AZ-500 Q&As

Microsoft Azure Security Technologies

Pass Microsoft AZ-500 Exam with 100% Guarantee

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

https://www.certbus.com/az-500.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

You have been tasked with delegate administrative access to your company\\'s Azure key vault.

You have to make sure that a specific user can set advanced access policies for the key vault. You also have to make sure that access is assigned based on the principle of least privilege.

Which of the following options should you use to achieve your goal?

A. A key vault access policy

B. Azure policy

C. Azure AD Privileged Identity Management (PIM)

D. Azure DevOps

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault

QUESTION 2

You have an Azure Container Registry named ContReg1 that contains a container image named image1.

You enable content trust for ContReg1.

After content trust is enabled, you push two images to ContReg1 as shown in the following table.

Name	Details
image2	Image was pushed with client content trust enabled.
image3	Image was pushed with client content trust disabled.

Which images are trusted images?

A. image1 and image2 only

B. image2 only

C. image1, image2, and image3

D. https://www.certbus.com/az-500.html

Correct Answer: B

Azure Container Registry implements Docker\\'s content trust model, enabling pushing and pulling of signed images.

To push a trusted image tag to your container registry, enable content trust and push the image with docker push.

To work with trusted images, both image publishers and consumers need to enable content trust for their Docker clients.

As a publisher, you can sign the images you push to a content trust-enabled registry.

Reference:

https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust

QUESTION 3

HOTSPOT

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

Name	Location	Subnet	Peered network
VNET1	East US	Subnet1	VNET2
VNET2	West US	Subnet2, Subnet3	VNET1
VNET4	East US	Subnet4	*None*

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

Name	Application security group	Network security group (NSG)	Connected to	Public IP address
VM1	ASG1	NSG1	Subnet1	No
VM2	ASG2	NSG1	Subnet2	No
VM3	ASG2	NSG1	Subnet3	Yes
VM4	ASG4	NSG1	Subnet4	Yes

The firewalls on all the virtual machines allow ping traffic.

NSG1 is configured as shown in the following exhibit. Inbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
110	Allow_RDP	3389	Any	Any	Any	Allow ...
130	Rule1	Any	Any	ASG1	Any	Allow ...
140	Rule2	Any	Any	ASG2	Any	Allow ...
150	Rule3	Any	Any	ASG4	Any	Allow ...
160	Rule4	Any	Any	Any	Any	Deny ...
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow ...
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	Allow ...
65500	DenyAllInBound	Any	Any	Any	Any	Deny ...

Outbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow ...
65001	AllowInternetOutBou...	Any	Any	Any	Internet	Allow ...
65500	DenyAllOutBound	Any	Any	Any	Any	Deny ...

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
VM1 can ping VM3 successfully.	○	○
VM2 can ping VM4 successfully.	○	○
VM3 can be accessed by using Remote Desktop from the internet.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
VM1 can ping VM3 successfully.	○	○
VM2 can ping VM4 successfully.	○	○
VM3 can be accessed by using Remote Desktop from the internet.	○	○

Box 1: Yes

VM1 and VM3 are on peered VNets. The firewall rules with a source of ASG1 and ASG2 allow ‘any’ traffic on ‘any’ protocol so pings are allowed between VM1 and VM3.

Box 2: No

VM2 and VM4 are on separate VNets and the VNets are not peered. Therefore, the pings would have to go over the Internet. VM4 does have a public IP and the firewall allows pings. However, for VM2 to be able to ping VM4, VM2 would

also need a public IP address. In Azure, pings don\\'t go out through the default gateway as they would in a physical network. For an Azure VM to ping external IPs, the VM must have a public IP address assigned to it.

Box 3: Yes

VM3 has a public IP address and the firewall allows traffic on port 3389.

QUESTION 4

You have Azure virtual machines that have Update Management enabled. The virtual machines are configured as shown in the following table.

Name	Operating system	Region	Resource group
VM1	Windows Server 2012	East US	RG1
VM2	Windows Server 2012 R2	West US	RG1
VM3	Windows Server 2016	West US	RG2
VM4	Ubuntu Server 18.04 LTS	West US	RG2
VM5	Red Hat Enterprise Linux 7.4	East US	RG1
VM6	CentOS 7.5	East US	RG1

