AZ-700 Q&As

Designing and Implementing Microsoft Azure Networking Solutions

Pass Microsoft AZ-700 Exam with 100% Guarantee

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

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

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

HOTSPOT

You configure a route table named RT1 that has the routes shown in the following table.

Name	Prefix	Next hop type	Next hop IP address
Route1	0.0.0.0/0	Network virtual appliance (NVA)	192.168.0.4
Route2	10.0.0.0/24	Network virtual appliance (NVA)	192.168.0.4

You have an Azure virtual network named Vnet1 that has the subnets shown in the following table.

Name	Prefix	Route table
DMZ	192.168.0.0/24	None
FrontEnd	192.168.1.0/24	RT1
BackEnd	192.168.2.0/24	None

You have the resources shown in the following table.

Name	IP address	Type
NVA1	192.168.0.4	NVA
VM1	192.168.1.4	Virtual machine
VM2	192.168.2.4	Virtual machine

Vnet1 connects to an ExpressRoute circuit. The on-premises router advertises the following routes:

1.

0.0.0.0/0

2.

10.0.0.0/16

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

NOTE: Each correct selection is worth one point.

Hot Area:

Statements	Yes	No
Internet traffic from NVA1 is routed to the on-premises network	○	○
Traffic from VM1 is routed to the on-premises network through NVA1	○	○
Traffic from VM1 is routed to VM2 though NVA1	○	○

Correct Answer:

Statements	Yes	No
Internet traffic from NVA1 is routed to the on-premises network	○	○
Traffic from VM1 is routed to the on-premises network through NVA1	○	○
Traffic from VM1 is routed to VM2 though NVA1	○	○

Box 1: Yes

NVA1 with IP (NVA-network virtual appliance) 192.168.0.4 is on the DMZ subnet. It will use route 10.0.0.0/16 to the on-premises network.

Box 2: No

VM2 has IP address 192.168.2.4 and is on the BackEnd subnet. VM2 will not use the RT1 route table, and will not reach the on-premises network through NVA1.

Box 3: Yes

VM1 with IP address 192.168.1.4 is on the FrontEnd subnet, and will use the RT1 routing table. It will use Route2 and Next Hop IP address 192.168.0.4, IP address of NVA1, to reach VM2.

QUESTION 2

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

Name	In resource group	Location
Vnet1	RG1	West US
Vnet2	RG1	Central US
Vnet3	RG2	Central US
Vnet4	RG2	West US
Vnet5	RG3	East US

You plan to deploy an Azure firewall named AF1 to RG1 in the West US Azure region. To which virtual networks can you deploy AF1?

A. Vnet1 and Vnet4 only

B. Vnet1, Vnet2, Vnet3, and Vnet4

C. Vnet1 only

D. Vnet1 and Vnet2 only

E. Vnet1, Vnet2, and Vnet4 only

Correct Answer: C

Azure Firewall operates in a single VNET.

Azure Firewall is a regional service.

Yes. Vnet1: Same VNET and same region.

No. Vnet2: Same Resource Group but different VNET and different region. Must be in the same region.

No. Vnet3: Different VNET, different region. Must be in the same region.

No. Vnet4: Different VNET, same region.

Reference:

https://docs.microsoft.com/en-us/azure/architecture/networking/guide/well-architected-framework-azure-firewall

QUESTION 3

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

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

To complete this task, sign in to the Azure portal.

A. See explanation below.

B. Placeholder

C. Placeholder

D. Placeholder

Correct Answer: A

You can use a network security group to filter inbound and outbound network traffic to and from Azure resources in an Azure virtual network. Plan Stage 1: Create a network security group

Stage 2: Associate network security group to subnet Stage 3: Create security rule Stage 1: Create a network security group

A network security group (NSG) secures network traffic in your virtual network.

Step 1: From the Azure portal menu, select + Create a resource > Networking > Network security group, or search for Network security group in the portal search box.

Step 2: Select Create.

Step 3: On the Basics tab of Create network security group, enter or select this information:

Details omitted

Step 4: Select the Review + create tab, or select the blue Review + create button at the bottom of the page.

