

PRACTICE QUESTIONS

Microsoft

SC-500

Microsoft Certified: Cloud and AI Security Engineer Associate

SHARED BY [u/swiftyak1995](#) on aiexamcerts

EDITION	Free Set 2
QUESTIONS	10
SHARED	October 15, 2026
EXAM	Microsoft SC-500, Microsoft Certified: Cloud and AI Security Engineer Associate

Shared by [u/swiftyak1995](#) 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. An Azure virtual machine must call Microsoft Graph and an Azure SQL database, and the team wants Azure to rotate the credentials automatically. Which identity type fits best?
 - A A service principal with a password that is rotated manually
 - B A service principal with a certificate that is renewed manually
 - C An app registration with a client secret stored in Key Vault
 - D A managed identity assigned to the virtual machine

Answer: D

Managed identities are created and rotated by Microsoft Entra ID, so the workload never handles a secret that someone has to maintain. A service principal with a manually rotated password or a manually renewed certificate adds a credential that the team must track and renew. A client secret kept in Key Vault is still a secret that someone has to maintain, since the app needs a credential to reach the vault.

2. Microsoft Sentinel stores its data in a separate database, so Log Analytics retention settings for the workspace do not apply to Sentinel data.
 - A True
 - B False

Answer: B (False)

Sentinel is built on Log Analytics, and the tables it queries live in the workspace, so the workspace retention and archive configuration applies. Retention is therefore set in the workspace rather than in a separate Sentinel store. The statement is false because the data does not sit in a separate database.

3. Which feature gives a workload in a virtual network a private IP address for an Azure SQL database, so that the connection stays on the private network?
 - A A service endpoint
 - B A public endpoint restricted by a firewall IP rule
 - C A private endpoint
 - D A VNet peering connection to the database region

Answer: C

A private endpoint creates a network interface with a private IP address in your subnet that maps to the database, so connections stay on the private network. A service endpoint extends the virtual network identity to the service, but the database still uses its public address. A firewall rule on a public endpoint still accepts traffic on that public address.

4. Microsoft Sentinel queries workspace data with the _____ Query Language, also known as KQL.

Answer: Kusto

KQL is the query language used by Log Analytics and Microsoft Sentinel, and it takes its name from the Kusto engine behind them. Analytics rules, hunting queries, and workbooks all use it. Languages such as T-SQL are not used for workspace log queries.

5. Which two controls reduce data exposure when an Azure AI Foundry project calls an Azure OpenAI model? (Choose two.)

- A Enable public network access from all IP addresses
- B Deploy the model in a region closer to the users
- C Use a private endpoint for the Azure OpenAI resource
- D Share one API key across all developers
- E Disable local key-based authentication on the resource

Answer: C, E

A private endpoint keeps calls on the private network, and disabling local authentication forces callers to use Microsoft Entra ID tokens. Public access from all addresses widens exposure, and choosing a region closer to users affects latency rather than data exposure. A shared API key removes accountability for who made each call.

6. Which SQL feature keeps selected column values encrypted so that the database engine never sees the plaintext, even for a highly privileged administrator?

- A Always Encrypted
- B Transparent Data Encryption
- C Dynamic Data Masking
- D SQL auditing

Answer: A

Always Encrypted encrypts sensitive columns on the client side, and the keys stay outside the database engine, so administrators see only ciphertext for those columns. Transparent Data Encryption protects files and backups at rest but decrypts data for any authorized query. Dynamic Data Masking only hides values in query results and does not encrypt stored data.

7. Which storage account setting makes the service reject requests that arrive over unencrypted HTTP?
- A Enable blob versioning to keep earlier object copies
 - B Require secure transfer for REST API operations
 - C Set the minimum TLS version to 1.0
 - D Enable soft delete for containers

Answer: B

Requiring secure transfer makes the storage service reject requests that do not use HTTPS, which protects data in transit. Blob versioning keeps earlier copies of an object and has no effect on the transport. A minimum TLS version of 1.0 weakens protection, and soft delete recovers deleted containers without encrypting traffic.

8. Azure AI Content Safety can classify text against harm categories such as hate, sexual, violence, and self-harm, and it reports a severity level for each detection.
- A True
 - B False

Answer: A (True)

Content Safety returns a category and a severity level for each harm category it detects, so a policy can set different thresholds per category. Applications use those thresholds to block, flag, or send content for review. The output is a graded score rather than a simple yes or no.

9. Which Defender for Cloud plan adds malware scanning for files uploaded to Azure Blob Storage?
- A Defender for SQL
 - B Defender for Storage
 - C Defender for DNS
 - D Defender for Containers

Answer: B

Defender for Storage includes malware scanning of uploaded blobs along with threat detection for storage accounts. Defender for SQL protects database workloads, and Defender for DNS monitors DNS queries. Defender for Containers covers Kubernetes and container registries, so it does not scan blob uploads.

10. Which Defender for Servers capability limits management port access to a VM for a set time after an approved request?
- A Adaptive network hardening
 - B File integrity monitoring
 - C Just-in-time VM access
 - D Adaptive application controls

Answer: C

Just-in-time VM access opens management ports for a limited time after a request is approved, then closes them automatically. Adaptive network hardening recommends tighter NSG rules but does not open ports on demand. File integrity monitoring tracks changes to files and registry keys, and adaptive application controls allow only approved executables.