AZ-104$^{Q\&As}$

Microsoft Azure Administrator

Pass Microsoft AZ-104 Exam with 100% Guarantee

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

https://www.pass2lead.com/az-104.html

100% Passing Guarantee
100% Money Back Assurance

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

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 subscription named Subscription1. Subscription1 contains a resource group named RG1. RG1 contains resources that were deployed by using templates.

You need to view the date and time when the resources were created in RG1.

Solution: From the RG1 blade, you click Deployments.

Does this meet the goal?

A. Yes

B. No

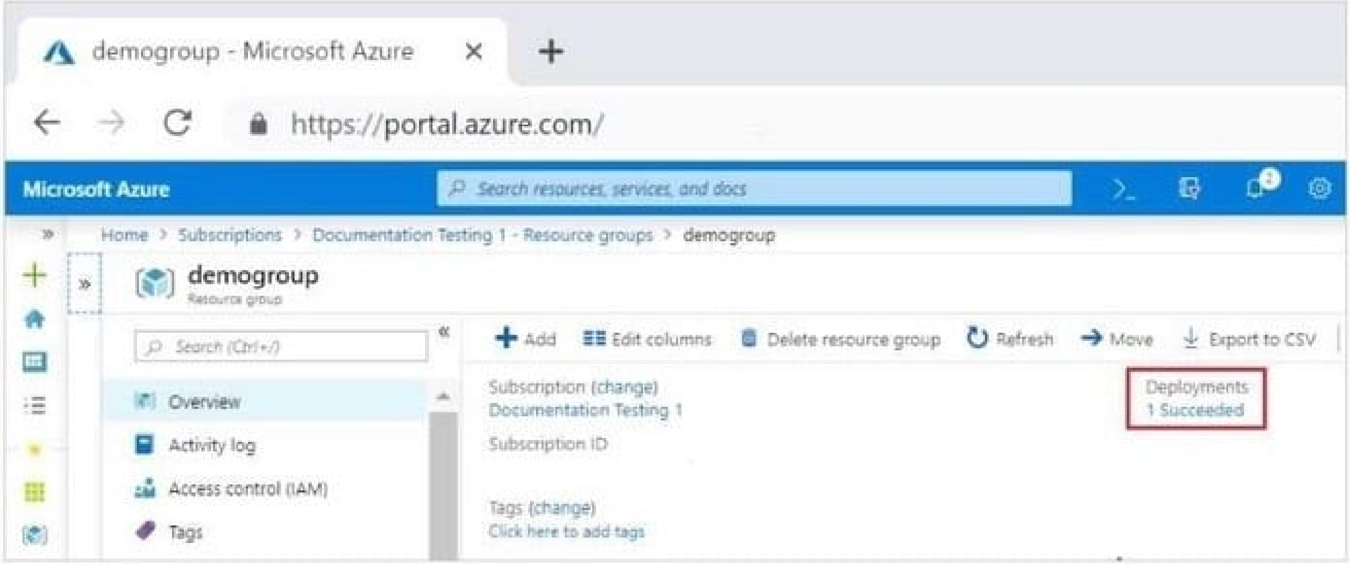
Correct Answer: A

1.

Select the resource group (Here RG1) you want to examine.

2.

Select the link under Deployments.


demogroup - Microsoft Azure
https://portal.azure.com/
Microsoft Azure
Search resources, services, and docs
Home > Subscriptions > Documentation Testing 1 - Resource groups > demogroup
demogroup
Resource group
Search (Ctrl+/)
Add
Edit columns
Delete resource group
Refresh
Move
Export to CSV
Overview
Activity log
Access control (IAM)
Tags