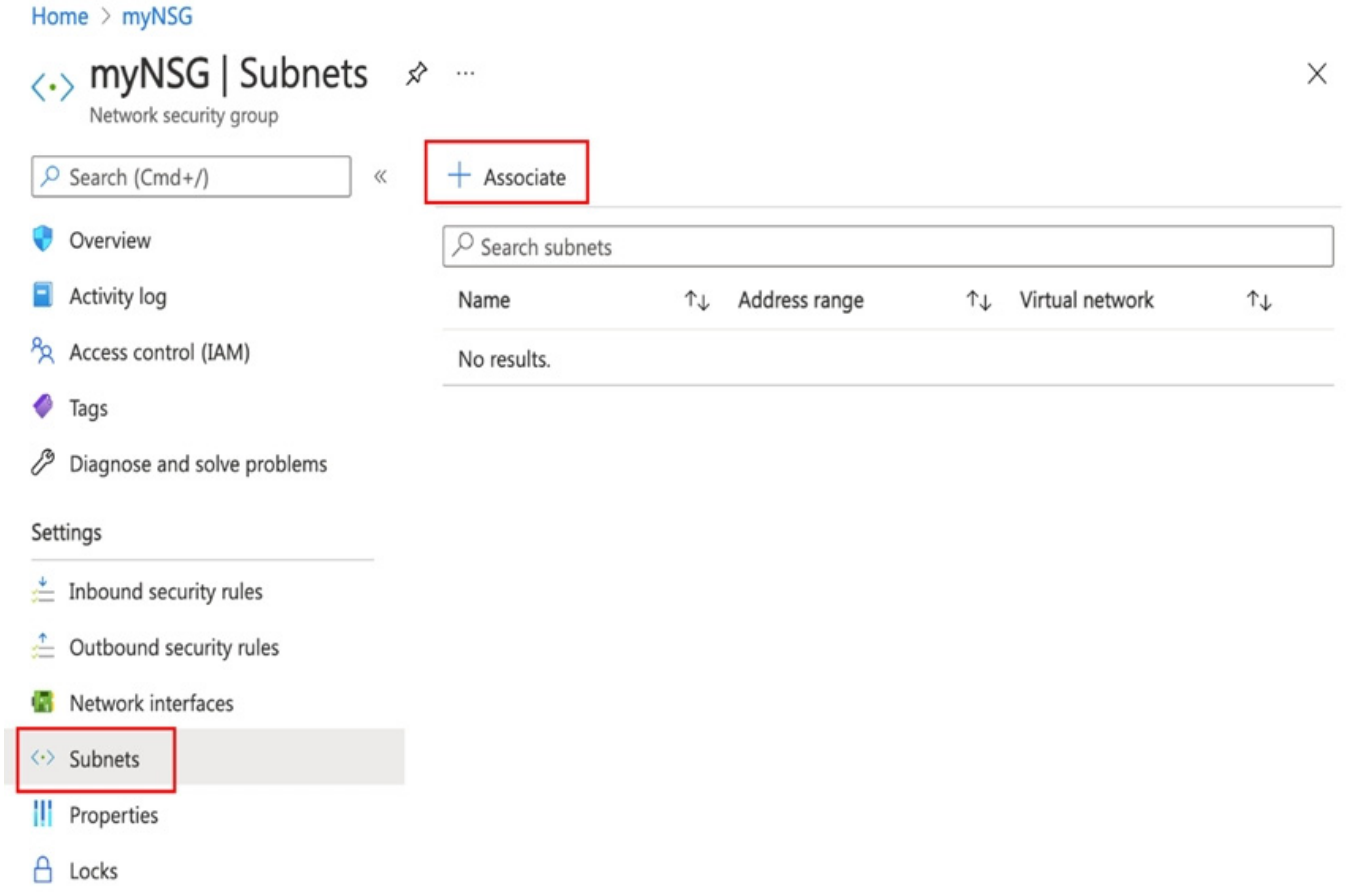
Step 5: Select Create.

Stage 2: Associate network security group to subnet

In this section, you\\'ll associate the network security group with the subnet of the virtual network you created earlier.