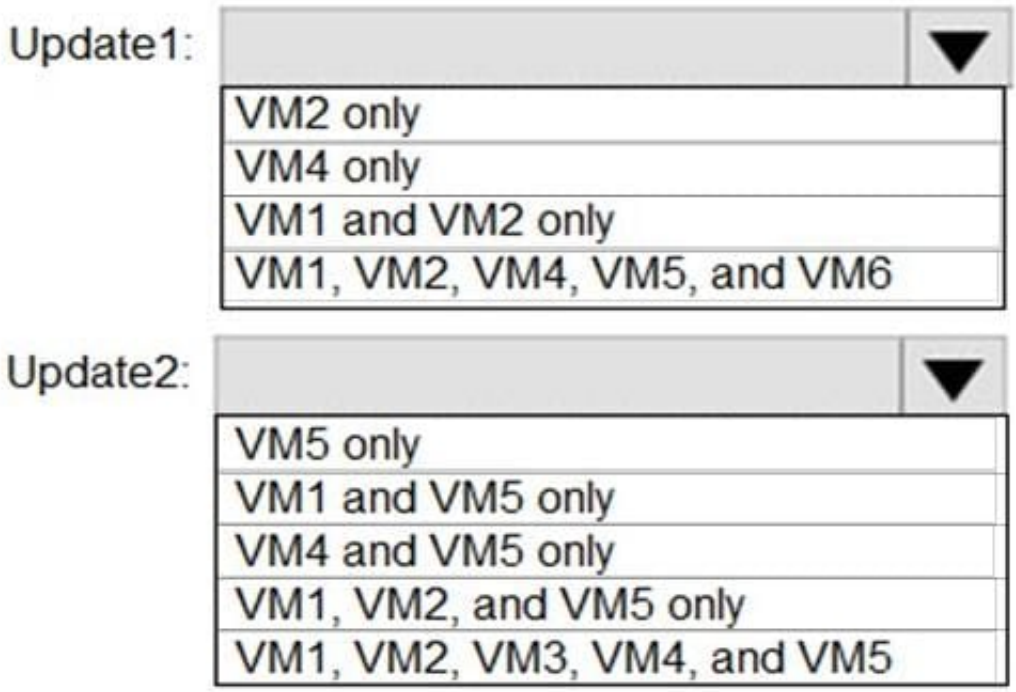
You schedule two update deployments named Update1 and Update2. Update1 updates VM3. Update2 updates VM6.

Which additional virtual machines can be updated by using Update1 and Update2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

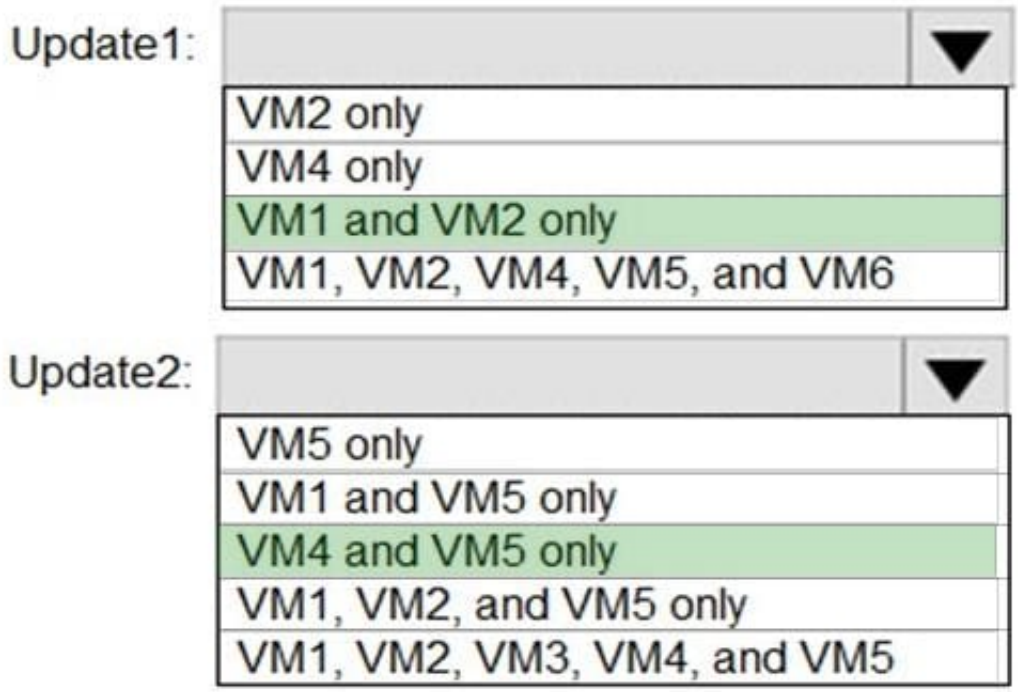
Hot Area:

Answer Area



Correct Answer:

Answer Area



Update1: VM1 and VM2 only VM3: Windows Server 2016 West US RG2

Update2: VM4 and VM5 only VM6: CentOS 7.5 East US RG1

For Linux, the machine must have access to an update repository. The update repository can be private or public.