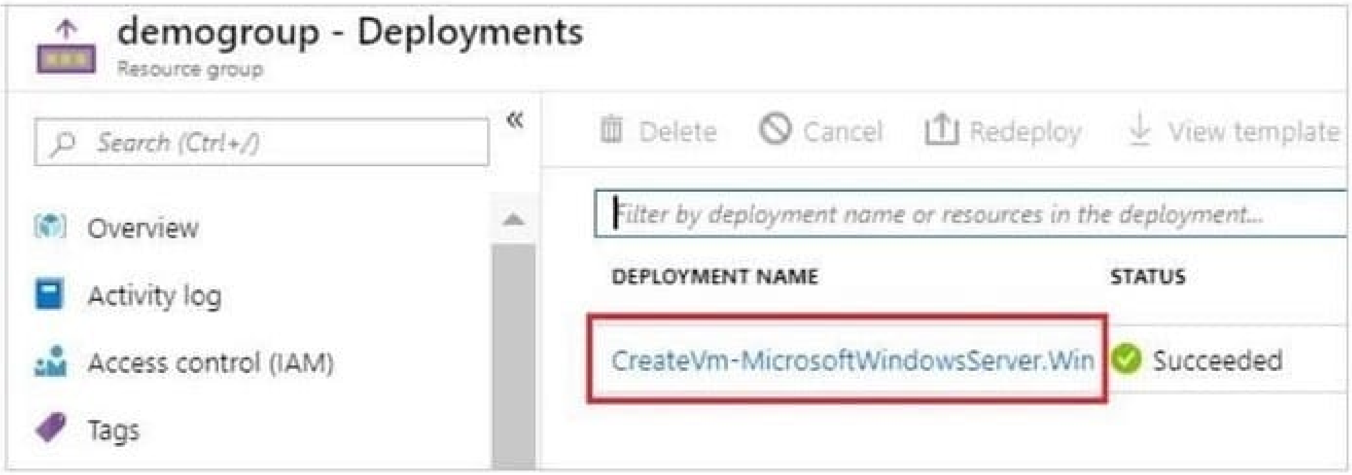
Subscription (change)
Documentation Testing 1

Subscription ID

Tags (change)
Click here to add tags

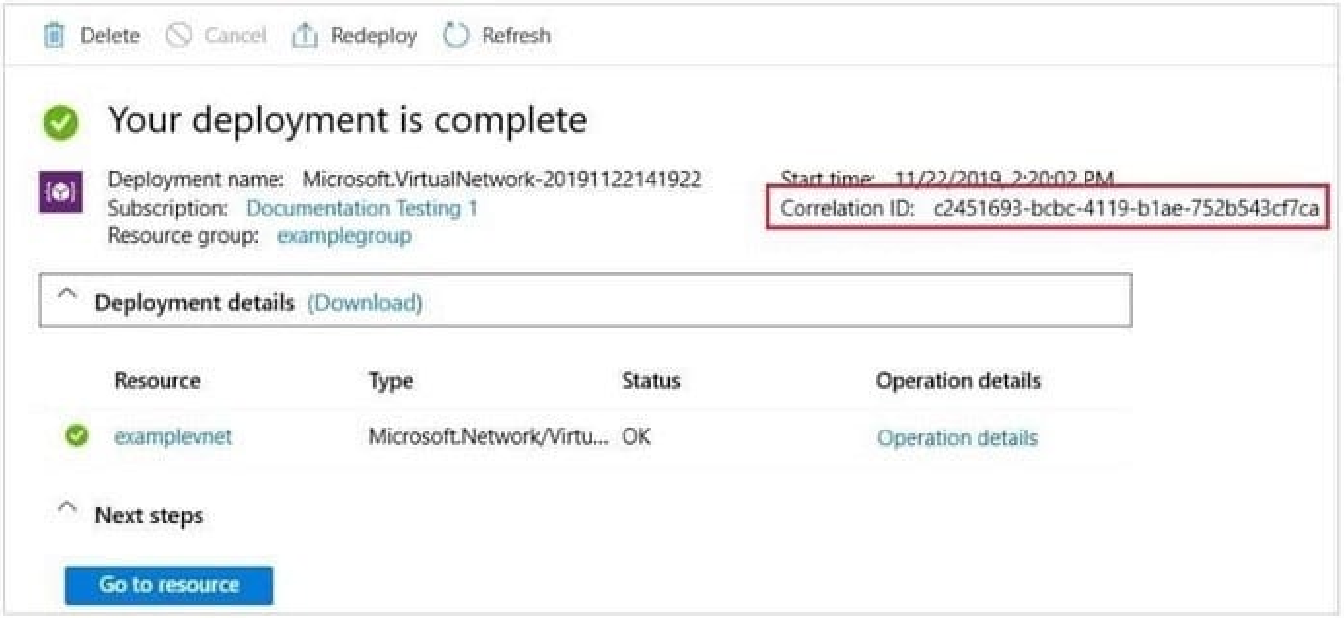
Deployments
1 Succeeded

3. Select one of the deployments from the deployment history.



DEPLOYMENT NAME	STATUS
CreateVm-MicrosoftWindowsServer.Win	✓ Succeeded

4. You will see a history of deployment for the resource group, including the correlation ID.



Your deployment is complete

Deployment name: Microsoft.VirtualNetwork-20191122141922
Subscription: Documentation Testing 1
Resource group: examplegroup