Step 6: Search for myNsg (the name you give in stage 1) in the portal search box.

Step 7: Select Subnets from the Settings section of myNSG.



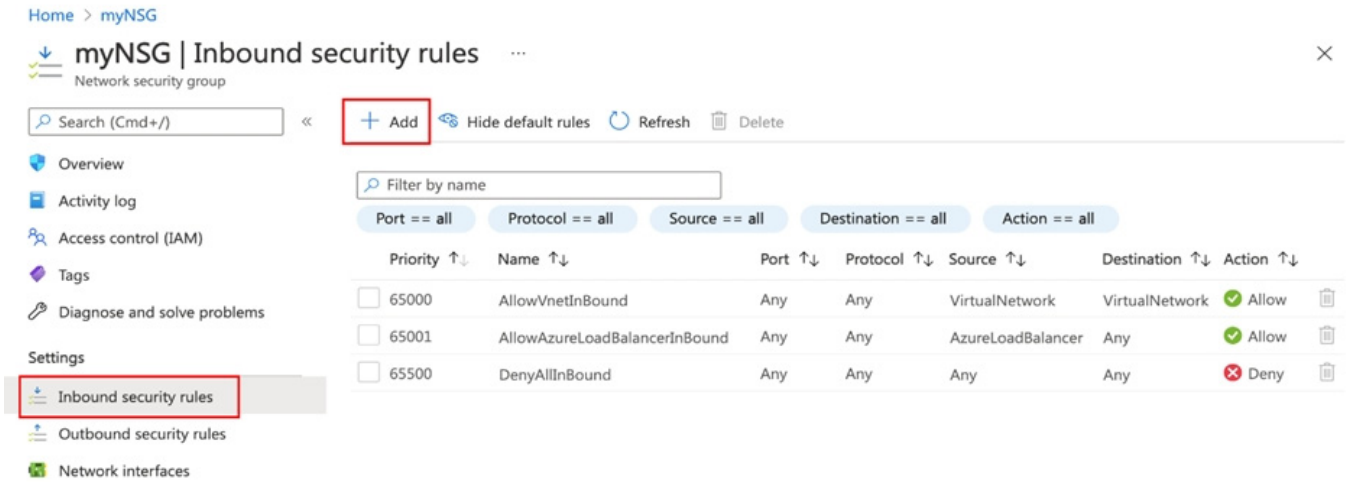
Step 8: In the Subnets page, select + Associate:

Step 9: Under Associate subnet, select myVNet (the virtual network that is available) for Virtual network.

Step 10: Select subnet1-2 for Subnet, and then select OK.

Stage 3: Create security rule

Step 11: Select Inbound security rules from the Settings section of myNSG.



Step 12: In Inbound security rules page, select + Add:

Step 13: Create a security rule that blocks TCP port 5585 to the network security group you created earlier. In Add inbound security rule page, enter or select this information:

(You need to prevent all Azure hosts outside of subnet1-2 from connecting to TCP port 5585 on hosts on subnet1-2.)

Source: Leave the default of Any.

Source port ranges: Leave the default of (*).

Destination: Select Network security group.

Destination Network security groups: Select the network security group you created earlier.

Service: Leave the default of Custom.