References: https://docs.microsoft.com/en-us/azure/automation/automation-update-management

QUESTION 5

HOTSPOT

You have an Azure Sentinel workspace that has the following data connectors:

1.

Azure Active Directory Identity Protection

2.

Common Event Format (CEF)

3.

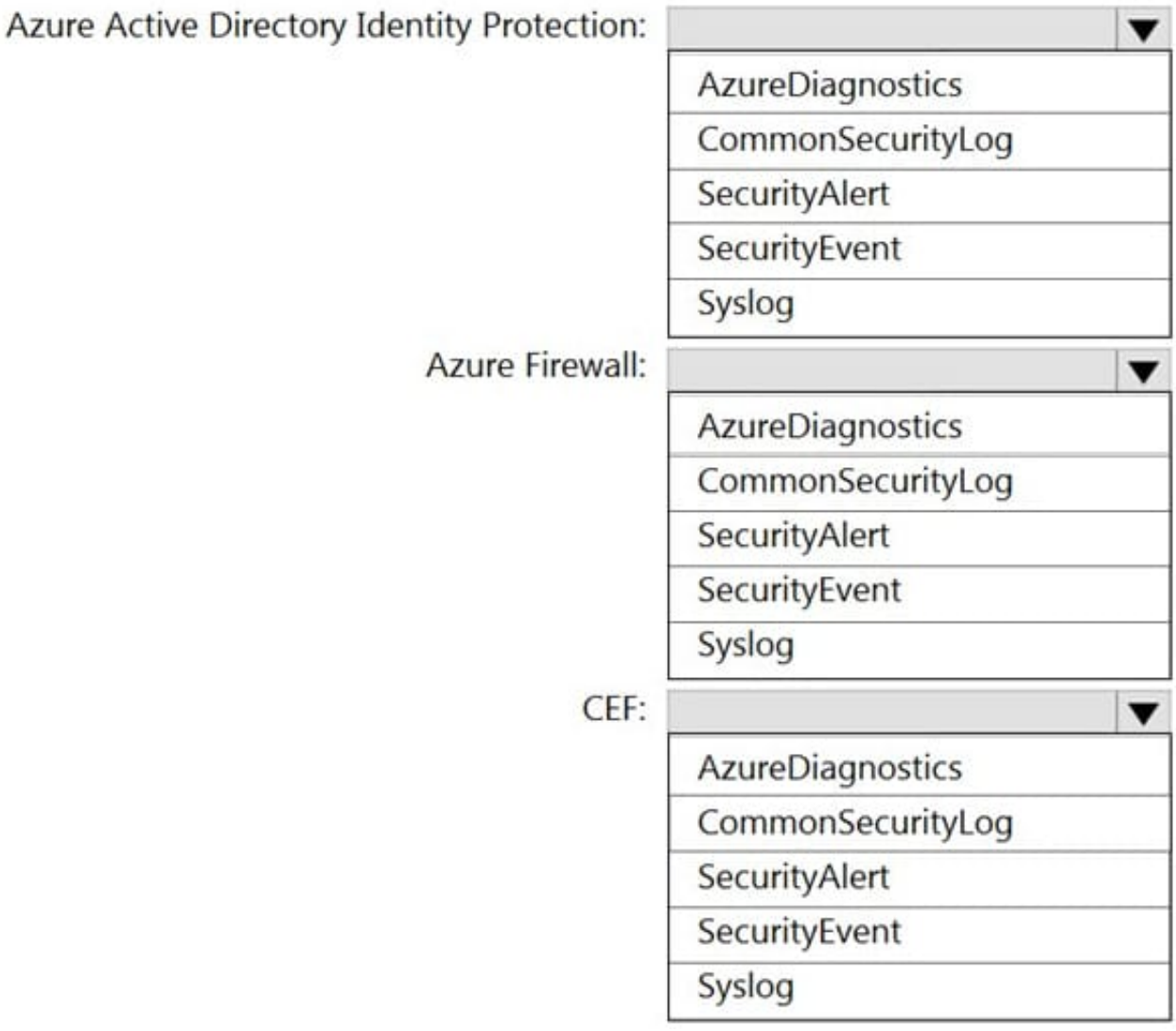
Azure Firewall

You need to ensure that data is being ingested from each connector.

