

PRACTICE QUESTIONS

Microsoft

SC-500

Microsoft Certified: Cloud and AI Security Engineer Associate

SHARED BY [u/quiet_robin_29](#) on aiexamcerts

EDITION	Free Set 1
QUESTIONS	10
SHARED	October 15, 2026
EXAM	Microsoft SC-500, Microsoft Certified: Cloud and AI Security Engineer Associate

Shared by u/quiet_robin_29 on aiexamcerts

10 practice questions for the Microsoft SC-500 exam, Microsoft Certified: Cloud and AI Security Engineer Associate, each followed by its answer and a short explanation. More free sets and the full practice exam: www.aiexamcerts.com/microsoft/sc-500. Spotted a mistake? Email support@aiexamcerts.com with the exam code SC-500 and the question number.

1. Which built-in Azure RBAC role lets a principal read secret values from a Key Vault without being able to change the vault configuration?
 - A Key Vault Reader on the vault
 - B Key Vault Secrets User
 - C Key Vault Contributor
 - D Reader

Answer: B

Key Vault Secrets User grants data-plane read access to secret contents, which is what an application needs at runtime. Key Vault Reader returns only vault metadata, and Key Vault Contributor manages the vault itself without granting access to secret data. The generic Reader role exposes resource properties but not the secret values inside the vault.

2. Blobs can be kept unchangeable for a fixed period by applying a time-based retention policy to a container with _____ storage enabled.

Answer: immutable

Immutable storage with a time-based retention policy, often described as write-once, read-many, prevents modification and deletion until the retention interval expires. The policy is applied to containers within the account. Soft delete recovers deleted blobs but does not block deletion, so it does not satisfy a write-once requirement.

3. A Conditional Access policy must require phishing-resistant multifactor authentication for every administrator sign-in. Which grant control should be configured?
 - A Require multifactor authentication
 - B Require Microsoft Entra hybrid joined device and a compliant state
 - C Require authentication strength set to Phishing-resistant MFA
 - D Require approved client app

Answer: C

Authentication strength lets the policy demand a class of method, and the built-in Phishing-resistant MFA strength accepts only methods such as FIDO2 security keys and Windows Hello for Business. The plain Require multifactor authentication grant accepts weaker methods such as SMS codes. Requiring a hybrid joined device is a device control and does not govern which authentication method the user performs.

4. Azure Front Door with a web application firewall can block malicious requests at the edge before they reach the origin, and the origin can be restricted to accept traffic only from Front Door.
- A True
 - B False

Answer: A (True)

Front Door terminates client connections at the edge and applies WAF rules there, so malicious requests are stopped before reaching the origin. Restricting the origin to Front Door traffic, for example with an access restriction that uses the AzureFrontDoor.Backend service tag, stops clients from bypassing the edge. Both controls are needed for the edge to be effective.

5. Which two actions help protect Azure SQL Database data at rest? (Choose two.)
- A Apply Dynamic Data Masking to a reporting view
 - B Enable Transparent Data Encryption with a customer-managed key in Key Vault
 - C Create a virtual network rule for the application subnet
 - D Use Always Encrypted for sensitive columns
 - E Enable active geo-replication to a paired region

Answer: B, D

Transparent Data Encryption with a customer-managed key protects database files and backups at rest, and Always Encrypted keeps selected columns encrypted inside the database. Dynamic Data Masking changes only what a user sees in query results. A virtual network rule restricts network access rather than encrypting stored data, and geo-replication improves availability without adding encryption.

6. A VM has no public IP address, and administrators need browser-based RDP or SSH access over TLS without exposing port 3389 or 22 to the internet. Which service fits best?
- A An Azure Load Balancer inbound NAT rule for port 3389
 - B Azure Bastion
 - C A public IP address with an NSG rule allowing port 3389 from Any
 - D Azure Front Door with a WAF policy

Answer: B

Azure Bastion provides managed RDP and SSH sessions through the Azure portal over TLS, so the VM needs no public IP and no management port is exposed. An inbound NAT rule or an open NSG rule on a public IP exposes the management port directly to the internet. Azure Front Door serves HTTP and HTTPS application traffic, so it cannot provide RDP access.

7. A policy must automatically deploy a missing diagnostic setting to each supported resource that lacks one. Which Azure Policy effect fits?
- A DeployIfNotExists
 - B Audit
 - C Deny
 - D Disabled

Answer: A

DeployIfNotExists evaluates resources and, when the related configuration is missing, deploys it using a template and a managed identity. Audit only reports noncompliance and does not fix anything. Deny blocks a deployment that does not comply, and Disabled turns the rule off, so neither remediates existing resources.

8. Microsoft Defender for Cloud includes Cloud Security Posture Management, abbreviated as _____, which provides posture recommendations and attack path analysis.

Answer: CSPM

CSPM stands for Cloud Security Posture Management, the Defender for Cloud capability that assesses configuration, produces recommendations, and maps attack paths. The Defender CSPM plan adds features such as attack path analysis and governance rules on top of the free foundational posture. Confusing it with workload protection, which covers servers and containers, is a common error.

9. Which Microsoft Sentinel component stores a reference list, such as VIP users or approved IP ranges, that analytics rules can query?
- A Workbook
 - B Watchlist
 - C Hunting bookmark
 - D Incident task

Answer: B

A watchlist is a reference dataset uploaded to the workspace and queried with a lookup in KQL, which makes it useful for allowlists and VIP lists. Workbooks are visual dashboards rather than reference data. Hunting bookmarks save query results for later investigation, and incident tasks track analyst work items.

10. An analyst wants to search 90 days of historical logs for a suspicious IP address without creating an alert. Which Sentinel feature fits?
- A Scheduled analytics rules
 - B Automation rules
 - C Hunting queries
 - D Fusion detections

Answer: C

Hunting queries are KQL searches that run on demand against historical data and do not create alerts unless an analyst promotes a finding. Scheduled analytics rules generate alerts on a cadence, which is the wrong tool for ad hoc exploration. Automation rules act on incidents, and Fusion is a detection that correlates signals automatically.