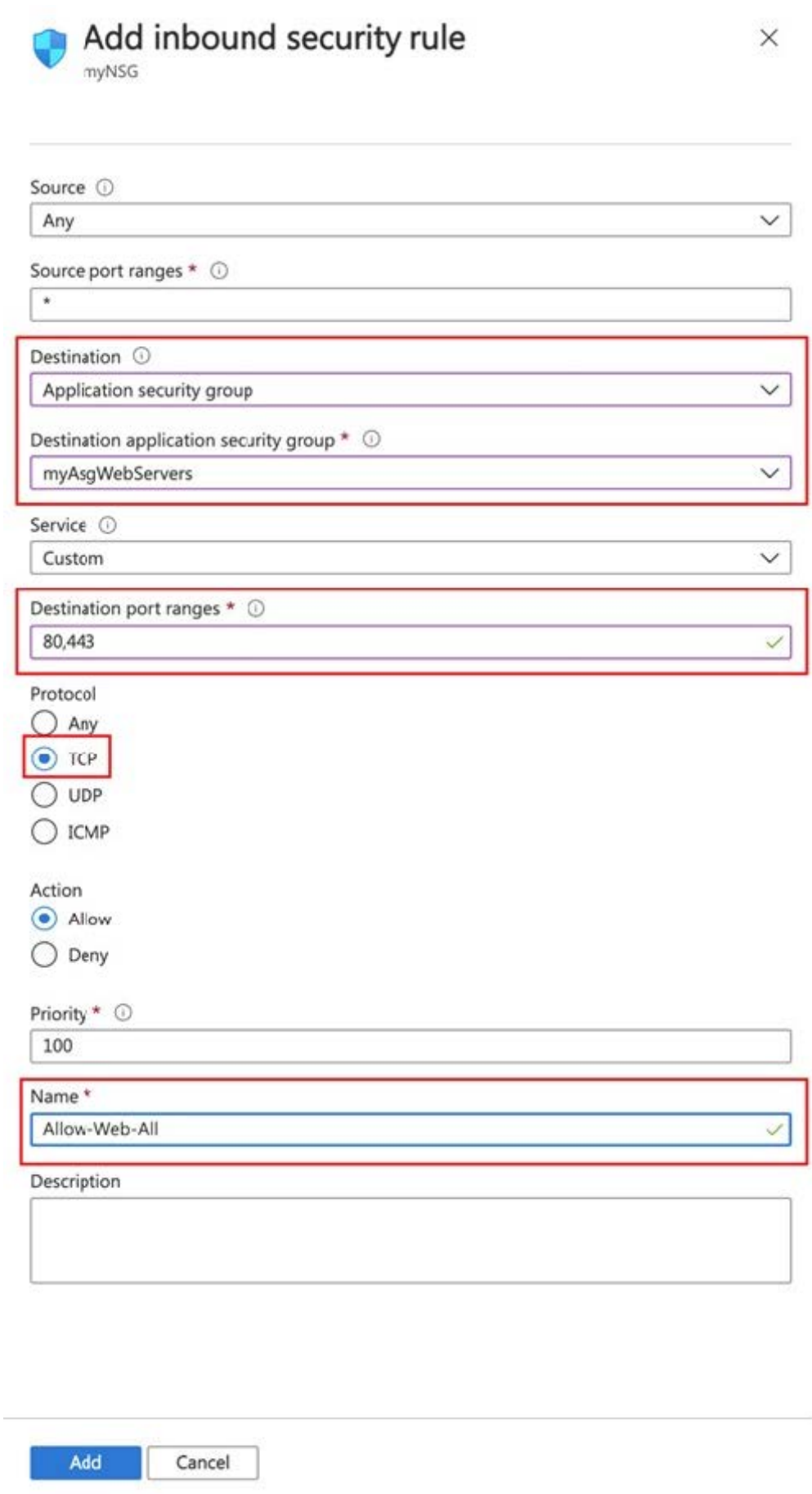
Destination port ranges: Enter 5585

Protocol: Select TCP.

Action: Deny

Priority Leave the default of 100.

Name: Enter something


Add inbound security rule
myNSG
Source
Any
Source port ranges *
*
Destination
Application security group
Destination application security group *
myAsgWebServers
Service
Custom
Destination port ranges *
80,443
Protocol
Any
TCP
UDP
ICMP
Action
Allow
Deny
Priority *
100
Name *
Allow-Web-All
Description
Add
Cancel

Step 14: Select Add.

Reference: https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic

QUESTION 4

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

To complete this task, sign in to the Azure portal.