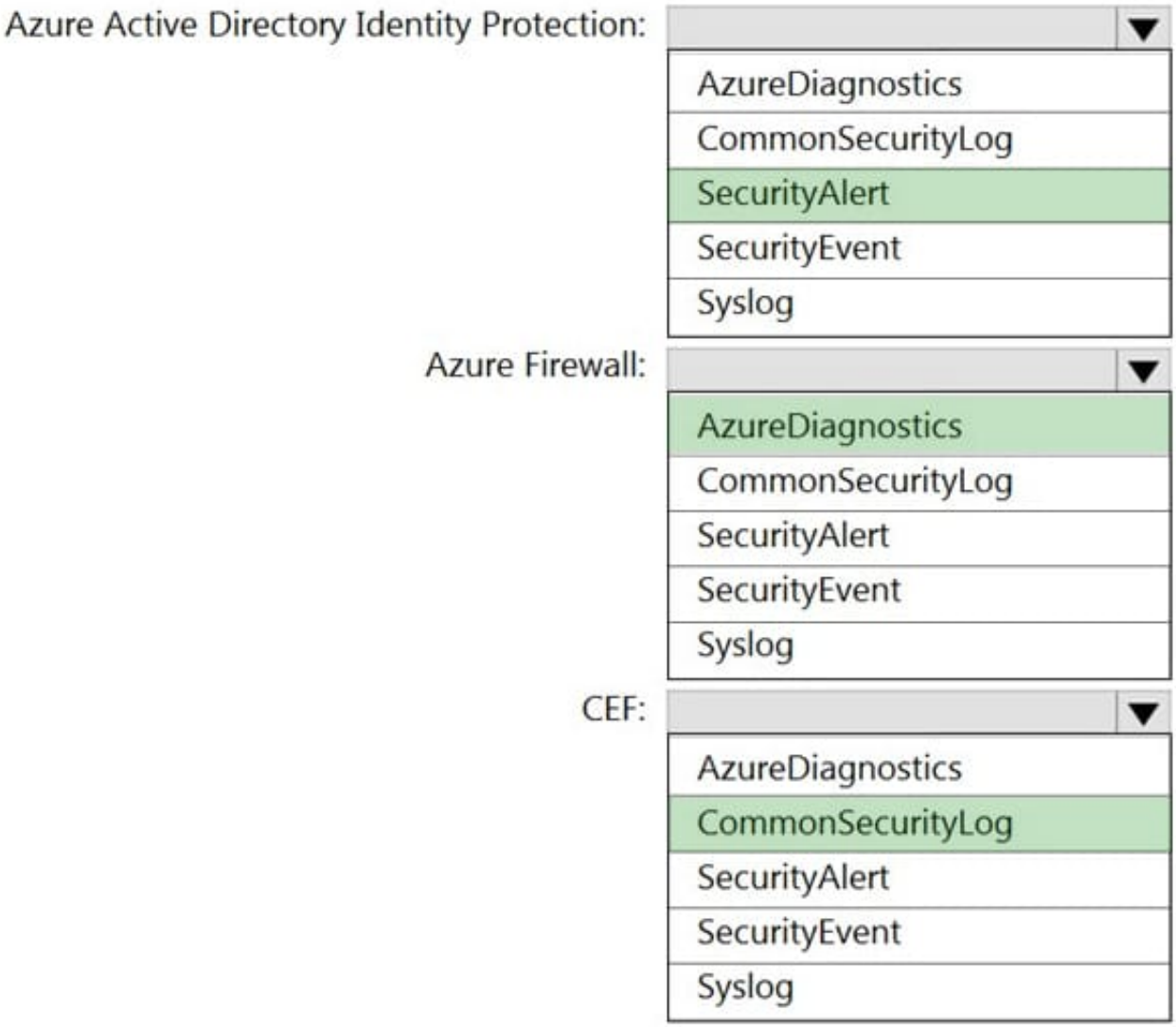
From the Logs query window, which table should you query for each connector? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Reference: https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-ad-identity-protection https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-firewall https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources

QUESTION 6

From Azure Security Center, you enable Azure Container Registry vulnerability scanning of the images in Registry1. You perform the following actions:

1.

Push a Windows image named Image1 to Registry1.

2.

Push a Linux image named Image2 to Registry1.

3.

Push a Windows image named Image3 to Registry1.

4.

Modify Image1 and push the new image as Image4 to Registry1.

5.

Modify Image2 and push the new image as Image5 to Registry1.

Which two images will be scanned for vulnerabilities? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Image4

B. Image2

C. Image1

D. Image3

E. Image5

Correct Answer: BE

Only Linux images are scanned. Windows images are not scanned.

Reference: https://docs.microsoft.com/en-us/azure/security-center/azure-container-registry-integration

QUESTION 7

DRAG DROP

You are configuring network connectivity for two Azure virtual networks named VNET1 and VNET2.

