

➤ **Vendor: Microsoft**

➤ **Exam Code: AZ-500**

➤ **Exam Name: Microsoft Azure Security Technologies**

➤ **New Updated Questions from [Braindump2go](#) (Updated in [June/2021](#))**

Visit Braindump2go and Download Full Version AZ-500 Exam Dumps

QUESTION 269

You are troubleshooting a security issue for an Azure Storage account.
You enable the diagnostic logs for the storage account.
What should you use to retrieve the diagnostics logs?

- A. Azure Security Center
- B. Azure Monitor
- C. the Security admin center
- D. Azure Storage Explorer

Answer: B

Explanation:

<https://docs.microsoft.com/en-us/azure/storage/blobs/monitor-blob-storage?tabs=azure-portal>

QUESTION 270

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

Name	Type
VM1	Virtual machine
VNET1	Virtual network
storage1	Storage account
Vault1	Key vault

You plan to enable Azure Defender for the subscription.
Which resources can be protected by using Azure Defender?

- A. VM1, VNET1, storage1, and Vault1
- B. VM1, VNET1, and storage1 only
- C. VM1, storage1, and Vault1 only
- D. VM1 and VNET1 only
- E. VM1 and storage1 only

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/azure/security-center/azure-defender>

QUESTION 271

You have an Azure subscription that contains a resource group named RG1 and a security group named ServerAdmins. RG1 contains 10 virtual machines, a virtual network named VNET1, and a network security group

[AZ-500 Exam Dumps](#) [AZ-500 Exam Questions](#) [AZ-500 PDF Dumps](#) [AZ-500 VCE Dumps](#)

<https://www.braindump2go.com/az-500.html>

(NSG) named NSG1. ServerAdmins can access the virtual machines by using RDP.

You need to ensure that NSG1 only allows RDP connections to the virtual machines for a maximum of 60 minutes when a member of ServerAdmins requests access.

What should you configure?

- A. an Azure policy assigned to RG1
- B. a just in time (JIT) VM access policy in Azure Security Center
- C. an Azure Active Directory (Azure AD) Privileged Identity Management (PIM) role assignment
- D. an Azure Bastion host on VNET1

Answer: B

Explanation:

<https://docs.microsoft.com/en-us/azure/security-center/just-in-time-explained>

QUESTION 272

You have a web app named WebApp1.

You create a web application firewall (WAF) policy named WAF1.

You need to protect WebApp1 by using WAF1.

What should you do first?

- A. Deploy an Azure Front Door.
- B. Add an extension to WebApp1.
- C. Deploy Azure Firewall.

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/azure/frontdoor/quickstart-create-front-door>

QUESTION 273

You have an Azure subscription that contains an Azure SQL database named sql1.

You plan to audit sql1.

You need to configure the audit log destination. The solution must meet the following requirements:

- Support querying events by using the Kusto query language.
- Minimize administrative effort.

What should you configure?

- A. an event hub
- B. a storage account
- C. a Log Analytics workspace

Answer: C

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/tutorial-log-analytics-wizard>

QUESTION 274

Hotspot Question

You have a management group named Group1 that contains an Azure subscription named sub1. Sub1 has a subscription ID of 11111111-1234-1234-1111111111.

You need to create a custom Azure role-based access control (RBAC) role that will delegate permissions to manage the tags on all the objects in Group1.

What should you include in the role definition of Role1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Resource provider:

Assignable scope:

Answer:

Answer Area

Resource provider:

Assignable scope:

Explanation:

Note: Assigning a custom RBAC role as the Management Group level is currently in preview only. So, for now the answer to the assignable scope is the subscription level.

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations>

<https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles>

<https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal#step-5-assignable-scopes>

QUESTION 275

Hotspot Question

You have an Azure subscription that contains the custom roles shown in the following table.

Name	Type
Role1	Azure Active Directory (Azure AD)
Role2	Azure subscription

In the Azure portal, you plan to create new custom roles by cloning existing roles. The new roles will be configured as shown in the following table.