Start time: 11/22/2019, 2:20:02 PM
Correlation ID: c2451693-bcbc-4119-b1ae-752b543cf7ca

Deployment details (Download)

Resource	Type	Status	Operation details
✓ examplevnet	Microsoft.Network/Virtu...	OK	Operation details

Next steps

Reference: https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/deployment-history?tabs=azure-portal

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 virtual machine named VM1 that runs Windows Server 2016.

You need to create an alert in Azure when more than two error events are logged to the System event log on VM1 within an hour.

Solution: You create an Azure storage account and configure shared access signatures (SASs). You install the Microsoft Monitoring Agent on VM1. You create an alert in Azure Monitor and specify the storage account as the source.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Instead: You create an Azure Log Analytics workspace and configure the data settings. You install the Microsoft Monitoring Agent on VM1. You create an alert in Azure Monitor and specify the Log Analytics workspace as the source.

1.

Creating an Azure storage account and configuring shared access signatures (SASs) is not necessary for monitoring events on a virtual machine. Azure Monitor can directly collect events from the VM\\'s System event log using the Microsoft Monitoring Agent.

2.

The Microsoft Monitoring Agent can indeed collect logs and send them to Azure Monitor, but specifying a storage account as the source would not be the typical approach for monitoring System event logs. You would usually send the logs directly to a Log Analytics workspace.

3.

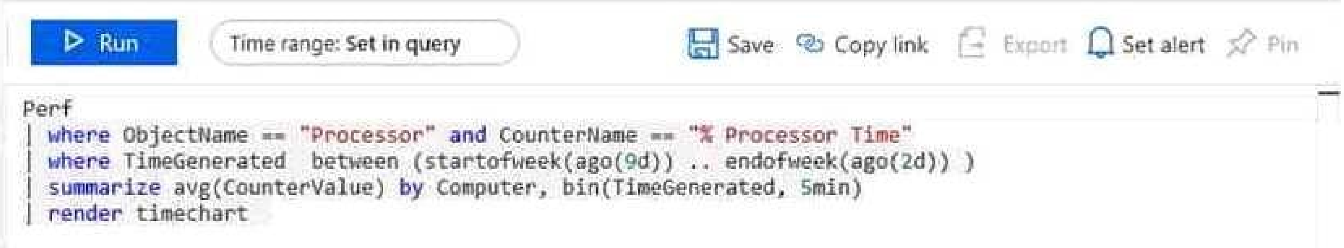
To monitor the System event log for specific events, you would set up a Log Analytics workspace, configure the Microsoft Monitoring Agent to send logs to that workspace, and then set up an alert based on a query that examines those logs.