You need to implement VPN gateways for the virtual networks to meet the following requirements:

1.

VNET1 must have six site-to-site connections that use BGP.

2.

VNET2 must have 12 site-to-site connections that use BGP.

3.

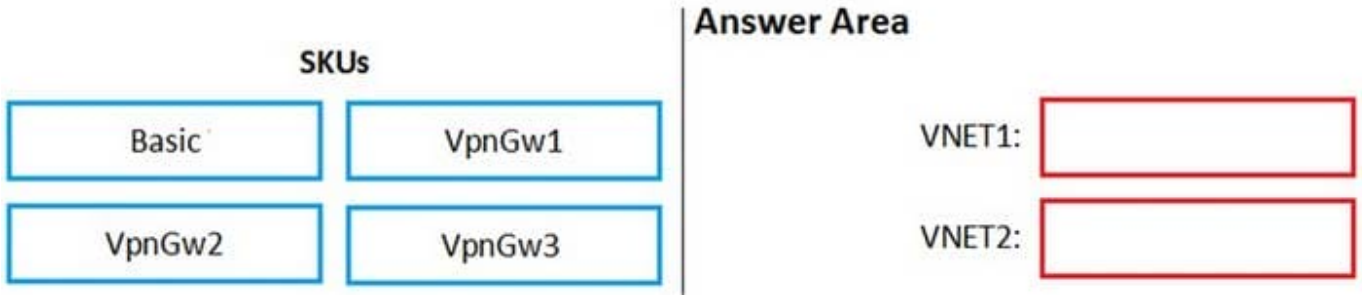
Costs must be minimized.

Which VPN gateway SKU should you use for each virtual network? To answer, drag the appropriate SKUs to the correct networks. Each SKU may be used once, more than once, or not at all. You may need to drag the split bar between

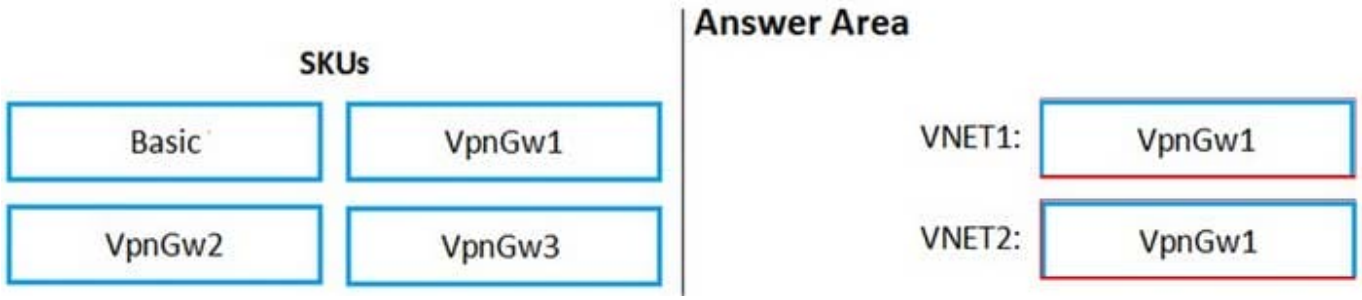
panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



References: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways#gwsku

QUESTION 8

HOTSPOT

You have an Azure subscription that contains an Azure Sentinel workspace.

Azure Sentinel is configured to ingest logs from several Azure workloads. A third-party service management platform is used to manage incidents.

You need to identify which Azure Sentinel components to configure to meet the following requirements:

1.

When Azure Sentinel identifies a threat, an incident must be created.

2.

A ticket must be logged in the service management platform when an incident is created in Azure Sentinel.

Which component should you identify for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

When Azure Sentinel identifies a threat, an incident must be created:

- Analytics
- Data connectors
- Playbooks
- Workbooks

A ticket must be logged in the service management platform when an incident is created in Azure Sentinel:

- Analytics
- Data connectors
- Playbooks
- Workbooks

Correct Answer:

Answer Area

When Azure Sentinel identifies a threat, an incident must be created:

- Analytics
- Data connectors
- Playbooks
- Workbooks

A ticket must be logged in the service management platform when an incident is created in Azure Sentinel:

- Analytics
- Data connectors
- Playbooks
- Workbooks

Reference: https://docs.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

QUESTION 9

You have an Azure subscription that contains a resource group named RG1 and the network security groups (NSGs) shown in the following table.

Name	Location	Flow logs status
NSG1	West Europe	Off
NSG2	West Europe	Off

You create the Azure policy shown in the following exhibit.