Name	Type
Role3	Azure AD
Role4	Azure subscription

Which roles can you clone to create each new role? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Role3:

Role4:

Answer:

Answer Area

Role3:

Role4:

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/roles/custom-create>

<https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal>

QUESTION 276

Drag and Drop Question

You have an Azure subscription that contains the following resources:

- A network virtual appliance (NVA) that runs non-Microsoft firewall software and routes all outbound traffic from the virtual machines to the internet
- An Azure function that contains a script to manage the firewall rules of the NVA
- Azure Security Center standard tier enabled for all virtual machines
- An Azure Sentinel workspace
- 30 virtual machines

You need to ensure that when a high-priority alert is generated in Security Center for a virtual machine, an incident is created in Azure Sentinel and then a script is initiated to configure a firewall rule for the NVA.

How should you configure Azure Sentinel to meet the requirements? To answer, drag the appropriate components to the correct requirements. Each component 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.

Components	Answer Area
A data connector for Security Center	Enable alert notifications from Security Center: <input type="text" value="Component"/>
A data connector for the firewall software	Create an incident: <input type="text" value="Component"/>
A playbook	Initiate a script to configure the firewall rule: <input type="text" value="Component"/>
A rule	
A Security Events connector	
A workbook	

Answer:

Components	Answer Area
A data connector for the firewall software	Enable alert notifications from Security Center: A data connector for Security Center
	Create an incident: A rule
A Security Events connector	Initiate a script to configure the firewall rule: A playbook
A workbook	

Explanation:

<https://docs.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts>
<https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center>

QUESTION 277

Hotspot Question

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

Name	Type	Description
EventHub1	Azure Event Hubs	Not applicable
Adf1	Azure Data Factory	Not applicable
NVA1	Network virtual appliance (NVA)	The NVA sends security event messages in the Common Event Format (CEF).

You have an Azure subscription named Subscription2 that contains the following resources:

- An Azure Sentinel workspace
- An Azure Event Grid instance

You need to ingest the CEF messages from the NVAs to Azure Sentinel.

What should you configure for each subscription? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Subscription1:	<div>▼</div> <div>An Azure Log Analytics agent on a Linux virtual machine</div> <div>A Data Factory pipeline</div> <div>An Event Hubs namespace</div> <div>An Azure Service Bus queue</div>
Subscription2:	<div>▼</div> <div>A new Azure Log Analytics workspace</div> <div>A new Azure Sentinel data connector</div> <div>A new Azure Sentinel playbook</div> <div>A new Event Grid resource provider</div>

Answer:

Answer Area

Subscription1:	<div>▼</div> <div>An Azure Log Analytics agent on a Linux virtual machine</div> <div>A Data Factory pipeline</div> <div>An Event Hubs namespace</div> <div>An Azure Service Bus queue</div>
Subscription2:	<div>▼</div> <div>A new Azure Log Analytics workspace</div> <div>A new Azure Sentinel data connector</div> <div>A new Azure Sentinel playbook</div> <div>A new Event Grid resource provider</div>

QUESTION 278

SIMULATION

[AZ-500 Exam Dumps](#) [AZ-500 Exam Questions](#) [AZ-500 PDF Dumps](#) [AZ-500 VCE Dumps](#)

<https://www.braindump2go.com/az-500.html>

You need to ensure that the rg1lod10598168n1 Azure Storage account is encrypted by using a key stored in the KeyVault10598168 Azure key vault.

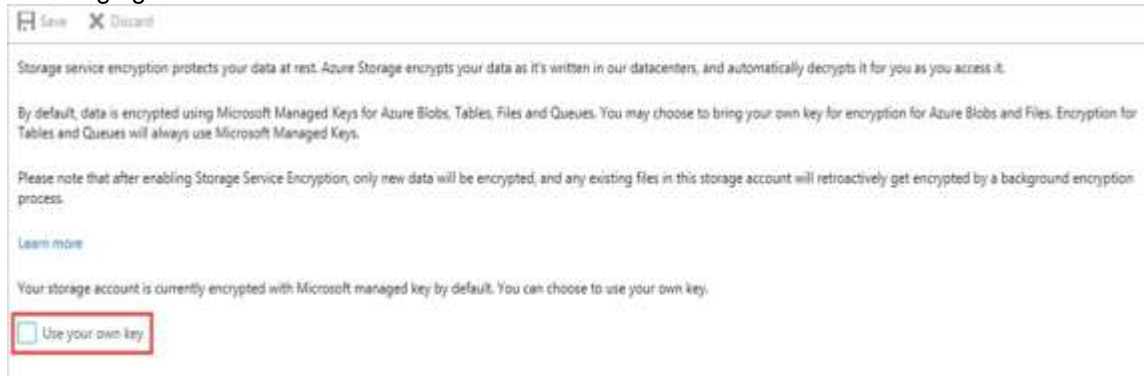
To complete this task, sign in to the Azure portal.

