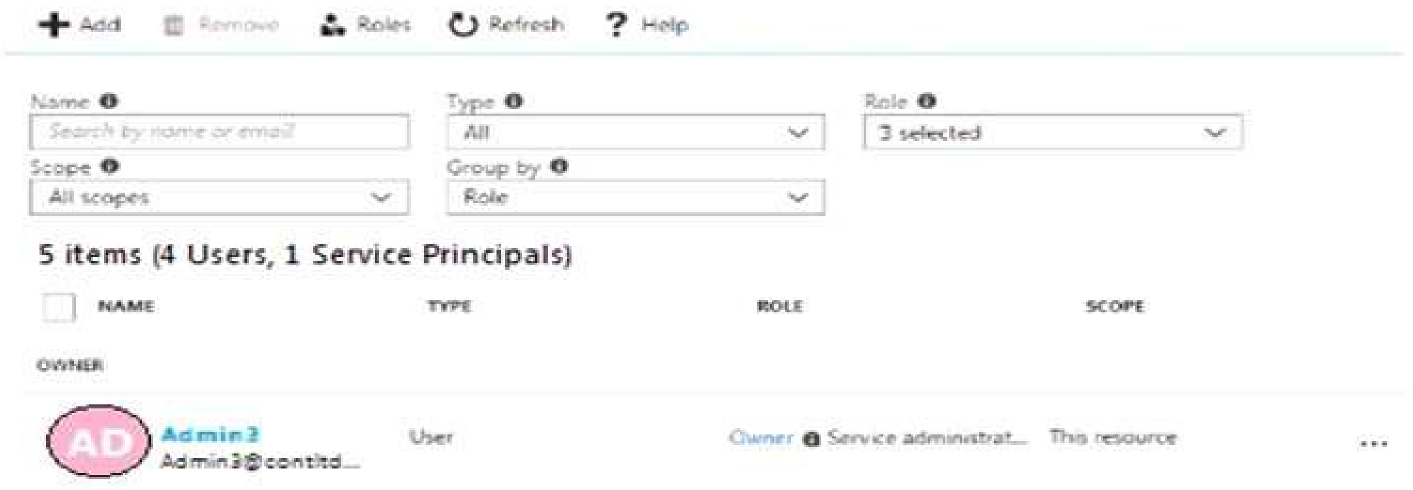
NEW QUESTION 74
You have an Azure Active Directory (Azure AD) tenant named Tenant1 and an Azure subscription named You enable Azure AD Privileged Identity Management.
You need to secure the members of the Lab Creator role. The solution must ensure that the lab creators request access when they create 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 76
HOTSPOT
You have an Azure Active Directory (Azure AD) tenant that contains three global administrators named Admin1, Admin2, and Admin3.
The tenant is associated to an Azure subscription. Access control for the subscription is configured as shown in the Access control exhibit. (Click the Exhibit tab.)