Basics Parameters Remediation Non-compliance messages Review + create

Basics

Scope	Azure Pass - Sponsorship/RG1
Exclusions	Azure Pass - Sponsorship/RG1/NSG1
Policy definition	Flow logs should be enabled for every network security group
Assignment name	Flow logs should be enabled for every network security group
Description	Description1
Policy enforcement	Enabled
Assigned by	Admin1

Parameters

effect	Audit

Remediation

Create managed identity	Yes
Managed identity location	westeurope
Create a remediation task	No

Non-compliance messages

Default non-compliance message	Message1

You assign the policy to RG1.

What will occur if you assign the policy to NSG1 and NSG2?

A. Flow logs will be enabled for NSG1 and NSG2.

B. Flow logs will be enabled for NSG2 only.

C. Flow logs will be disabled for NSG1 and NSG2.

D. Flow logs will be enabled for NSG1 only.

Correct Answer: B

QUESTION 10

HOTSPOT

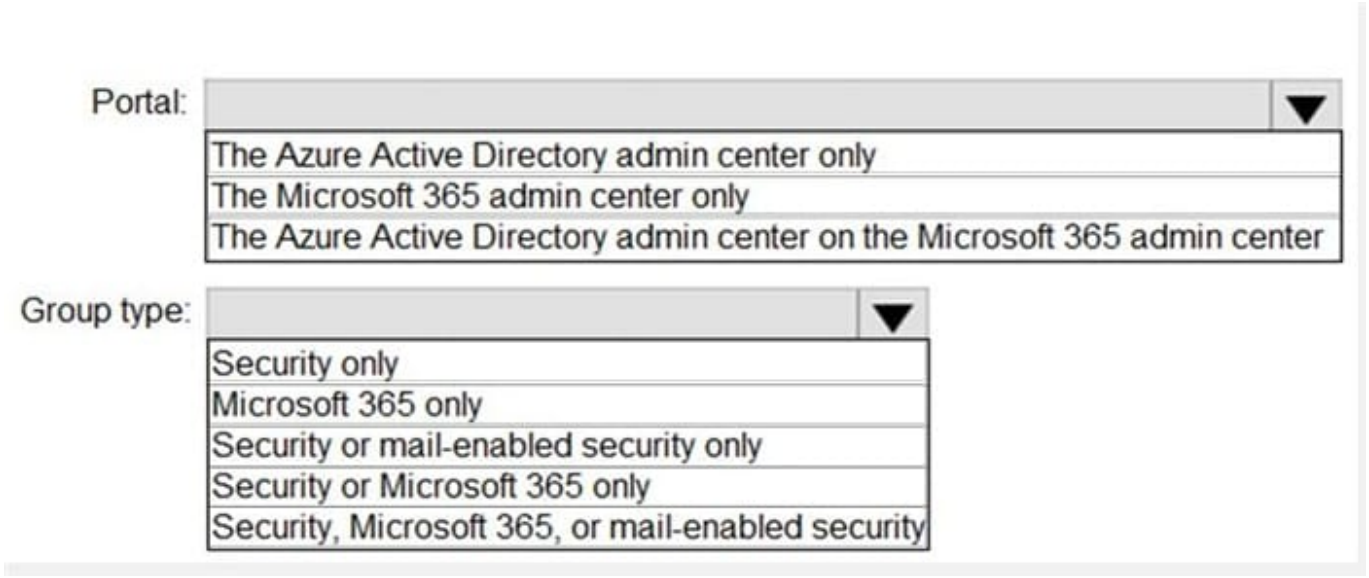
You have an Azure Active Directory (Azure AD) tenant named contoso.com that has Azure Active Directory Premium Plan 1 licenses.

You need to create a group named Group1 that will be assigned the Global reader role.