A. See explanation below.

B. Placeholder

C. Placeholder

D. Placeholder

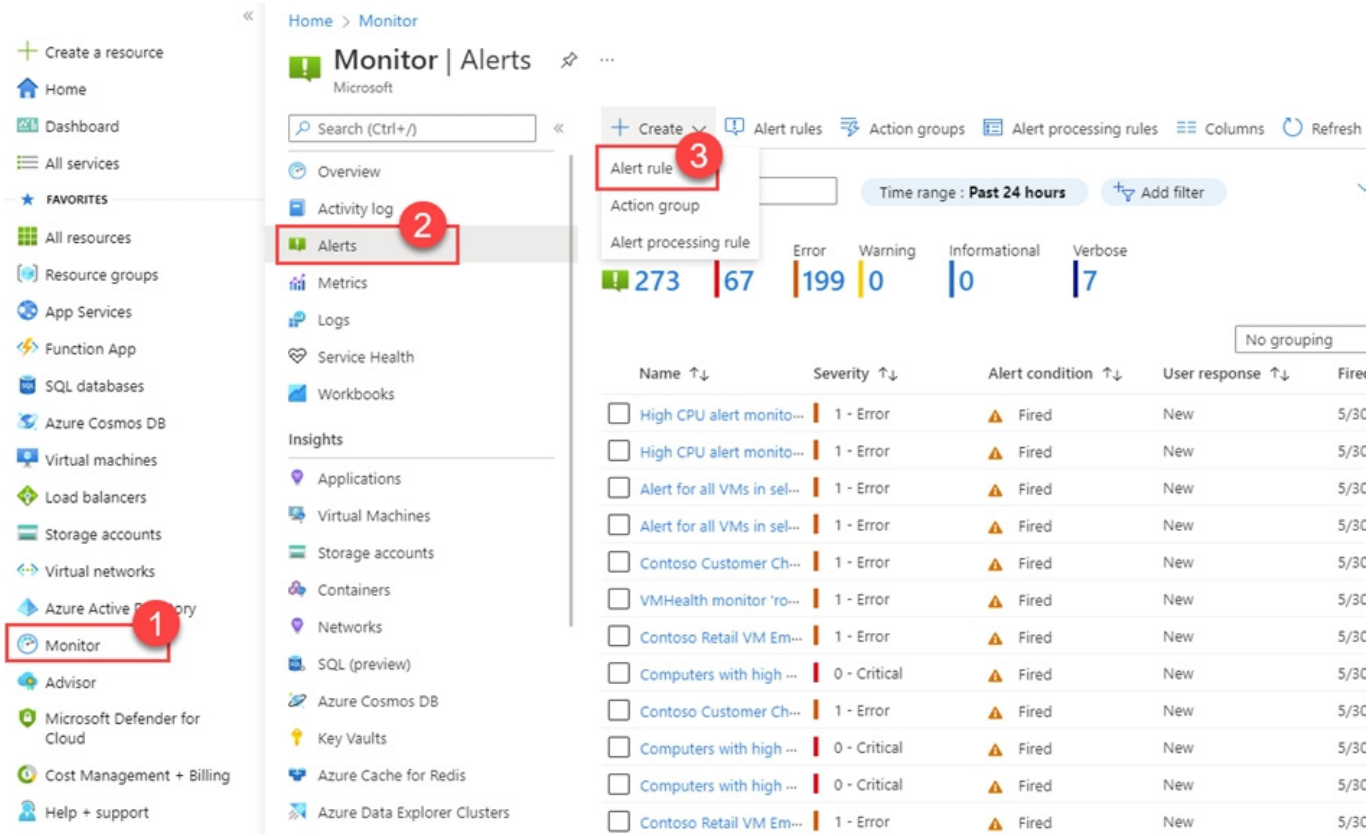
Correct Answer: A

Monitoring Azure virtual network Alerts Azure Monitor alerts proactively notify you when important conditions are found in your monitoring data. They allow you to identify and address issues in your system before your customers notice them. You can set alerts on metrics, logs, and the activity log.

Create a new alert rule in the Azure portal

Step 1: In the portal, select Monitor > Alerts.

Step 2: Open the + Create menu and select Alert rule.



Step 3: On the Select a resource pane, set the scope for your alert rule. You can filter by subscription, resource type, or resource location. We select Virtual Network.

The Available signal types for your selected resources are at the bottom right of the pane.

Step 4: Select Include all future resources to include any future resources added to the selected scope.

