

## PRACTICE QUESTIONS

Microsoft

# SC-300

Microsoft Identity and Access Administrator Associate

SHARED BY [u/Loyal-Falcon-8260](#) on aiexamcerts

|           |                                                                         |
|-----------|-------------------------------------------------------------------------|
| EDITION   | Free Set 2                                                              |
| QUESTIONS | 10                                                                      |
| SHARED    | October 15, 2026                                                        |
| EXAM      | Microsoft SC-300, Microsoft Identity and Access Administrator Associate |

---

Shared by u/Loyal-Falcon-8260 on aiexamcerts

10 practice questions for the Microsoft SC-300 exam, Microsoft Identity and Access Administrator Associate, each followed by its answer and a short explanation. More free sets and the full practice exam: [www.aiexamcerts.com/microsoft/sc-300](https://www.aiexamcerts.com/microsoft/sc-300). Spotted a mistake? Email [support@aiexamcerts.com](mailto:support@aiexamcerts.com) with the exam code SC-300 and the question number.

1. A user reports repeated Microsoft Authenticator prompts that they did not start. Which setting limits this MFA fatigue risk by requiring the user to type a number shown on the sign-in screen?
  - A Number matching
  - B Biometric unlock only
  - C Additional context showing the application and location
  - D Push notification approval only

**Answer: A**

Number matching makes the user type the number displayed on the sign-in screen into the app, so an attacker who triggers prompts cannot get approval by a simple tap. Biometric unlock protects the device but does not change the approval step, and additional context only shows the app and location without requiring a typed number. Push approval alone is the pattern that fatigue attacks exploit.

2. Legacy authentication protocols such as IMAP and POP3 support multifactor authentication, so a Conditional Access policy does not need to block them.
  - A True
  - B False

**Answer: B (False)**

Legacy protocols do not support modern authentication, so a password alone can be used to sign in and MFA cannot be enforced on them. A Conditional Access policy that targets legacy client apps blocks those sign-ins. Assuming MFA covers legacy protocols is the mistake this statement invites.

3. Which enterprise application property hides the app from users' My Apps portal?
  - A User assignment required setting turned on
  - B Automatic provisioning mode set to manual
  - C Single sign-on mode
  - D Visible to users setting turned off

**Answer: D**

Turning off the visible to users setting keeps the application out of the My Apps portal while it can still be assigned and used. User assignment required controls who can sign in, not whether the app is shown. Provisioning and single sign-on mode do not change portal visibility.

4. An application registration can use a federated identity credential so that it trusts tokens from an external identity provider instead of a stored \_\_\_\_\_.

**Answer: client secret** (also accepted: secret)

A federated identity credential removes the need to store a client secret for supported providers such as GitHub Actions, because the external token is exchanged for an Entra token. The trust is scoped to a specific subject. Secrets still need rotation wherever they remain in use.

5. Which two actions help secure privileged administrator accounts? (Choose two.)

- A Assign privileged roles through PIM as eligible assignments
- B Sync administrator accounts from on-premises Active Directory
- C Assign Global Administrator to every IT technician
- D Require phishing-resistant MFA for administrator accounts
- E Extend the sign-in frequency for administrators to 90 days

**Answer: A, D**

Eligible assignments through Privileged Identity Management keep privileged roles inactive until they are needed, and phishing-resistant MFA protects those accounts from credential theft. Syncing administrators from on-premises Active Directory exposes cloud roles to on-premises compromise, while broad Global Administrator assignments and a 90-day sign-in frequency both widen the attack surface.

6. Which Privileged Identity Management approach lets a global administrator use an admin role only when needed, with MFA and justification each time?

- A A permanent active assignment for the role
- B A Conditional Access policy that requires MFA for the role
- C A role-assignable group with permanent membership
- D An eligible assignment in Privileged Identity Management

**Answer: D**

An eligible assignment lets the administrator activate the role for a limited time after completing MFA and giving a justification. A permanent active assignment keeps the privilege on at all times. A Conditional Access policy requires MFA but does not make the role inactive until needed, and permanent group membership keeps the privilege on at all times.

7. Which Microsoft Entra feature lets an external partner user sign in to a company's apps using their own organization account?
- A B2B collaboration
  - B B2C custom policies
  - C Application proxy connector
  - D Local guest accounts with passwords

**Answer: A**

B2B collaboration invites external users into the tenant as guest accounts that sign in with their home identity. B2C is designed for customer identities rather than partner staff. Application Proxy publishes on-premises web apps, and local guest passwords are not a Microsoft Entra feature.

8. Managed identities let Azure workloads access resources without credentials in code, and Microsoft rotates the underlying credentials automatically.
- A True
  - B False

**Answer: A (True)**

A managed identity is backed by a service principal that Azure manages, and the platform handles credential issuance and rotation. The workload requests tokens from the local endpoint without any secret in its configuration. This removes a whole class of leaked-credential risk.

9. An AI agent app must call Microsoft Graph on behalf of a signed-in user. Which permission type is needed?
- A Application permission
  - B Delegated permission
  - C Owner role assignment
  - D Guest permission

**Answer: B**

Delegated permissions are used when an app acts on behalf of a signed-in user, and the effective access is limited to what that user can reach. Application permissions act without a user and would give the agent broader reach than intended. Role assignments and guest accounts are not API permission types.

10. Which Microsoft Entra report lists users flagged for suspicious activity by Identity Protection?

- A Usage and insights report
- B Risky users report
- C Sign-in activity export
- D Provisioning activity report

**Answer: B**

The risky users report lists users that Identity Protection has flagged, along with their risk level, so administrators can investigate or remediate. The usage and insights report summarizes activity volume. A sign-in activity export and provisioning reports do not carry risk classifications.