Reference: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agents-overview

QUESTION 3

HOTSPOT

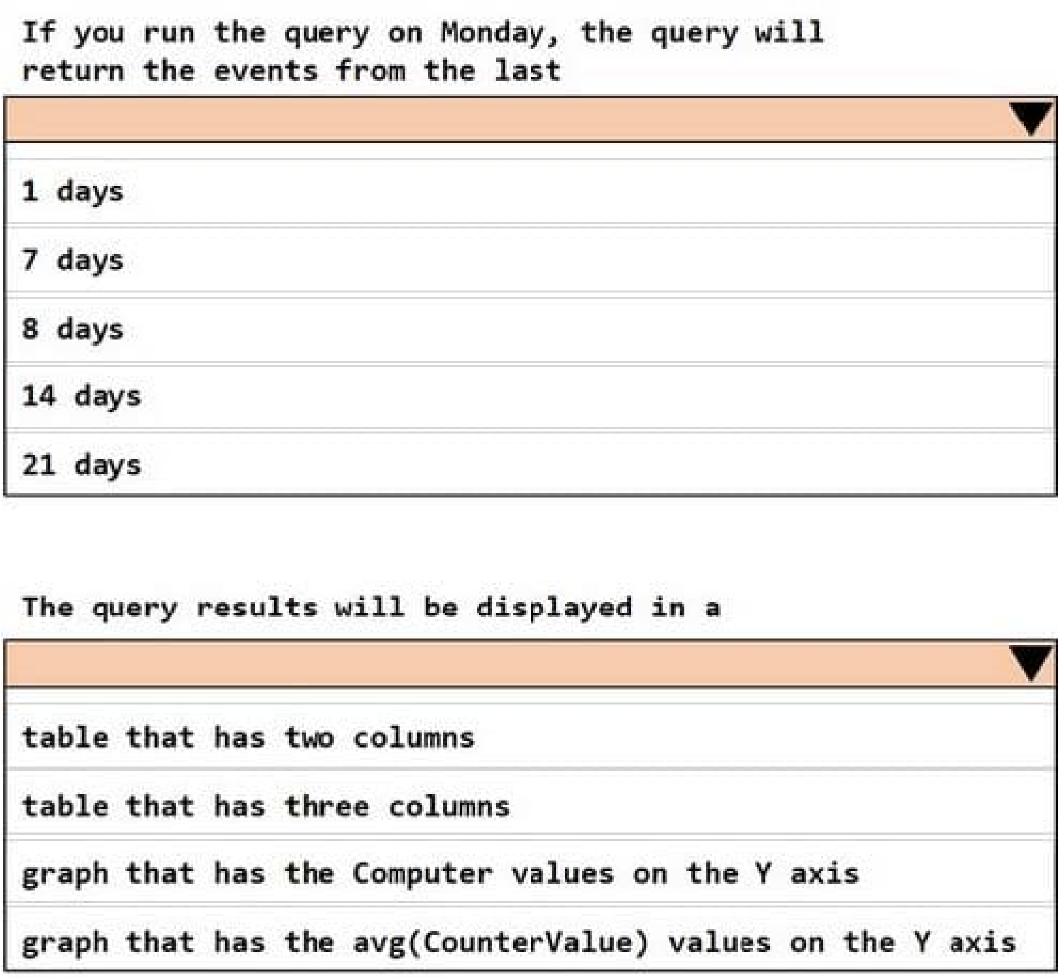
You have an Azure subscription that contains several virtual machines and an Azure Log Analytics workspace named Workspace1. You create a log search query as shown in the following exhibit.



```
Perf
| where ObjectName == "Processor" and CounterName == "% Processor Time"
| where TimeGenerated  between (startofweek(ago(9d)) .. endofweek(ago(2d)) )
| summarize avg(CounterValue) by Computer, bin(TimeGenerated, 5min)
| render timechart
```

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

Hot Area:



If you run the query on Monday, the query will return the events from the last

1 days

7 days

8 days

14 days

21 days

The query results will be displayed in a

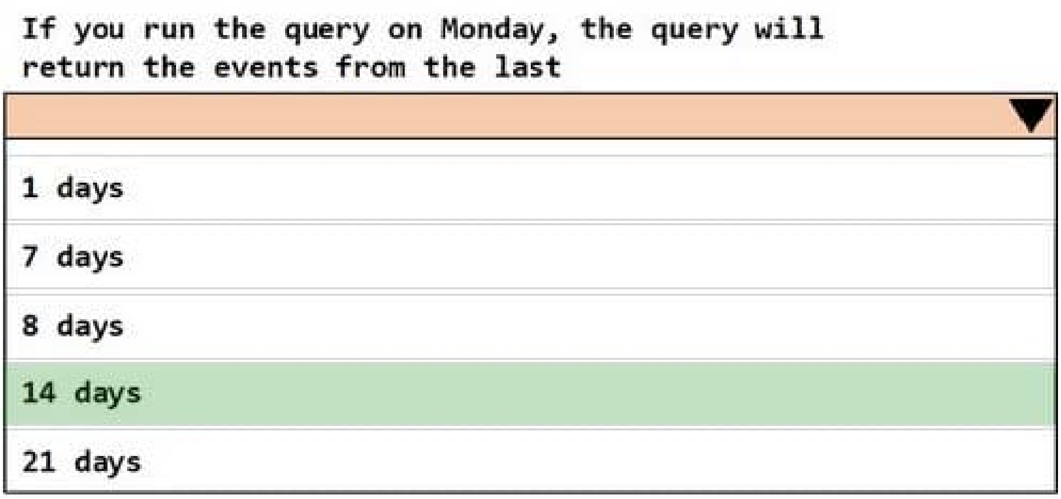
table that has two columns

table that has three columns

graph that has the Computer values on the Y axis

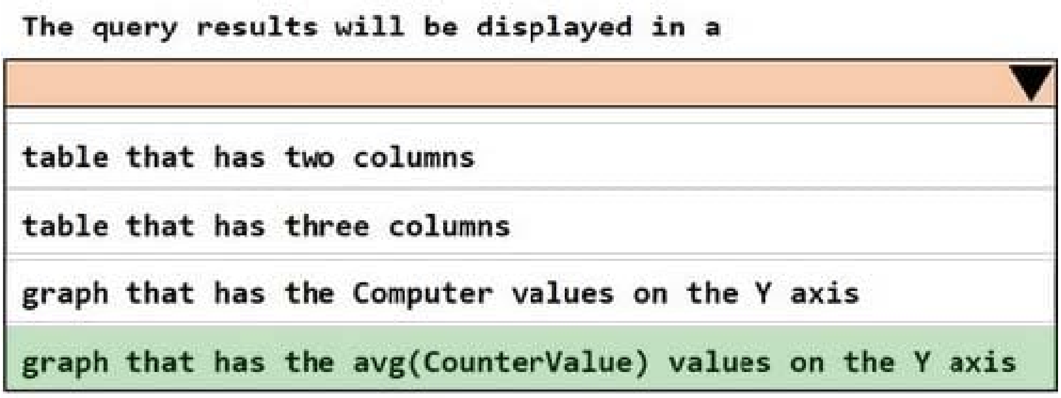
graph that has the avg(CounterValue) values on the Y axis

Correct Answer:



If you run the query on Monday, the query will return the events from the last

- 1 days
- 7 days
- 8 days
- [✓ 14 days]
- 21 days



The query results will be displayed in a

- table that has two columns
- table that has three columns
- graph that has the Computer values on the Y axis
- [✓ graph that has the avg(CounterValue) values on the Y axis]

Box 1: 14 days

Two weeks will be covered.

Note: Startofweek returns the start of the week containing the date, shifted by an offset, if provided.

Start of the week is considered to be a Sunday.

Endofweek returns the end of the week containing the date, shifted by an offset, if provided.

Last day of the week is considered to be a Saturday.

Box 2:

The render operator renders results in as graphical output. Timechart is a Line graph, where the first column is x-axis, and should be datetime. Other columns are y-axes. In this case the Y axis has avg(CounterValue) Values.

References:

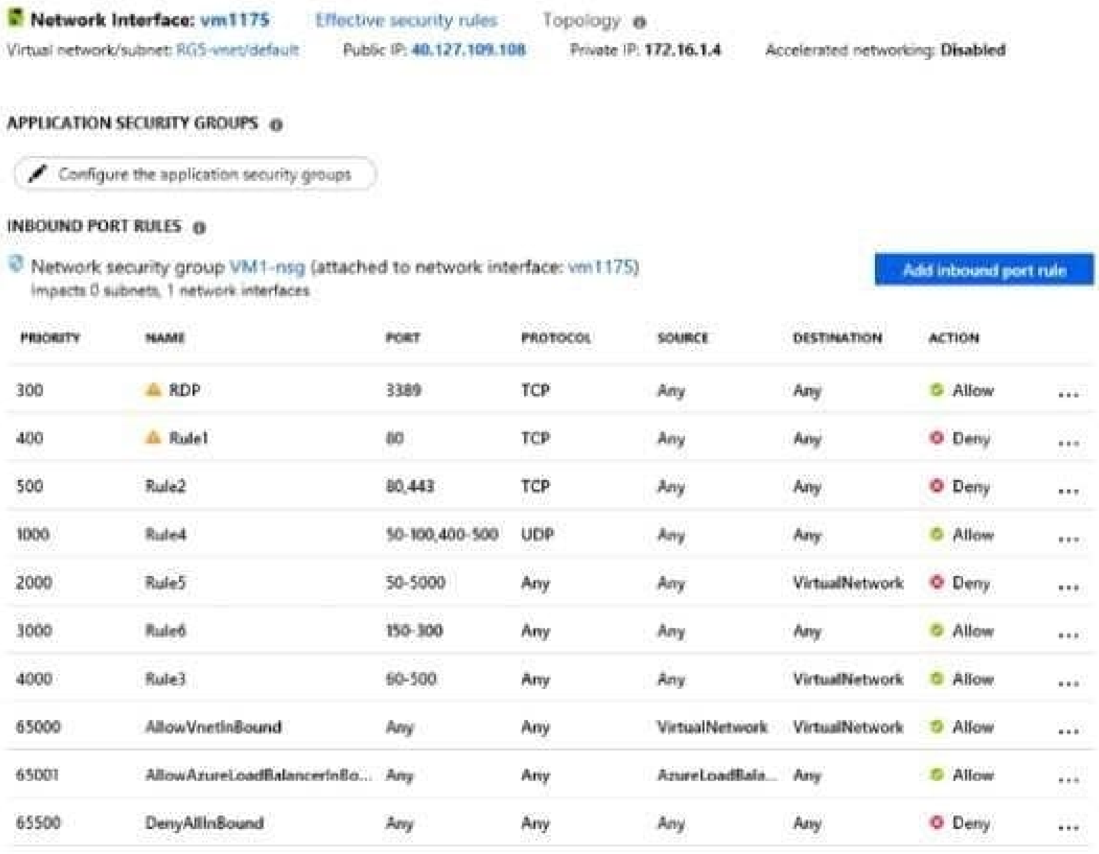
https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/log-query-overview

