

PRACTICE QUESTIONS

Microsoft

SC-100

Microsoft Cybersecurity Architect Expert

SHARED BY [u/frosty_gecko_91](#) on aiexamcerts

EDITION Free Set 1

QUESTIONS 10

SHARED October 15, 2026

EXAM Microsoft SC-100, Microsoft Cybersecurity Architect Expert

Shared by [u/frosty_gecko_91](#) 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 Azure Key Vault object type is used for cryptographic operations such as signing and encryption, where applications call the vault rather than retrieve the key itself?

- A Keys
- B Secrets
- C Certificates
- D Access policies

Answer: A

Keys in Key Vault are used for cryptographic operations, and applications can ask the vault to sign or encrypt on their behalf. Secrets are the tempting distractor because they are also stored in the vault, but a secret is returned to the caller as a value. Certificates bundle a key with X.509 metadata, and access policies only define permissions.

2. Audit reports such as ISO and SOC for Microsoft cloud services are published in the _____ Portal.

Answer: Service Trust (also accepted: Microsoft Service Trust)

The Microsoft Service Trust Portal publishes independent audit reports, certifications and compliance documentation for Microsoft cloud services. Architects use it as evidence when assessing a cloud provider's controls for a customer's own compliance program. The Microsoft Compliance Manager is a different tool that maps those controls to a customer's assessments.

3. An architect must restrict outbound internet access from spoke virtual networks to approved fully qualified domain names through one central control point. Which service fits best?

- A Network security group with service tags
- B Azure Bastion
- C Azure Firewall with application rules
- D Azure DDoS Protection

Answer: C

Azure Firewall application rules filter outbound traffic by FQDN and can be deployed centrally in a hub. A network security group with service tags is the tempting distractor, but service tags represent groups of IP ranges and do not provide FQDN filtering. Azure Bastion manages administrative sessions and Azure DDoS Protection mitigates volumetric attacks, so neither controls outbound destinations.

4. Azure Firewall makes network security groups unnecessary on individual subnets.
- A True
 - B False

Answer: B (False)

This is false. Azure Firewall inspects traffic at the hub boundary, while network security groups enforce rules directly on subnets and network interfaces, so Microsoft recommends using both for defense in depth. Network security groups are the tempting thing to drop, but removing them leaves east-west traffic inside a subnet unfiltered.

5. Which two Azure SQL Database features help protect sensitive data? (Choose two.)
- A Transparent data encryption
 - B Azure Bastion session management
 - C Always Encrypted
 - D Azure Front Door caching
 - E Azure Traffic Manager profiles

Answer: A, C

Transparent data encryption protects data at rest, and Always Encrypted keeps selected columns encrypted so the database engine never sees plaintext. Bastion, Front Door and Traffic Manager are networking services and do not protect data within the database.

6. Which Microsoft Defender for Endpoint capability cuts a compromised device off from the network while keeping its connection to the Defender service?
- A Attack surface reduction rules
 - B Device isolation
 - C Live response sessions
 - D Intune compliance policy

Answer: B

Device isolation restricts the device's network communication to the Defender for Endpoint service, which contains lateral movement while analysts investigate. Live response is the tempting distractor because it lets analysts run commands on the device, but it does not cut network access. Attack surface reduction rules prevent risky behavior rather than containing an active compromise.

7. Which Microsoft Sentinel data connector is recommended for ingesting Microsoft Entra ID sign-in and audit logs without writing custom code?
- A Custom log collector API fed by your own script
 - B Azure Monitor Agent on a file share
 - C Azure Logic Apps HTTP trigger
 - D Microsoft Entra ID built-in connector

Answer: D

The Microsoft Entra ID data connector is built into Sentinel and ingests sign-in and audit logs with no custom development. The custom log collector API is the tempting distractor because it can ingest any data, but it requires building and maintaining code. The Azure Monitor Agent collects host-based logs from machines rather than cloud identity logs.

8. Just-in-time VM access is a capability of the Microsoft Defender for _____ plan.

Answer: Servers

Just-in-time VM access is part of the Defender for Servers plan, where it temporarily opens management ports for approved users. Defender for Storage is a tempting distractor because it protects Azure resources too, but it covers storage account activity and malware, not virtual machine ports. Defender for Containers covers Kubernetes and container images.

9. Which Microsoft tool provides prebuilt assessments and improvement actions mapped to regulations such as ISO 27001 and NIST SP 800-53?
- A Microsoft Entra access reviews
 - B Microsoft Purview Audit
 - C Microsoft Purview Compliance Manager
 - D Azure Advisor

Answer: C

Compliance Manager provides assessments, controls and improvement actions mapped to regulations and standards, and it tracks compliance over time. Microsoft Purview Audit is the tempting distractor because it is a compliance product, but it records user and admin activity rather than mapping controls to regulations. Entra access reviews recertify access and Azure Advisor gives general recommendations.

10. Which Azure Policy effect should an architect use to stop a resource from being created when it breaks a rule?
- A Deny
 - B Audit
 - C AuditIfNotExists
 - D DeployIfNotExists

Answer: A

The Deny effect blocks a non-compliant request at creation or update time. Audit is the tempting distractor because it flags noncompliance, but it only records it and lets the resource exist. DeployIfNotExists adds a related resource when one is missing rather than blocking the request.