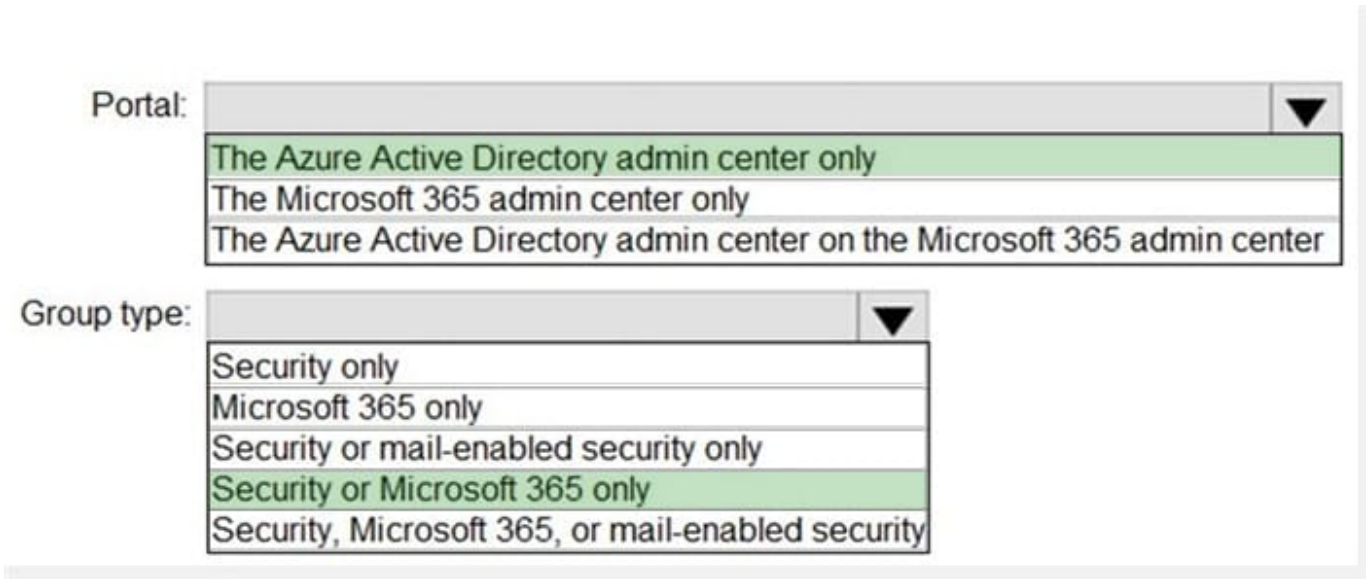
Which portal should you use to create Group1, and which type of group should you create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



QUESTION 11

HOTSPOT

You have an Azure subscription named Sub 1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Type
User1	Global administrator
User2	Security administrator
User3	Security reader
User4	License administrator

Each user is assigned an Azure AD Premium P2 license.

You plan to onboard and configure Azure AD Identity Protection.

Which users can onboard Azure AD Identity Protection, remediate users, and configure policies? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Users who can onboard Azure AD Identity Protection:
- User1 only
- User1 and User2 only
- User1,User2, and User3 only
- User1,User2, User3, and User4 only

Users who can remediate users and configure policies:
- User1 and User2 only
- User1 and User3 only
- User1, User2, and User3 only
- User1, User2, User3, and User4

Correct Answer:

Answer Area

Users who can onboard Azure AD Identity Protection:

- User1 only
- User1 and User2 only
- User1,User2, and User3 only
- User1,User2, User3, and User4 only

Users who can remediate users and configure policies:

- User1 and User2 only
- User1 and User3 only
- User1, User2, and User3 only
- User1, User2, User3, and User4

QUESTION 12

DRAG DROP

You have an Azure subscription named Sub1 that contains an Azure Log Analytics workspace named LAW1.

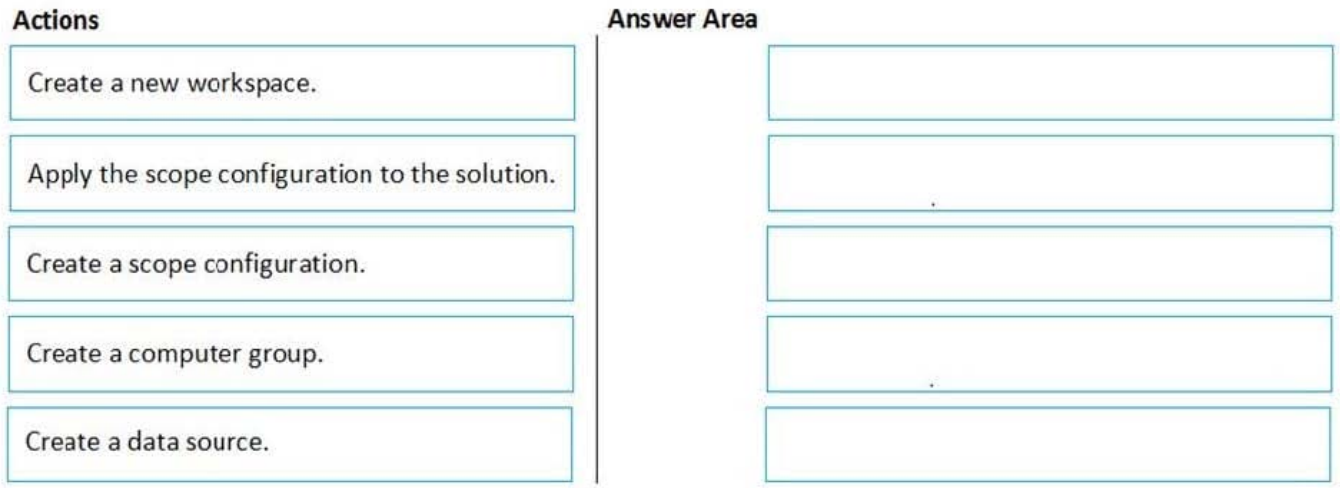
You have 500 Azure virtual machines that run Windows Server 2016 and are enrolled in LAW1.