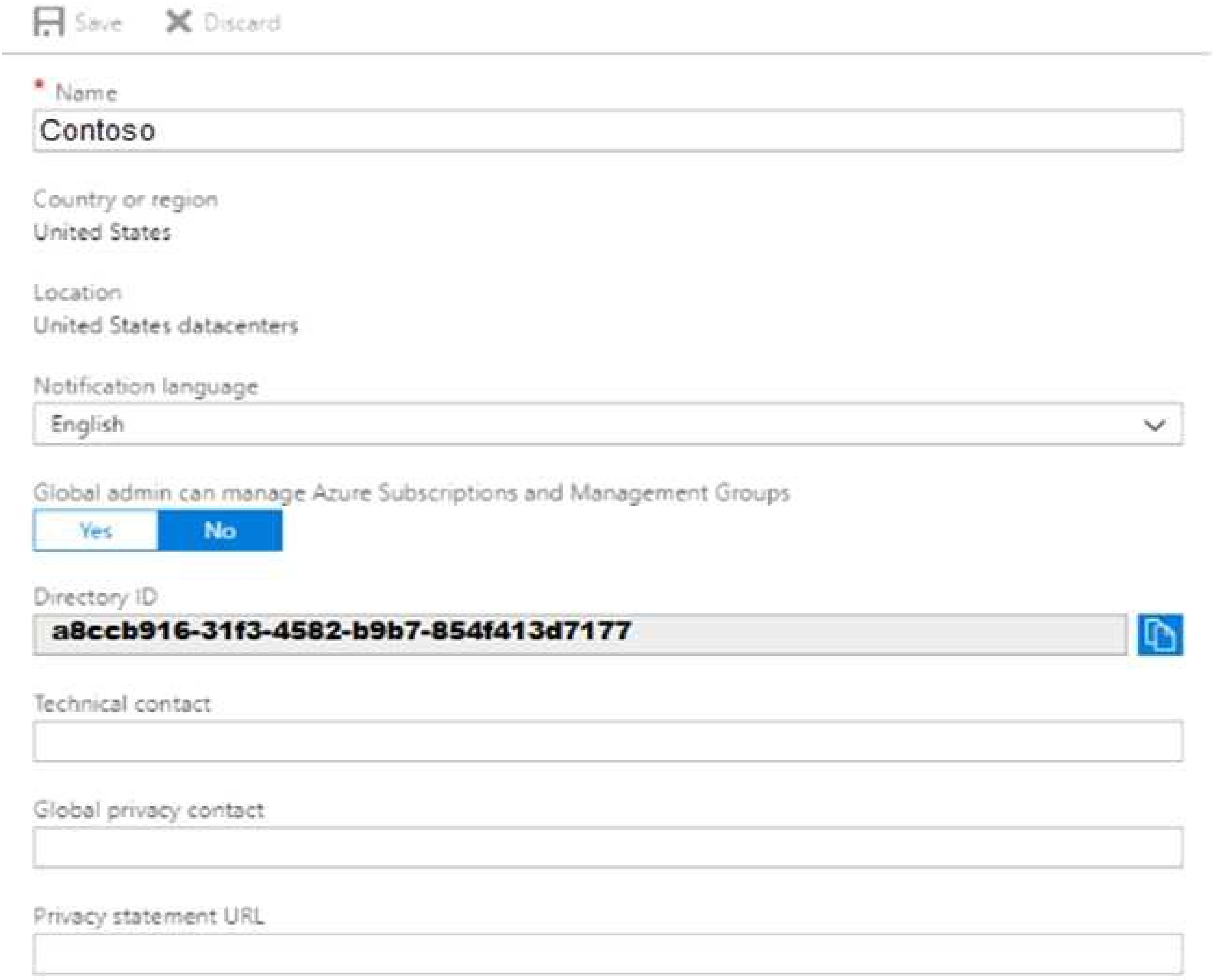


Name: Search by name or email
Type: All
Role: 3 selected
Scope: All scopes
Group by: Role

5 items (4 Users, 1 Service Principals)

NAME	TYPE	ROLE	SCOPE
OWNER			
Admin3 Admin3@contltd...	User	Owner Service administrat...	This resource

You sign in to the Azure portal as Admin1 and configure the tenant as shown in the Tenant exhibit. (Click the Exhibit tab.)



* Name
Contoso

Country or region
United States

Location
United States datacenters

Notification language
English

Global admin can manage Azure Subscriptions and Management Groups
Yes [✓ No]