Step 5: Select Done.

Step 6: Select Next: Condition at the bottom of the page.

Step 7: On the Select a signal pane, filter the list of signals by using the signal type and monitor service:

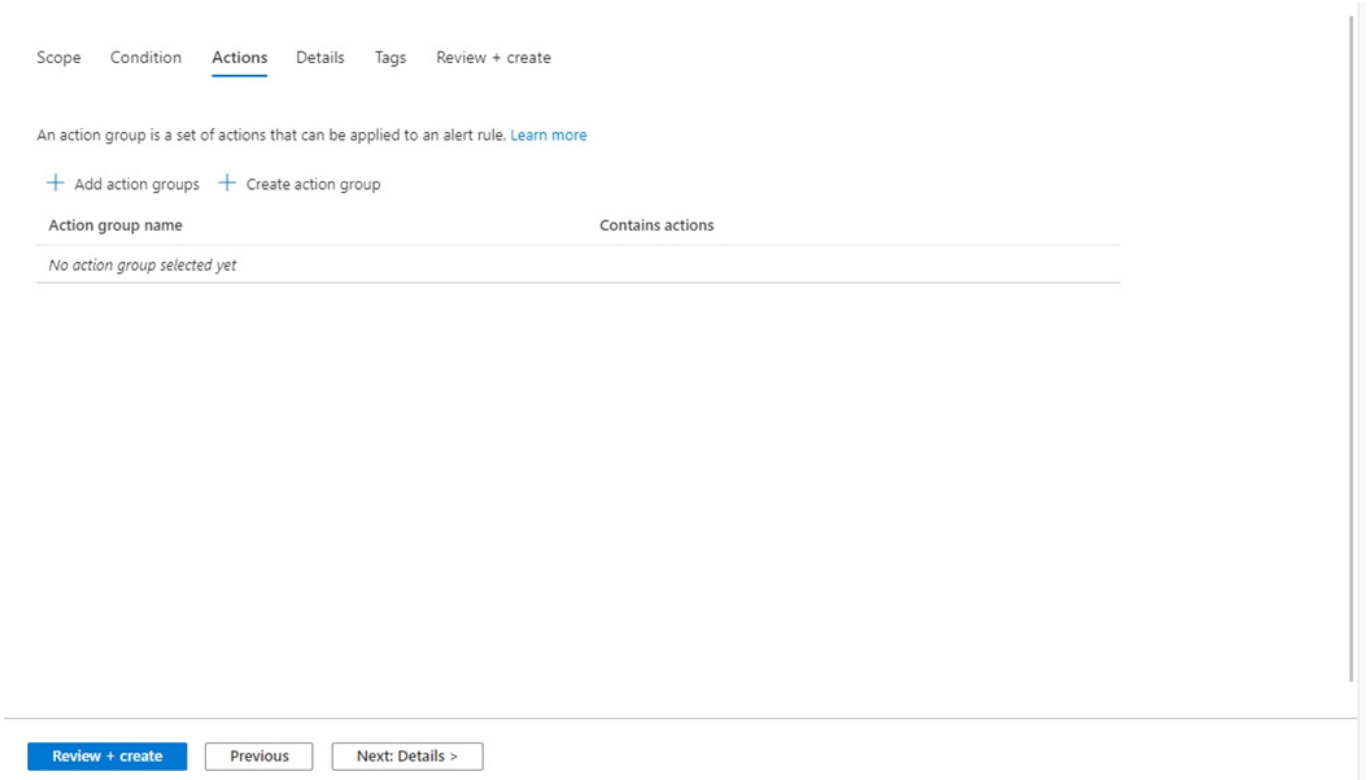
*

Signal type: The type of alert rule you\\'re creating. We select Activity log