https://docs-analytics-eus.azurewebsites.net/queryLanguage/query_language_renderoperator.html

QUESTION 4

You have an Azure virtual machine named VMV

The network interface for VM1 is configured as shown in the exhibit(Click the Exhibit tab.)



Network Interface: vm1175 Effective security rules Topology

Virtual network/subnet: RG5-vnet/default Public IP: 40.127.109.108 Private IP: 172.16.1.4 Accelerated networking: Disabled

APPLICATION SECURITY GROUPS

Configure the application security groups

INBOUND PORT RULES

Network security group VM1-nsg (attached to network interface: vm1175)
Impacts 0 subnets, 1 network interfaces

Add inbound port rule

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION	
300	⚠ RDP	3389	TCP	Any	Any	Allow	...
400	⚠ Rule1	80	TCP	Any	Any	Deny	...
500	Rule2	80,443	TCP	Any	Any	Deny	...
1000	Rule4	50-100,400-500	UDP	Any	Any	Allow	...
2000	Rule5	50-5000	Any	Any	VirtualNetwork	Deny	...
3000	Rule6	150-300	Any	Any	Any	Allow	...
4000	Rule3	60-500	Any	Any	VirtualNetwork	Allow	...
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	...
65001	AllowAzureLoadBalancerInBo...	Any	Any	AzureLoadBala...	Any	Allow	...
65500	DenyAllInBound	Any	Any	Any	Any	Deny	...

You deploy a web server on VM1. and then create a secure website that is accessible by using the HTTPS protocol. VM1 is used as a web server only.

You need to ensure that users can connect to the website from the internet.

What should you do?

A. For Rule4. change the protocol from UDP to Any

B. Modify the protocol of Rule4.

C. Modify the action of Rule1.

D. Change the priority of Rute3 to 450

Correct Answer: D

Rule 2 is blocking HTTPS access (port 443) and has a priority of 500. Changing Rule 3 (ports 60-500) and giving it a lower priority number will allow access on port 443. Note: Rules are processed in priority order, with lower numbers

processed before higher numbers, because lower numbers have higher priority. Once traffic matches a rule, processing stops.

Incorrect Answers:

A: HTTPS uses port 443. Rule6 only applies to ports 150 to 300. C, D: Rule 1 blocks access to port 80, which is used for HTTP, not HTTPS.

Reference:

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

QUESTION 5

You have two Azure virtual machines named VM1 and VM2 that run Windows Server. The virtual machines are in a subnet named Subnet1. Subnet1 is in a virtual network named VNet1.

You need to prevent VM1 from accessing VM2 on port 3389.

What should you do?

A. Create a network security group (NSG) that has an outbound security rule to deny destination port 3389 and apply the NSG to the network interface of VM1.

B. Configure Azure Bastion in VNet1.

C. Create a network security group (NSG) that has an outbound security rule to deny source port 3389 and apply the NSG to Subnet1.

D. Create a network security group (NSG) that has an inbound security rule to deny source port 3389 and apply the NSG to Subnet1.

Correct Answer: A

By creating an outbound security rule in a network security group (NSG) to deny destination port 3389, you can prevent VM1 from accessing port 3389 on VM2. By applying the NSG to the network interface of VM1, you can enforce the security rule specifically for VM1.

This solution provides a centralized way to manage and enforce network security for VM1, and it helps to prevent unwanted access to port 3389 on VM2 from VM1.