Directory ID
a8ccb916-31f3-4582-b9b7-854f413d7177

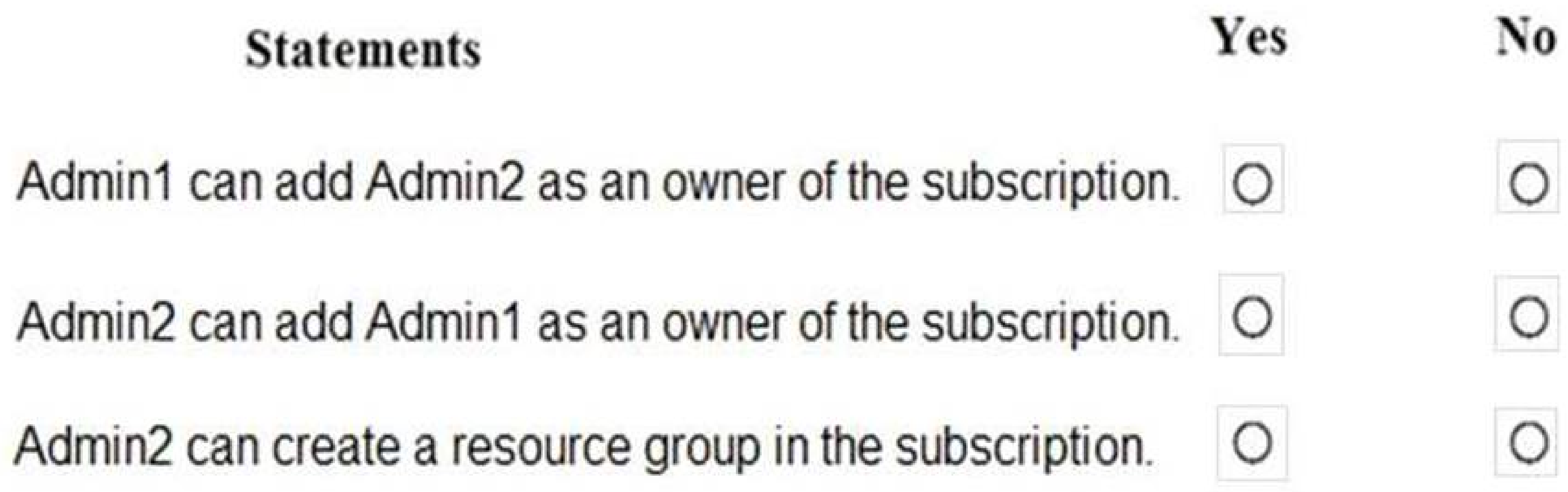
Technical contact

Global privacy contact

Privacy statement URL

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

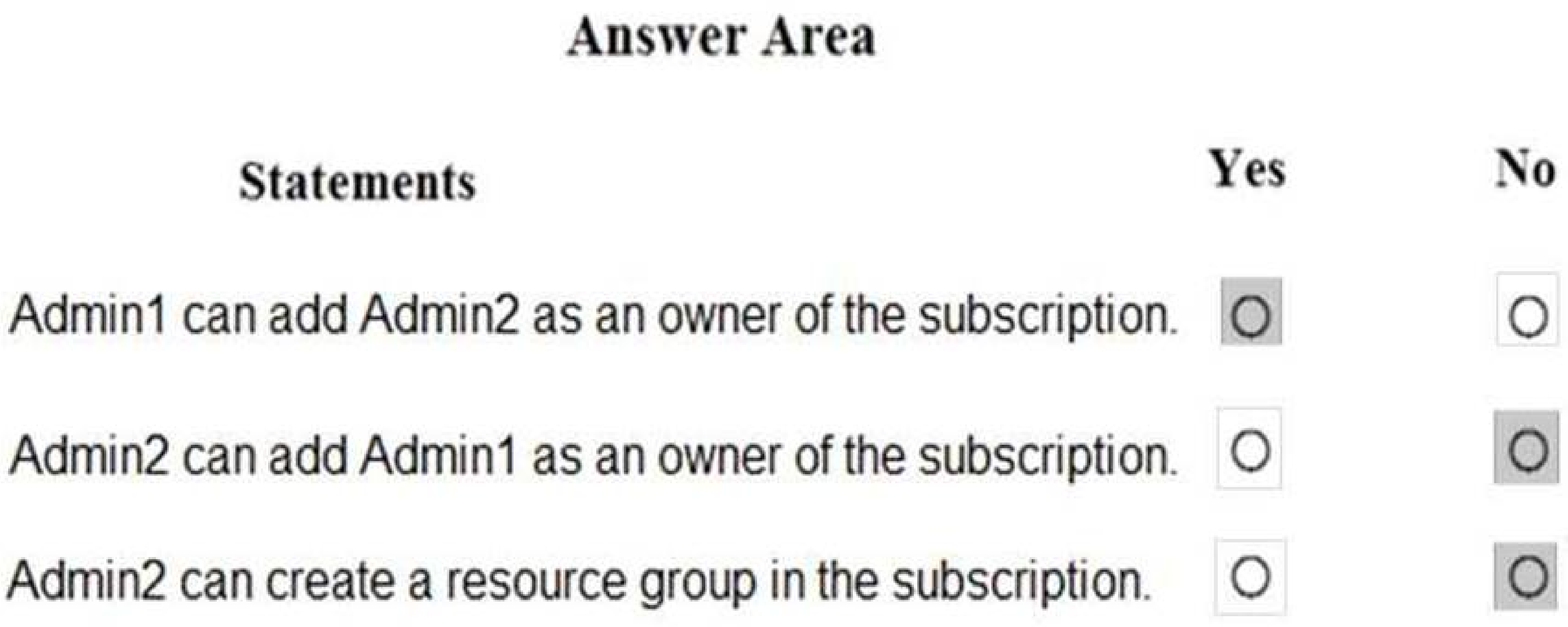
NOTE: Each correct selection is worth one point.



Statements	Yes	No
Admin1 can add Admin2 as an owner of the subscription.	○	○
Admin2 can add Admin1 as an owner of the subscription.	○	○
Admin2 can create a resource group in the subscription.	○	○

Answer:

Explanation:



Answer Area

Statements	Yes	No
Admin1 can add Admin2 as an owner of the subscription.	●	○
Admin2 can add Admin1 as an owner of the subscription.	○	●
Admin2 can create a resource group in the subscription.	○	●

NEW QUESTION 81
You have an Azure subscription.
You enable multi-factor authentication for all users.
Some users report that the email applications on their mobile device cannot co browser and from Microsoft Outlook 2016 on their computer.
You need to ensure that the users can use the email applications on their mobile device. What should you instruct the users to do?
The users can access Exchange Online by using a web

A. Enable self-service password reset.
B. Create an app password.
C. Reset the Azure Active Directory (Azure AD) password.
D. Reinstall the Microsoft Authenticator app.

Answer: A

Explanation: References:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks

NEW QUESTION 86
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 91
......