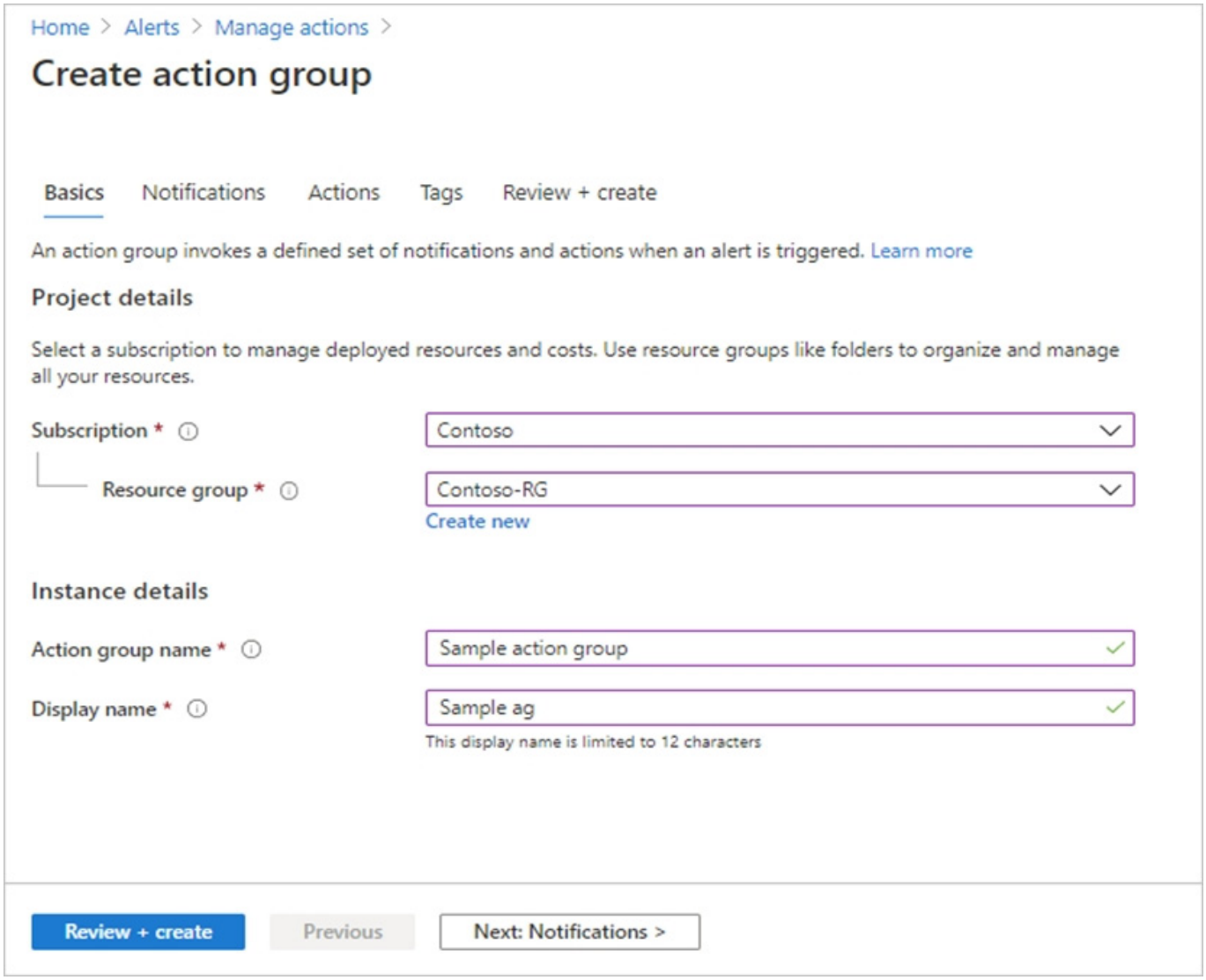
*

Monitor service: The service sending the signal. This list is pre-populated based on the type of alert rule you selected. We select Activity log – Administrative (The service that provides the Administrative activity log events)

Step 8: On the Actions tab, select to create the required action group.

