

PRACTICE QUESTIONS

Microsoft

SC-100

Microsoft Cybersecurity Architect Expert

SHARED BY [u/Cosmic-Summit-1493](#) on aiexamcerts

EDITION Free Set 2

QUESTIONS 10

SHARED October 15, 2026

EXAM Microsoft SC-100, Microsoft Cybersecurity Architect Expert

Shared by u/Cosmic-Summit-1493 on aiexamcerts

10 practice questions for the Microsoft SC-100 exam, Microsoft Cybersecurity Architect Expert, each followed by its answer and a short explanation. More free sets and the full practice exam:

www.aiexamcerts.com/microsoft/sc-100. Spotted a mistake? Email support@aiexamcerts.com with the exam code SC-100 and the question number.

1. Which Microsoft Entra Conditional Access grant control allows access only from devices that Microsoft Intune reports as compliant?

- A Require device to be marked as compliant
- B Require a password change for high-risk users
- C Exclude the user from the policy
- D Session sign-in frequency

Answer: A

The device compliance grant control checks the compliance state reported by Intune or another compliance provider before granting access. Session sign-in frequency is the tempting distractor because it is device-related in many policies, but it is a session control that limits how often users sign in and does not check device state. Excluding a user removes the policy rather than enforcing anything.

2. Microsoft Purview data loss prevention policies can enforce rules on content in Exchange Online, SharePoint Online and Microsoft Teams.

- A True
- B False

Answer: A (True)

This is true. Data loss prevention policies cover Exchange, SharePoint, OneDrive and Teams, and they can warn, block or audit when sensitive content is shared against policy. Sensitivity labels are the tempting distractor because they also protect content, but they classify and encrypt rather than running sharing-detection rules.

3. An application uses Azure OpenAI to answer questions over company documents. Which control most directly reduces the risk of prompt injection reaching the model?

- A Relying on a longer system prompt alone
- B Raising the temperature setting
- C Enabling Prompt Shields in Azure AI Content Safety
- D Disabling diagnostic logging

Answer: C

Prompt Shields analyzes user prompts and documents for jailbreak attempts and indirect prompt injection before the model acts on them. A longer system prompt is the tempting distractor, but instructions in the prompt can be overridden by injected text. Temperature only changes output randomness and disabling logging removes evidence without adding protection.

4. In Microsoft Sentinel, a _____ analytics rule runs a KQL query on a fixed schedule and creates alerts when results match.

Answer: scheduled

A scheduled analytics rule runs its KQL query at a defined frequency over a lookback window and generates alerts that can become incidents. Near-real-time rules are the tempting distractor because they run continuously against incoming events, which is a different rule type. Fusion rules correlate multistage attacks using machine learning rather than a fixed query.

5. Which two controls help enforce least privilege for Azure administrators? (Choose two.)

- A Permanent Global Administrator assignment for senior IT staff
- B Microsoft Entra Privileged Identity Management eligible role assignments
- C Network security group rules on the management subnet
- D Azure role-based access control with custom roles scoped to a resource group
- E Azure Firewall application rules for outbound traffic

Answer: B, D

Eligible assignments in Privileged Identity Management give just-in-time elevation with approval and expiry, and scoped custom roles limit permissions to the resources a task needs. Permanent Global Administrator assignment is the tempting distractor because it is convenient, but it grants standing tenant-wide privilege. Network security group rules and Azure Firewall application rules filter traffic but do not limit what an administrator is permitted to do.

6. A Sentinel analyst wants to search many days of logs for a pattern that no existing alert covers. Which feature should be used?

- A Scheduled analytics rule
- B Automation rule
- C Data connector
- D Hunting query

Answer: D

Hunting queries are KQL searches that analysts run on demand to look for threats that existing detections do not cover. Scheduled analytics rules are the tempting distractor, but they run on a schedule and raise alerts for known patterns. Automation rules respond to incidents and data connectors only bring logs into the workspace.

7. Which Azure Firewall SKU is required for TLS inspection of outbound HTTPS traffic?
- A Basic
 - B Premium
 - C Standard
 - D Standard with network rules only

Answer: B

TLS inspection is a Premium SKU capability that decrypts and inspects outbound HTTPS traffic. Standard is the tempting distractor because it includes FQDN filtering and threat intelligence, but it does not decrypt traffic. Basic is designed for small workloads and lacks these advanced inspection features.

8. Under the EU AI Act, obligations for high-risk AI systems fall only on the organizations that deploy them.
- A True
 - B False

Answer: B (False)

This is false. The Act assigns obligations to providers who develop or place systems on the market, and to deployers who use them, along with others in the supply chain. Deployers-only is the tempting misreading, since operators do have duties such as human oversight and monitoring.

9. A CISO asks who changed a firewall rule in an Azure subscription last week. Which log should be queried first?
- A Microsoft Entra sign-in logs
 - B Azure Monitor platform metrics
 - C Azure Activity log
 - D Network Watcher flow logs

Answer: C

The Azure Activity log records control-plane operations such as create, update and delete on Azure resources, including the identity that made each change. Microsoft Entra sign-in logs are the tempting distractor because they also show who acted, but they record authentication events rather than resource changes. Flow logs record network traffic and metrics record performance values.

10. A database subnet should accept traffic only from the application subnet on port 1433. Which control is the most direct fit?
- A Azure Bastion for admin sessions
 - B Network security group inbound rule allowing TCP 1433 from the application subnet
 - C Public IP with port forwarding
 - D Azure DDoS Protection plan

Answer: B

A network security group inbound rule scoped to the application subnet's address range and TCP port 1433 enforces exactly this rule on the database subnet. A public IP with port forwarding is the tempting distractor, but it exposes the database to the internet. Azure Bastion is for administrative sessions and DDoS Protection defends against volumetric floods.