Answer: See the explanation below.

Explanation::

Step 1: To enable customer-managed keys in the Azure portal, follow these steps:

1. Navigate to your storage account rg1lod10598168n1
2. On the Settings blade for the storage account, click Encryption. Select the Use your own key option, as shown in the following figure.



Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters, and automatically decrypts it for you as you access it.

By default, data is encrypted using Microsoft Managed Keys for Azure Blobs, Tables, Files and Queues. You may choose to bring your own key for encryption for Azure Blobs and Files. Encryption for Tables and Queues will always use Microsoft Managed Keys.

Please note that after enabling Storage Service Encryption, only new data will be encrypted, and any existing files in this storage account will retroactively get encrypted by a background encryption process.

[Learn more](#)

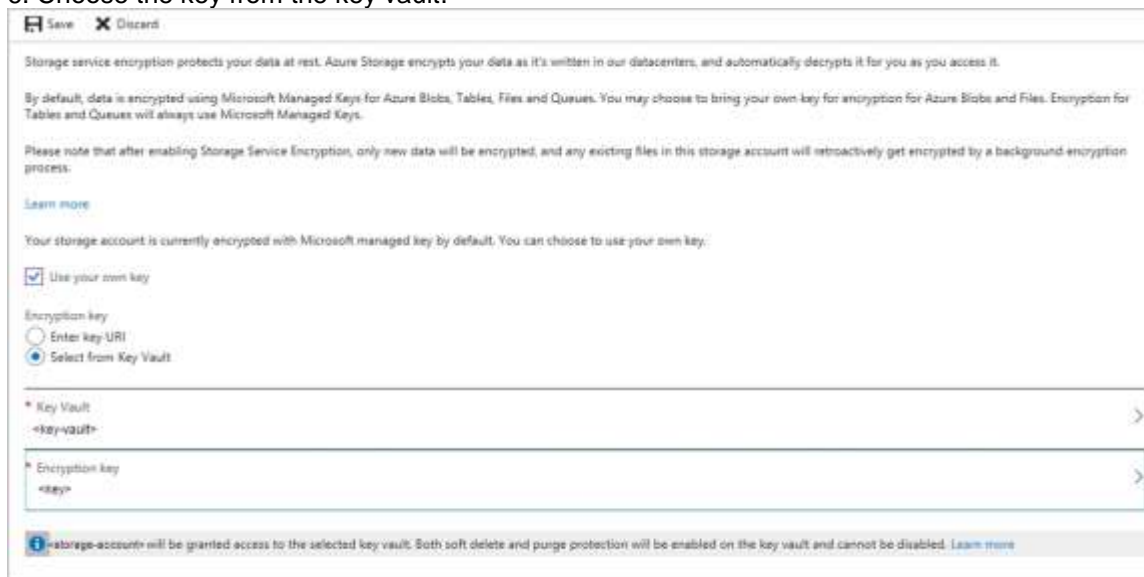
Your storage account is currently encrypted with Microsoft managed key by default. You can choose to use your own key.

☒ Use your own key

Step 2: Specify a key from a key vault

To specify a key from a key vault, first make sure that you have a key vault that contains a key. To specify a key from a key vault, follow these steps:

4. Choose the Select from Key Vault option.
5. Choose the key vault KeyVault10598168 containing the key you want to use.
6. Choose the key from the key vault.



Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters, and automatically decrypts it for you as you access it.

By default, data is encrypted using Microsoft Managed Keys for Azure Blobs, Tables, Files and Queues. You may choose to bring your own key for encryption for Azure Blobs and Files. Encryption for Tables and Queues will always use Microsoft Managed Keys.

Please note that after enabling Storage Service Encryption, only new data will be encrypted, and any existing files in this storage account will retroactively get encrypted by a background encryption process.

[Learn more](#)

Your storage account is currently encrypted with Microsoft managed key by default. You can choose to use your own key.

☒ Use your own key

Encryption key

☐ Enter key URI

☒ Select from Key Vault

* Key Vault
key-vault

* Encryption key
key

storage account will be granted access to the selected key vault. Both soft delete and purge protection will be enabled on the key vault and cannot be disabled. [Learn more](#)

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-encryption-keys-portal>