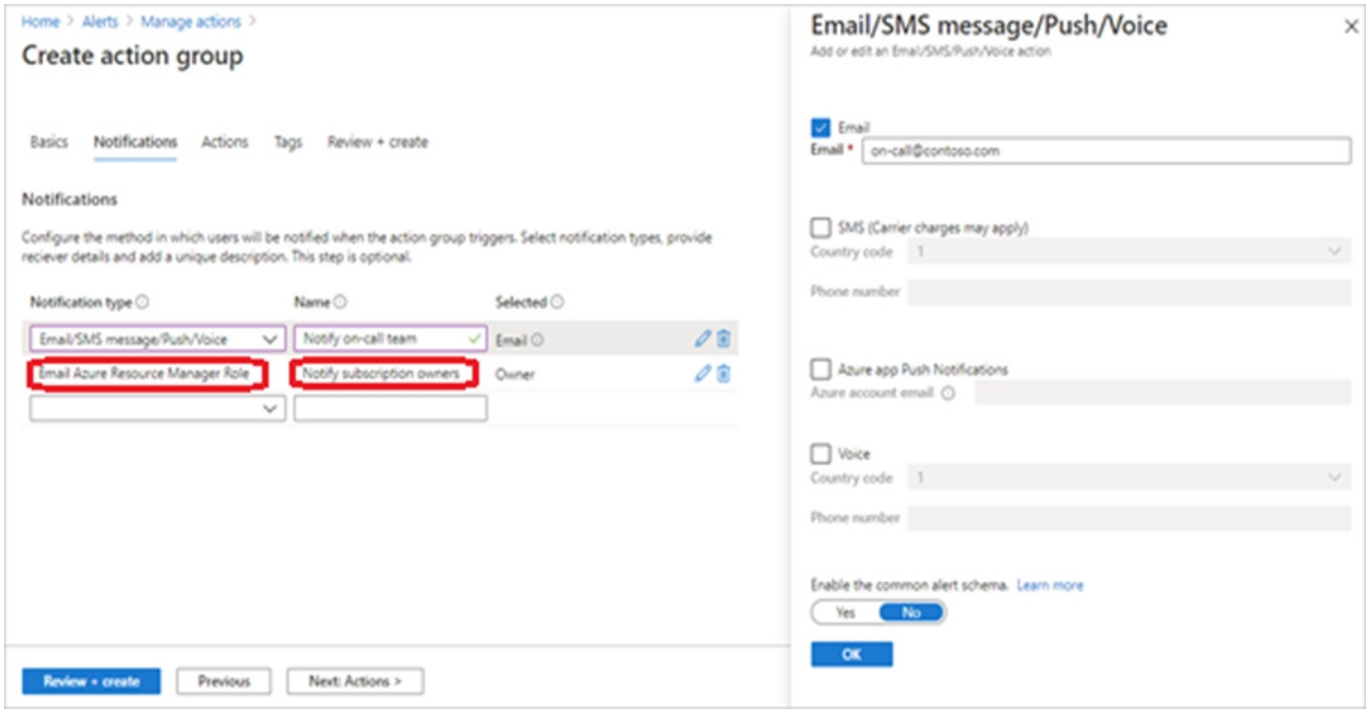


Step 9: Configure basic action group settings



Step 10: Configure notifications. To open the Notifications tab, select Next: Notifications. Alternately, at the top of the page, select the Notifications tab.

Step 11: Define a list of notifications to send when an alert is triggered. Notification: Email Azure Resource Manager Role Name: Notify Owner



Step 12: Select OK.

Step 13: Finish the remaining steps in the wizard.

Reference: https://learn.microsoft.com/en-us/azure/virtual-network/monitor-virtual-network https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-create-new-alert-rule?tabs=metric#create-a-new-alert-rule-in-the-azure-portal

---

QUESTION 5

You have an on-premises datacenter and an Azure subscription.

You plan to implement ExpressRoute FastPath.

You need to create an ExpressRoute gateway. The solution must minimize downtime if a single Azure datacenter fails.

Which SKU should you use?

A. ErGw1AZ

B. High performance

C. Ultra performance

D. ErGw3AZ

E. ErGw2AZ

Correct Answer: D

ErGw3Az and Ultra Performance SKU supports FastPath. ErGw3Az is Zone-redundant, but not Ultra Performance SKU.

Latest AZ-700 Dumps AZ-700 VCE Dumps AZ-700 Practice Test