You plan to add the System Update Assessment solution to LAW1.

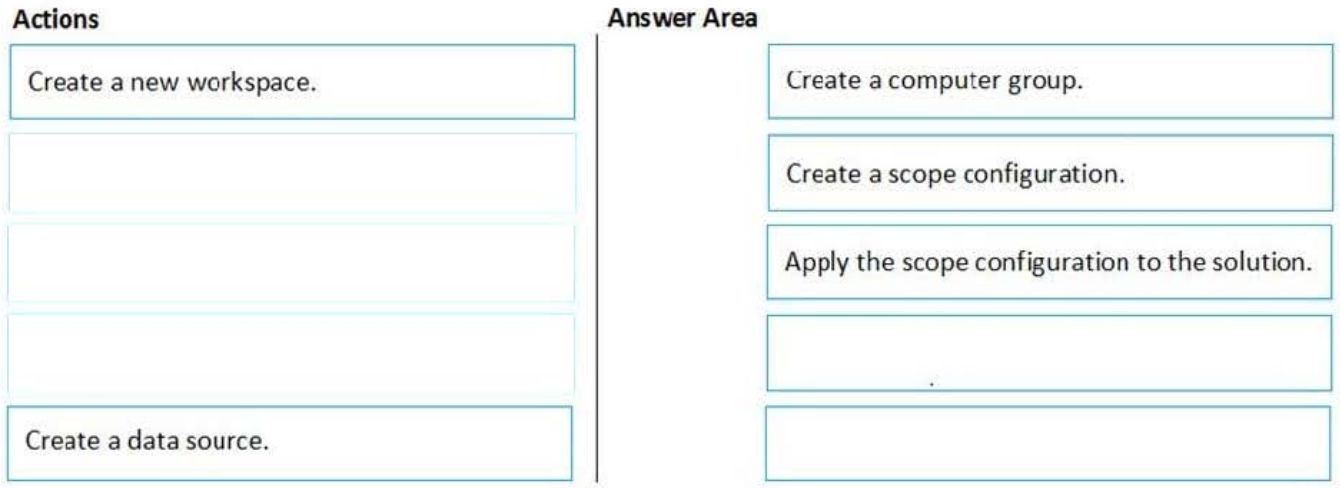
You need to ensure that System Update Assessment-related logs are uploaded to LAW1 from 100 of the virtual machines only.

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.

Select and Place:



Correct Answer:



References: https://docs.microsoft.com/en-us/azure/azure-monitor/insights/solution-targeting

QUESTION 13

You have an Azure environment.

You need to identify any Azure configurations and workloads that are non-compliant with ISO 27001:2013 standards.

What should you use?

A. Azure Active Directory (Azure AD) Identity Protection

B. Microsoft Defender for Cloud

C. Microsoft Defender for Identity

D. Microsoft Sentinel

Correct Answer: B

QUESTION 14

You have a sneaking suspicion that there are users trying to sign in to resources which are inaccessible to them.

You decide to create an Azure Log Analytics query to confirm your suspicions. The query will detect unsuccessful user sign-in attempts from the last few days. You want to make sure that the results only show users who had failed to sign-in

more than five times.

Which of the following should be included in your query?

A. The EventID and CountIf() parameters.

B. The ActivityID and CountIf() parameters.

C. The EventID and Count() parameters.

D. The ActivityID and Count() parameters.

Correct Answer: C

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

QUESTION 15

You have an Azure subscription named Sub1.

In Azure Security Center, you have a security playbook named Play1. Play1 is configured to send an email message to a user named User1.

You need to modify Play1 to send email messages to a distribution group named Alerts.

What should you use to modify Play1?

A. Azure DevOps

B. Azure Application Insights

C. Azure Monitor

D. Azure Logic Apps Designer

Correct Answer: D

You can change an existing playbook in Security Center to add an action, or conditions. To do that you just need to click on the name of the playbook that you want to change, in the Playbooks tab, and Logic App Designer opens up.

References: https://docs.microsoft.com/en-us/azure/security-center/security-center-playbooks