

PRACTICE QUESTIONS

Microsoft

SC-300

Microsoft Identity and Access Administrator Associate

SHARED BY [u/rustic_bison_43](#) on aiexamcerts

EDITION	Free Set 1
QUESTIONS	10
SHARED	October 15, 2026
EXAM	Microsoft SC-300, Microsoft Identity and Access Administrator Associate

Shared by u/rustic_bison_43 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. Spotted a mistake? Email support@aiexamcerts.com with the exam code SC-300 and the question number.

1. Which authentication strength should be required for administrators who must sign in only with FIDO2 security keys or Windows Hello for Business?

- A Passwordless MFA
- B Multifactor authentication
- C Phishing-resistant MFA
- D Password plus SMS verification

Answer: C

The built-in Phishing-resistant MFA strength accepts only FIDO2 security keys, Windows Hello for Business, and certificate-based authentication. Passwordless MFA is broader and also accepts methods such as Microsoft Authenticator phone sign-in, so it does not restrict sign-in to the methods named. A plain multifactor authentication requirement accepts weaker second factors.

2. Users can reset their own forgotten passwords when Microsoft Entra _____ password reset is enabled for them.

Answer: self-service (also accepted: self service)

Self-service password reset lets users reset passwords and unlock accounts after registering their authentication methods, which reduces help desk calls. Administrators choose which users or groups can use it. Users who have not registered methods cannot complete a reset on their own.

3. A user must sign in with a passkey stored on a physical security key. Which authentication method must be enabled for that sign-in?

- A SMS sign-in
- B Temporary Access Pass only
- C Voice call verification
- D FIDO2 security key

Answer: D

The FIDO2 security key method in the authentication methods policy allows passkeys stored on hardware keys to be registered and used for sign-in. SMS sign-in and voice calls are phone-based methods and are not passkeys on a hardware key. A Temporary Access Pass is a time-limited passcode for registration, not a passkey.

4. A service principal is the local representation of an application in a tenant, and an app registration is the global definition of that application.
- A True
 - B False

Answer: A (True)

An app registration defines the application and its settings, and it is the global object that the publishing tenant owns. A service principal is created in each tenant that uses the application and holds local permissions and assignments. Confusing the two is a common cause of consent and assignment problems.

5. Which two sign-in methods can Microsoft Entra Connect Sync configure for hybrid identities? (Choose two.)
- A Hardware token synchronization
 - B FIDO2 security key registration
 - C Password hash synchronization
 - D Certificate-based authentication policy
 - E Pass-through authentication

Answer: C, E

Password hash synchronization copies a hash of the on-premises password to Entra ID, and pass-through authentication validates the password against on-premises Active Directory through an agent. Hardware token synchronization is not a Connect Sync option, and FIDO2 key registration and certificate-based authentication policy are managed in Entra ID itself rather than configured by Entra Connect Sync.

6. Which consent setting stops users from approving third-party apps that request broad permissions, while still letting them ask an administrator for review?
- A User consent for all apps
 - B Guest sign-in only
 - C Admin consent workflow
 - D Tenant restrictions v2

Answer: C

The admin consent workflow blocks user consent for apps that require admin approval and sends the request to a reviewer. Allowing user consent for all apps lets users grant broad access without review. Guest sign-in and tenant restrictions control other scenarios and do not govern app consent.

7. Which entitlement management object bundles groups, apps, and SharePoint sites that users can request together?
- A Access review definition
 - B Dynamic group rule
 - C Access package
 - D Conditional Access template

Answer: C

An access package bundles resources such as groups, applications, and SharePoint sites, and users request the package as one unit. An access review definition schedules a review of existing access. A dynamic group rule sets membership based on attributes, and a Conditional Access template sets policy conditions.

8. Workload identity _____ lets a GitHub Actions workflow obtain Microsoft Entra tokens without storing a client secret.

Answer: federation (also accepted: federated identity)

Workload identity federation trusts short-lived OIDC tokens from GitHub, which are exchanged for Microsoft Entra tokens during the workflow run. No long-lived secret needs to be stored in the repository. The federated credential can be scoped to a repository, branch, or environment.

9. A workload must read blobs in an Azure Storage account using its managed identity. Which role is the least privileged option that allows reading blob data?
- A Storage Blob Data Reader
 - B Storage Blob Data Owner
 - C Reader
 - D Storage Queue Data Reader

Answer: A

Storage Blob Data Reader grants read access to blob data, which is the minimum needed here. Storage Blob Data Owner also allows changes and POSIX ACL management, which is too broad. The generic Reader role covers management-plane metadata only, and Storage Queue Data Reader reads queues rather than blobs.

10. Which Microsoft Entra log shows sign-ins made by a service principal or managed identity?
- A Service principal sign-in logs
 - B Audit logs for directory changes
 - C Provisioning logs for sync activity
 - D Interactive user sign-in logs

Answer: A

Service principal sign-in logs record authentication by workloads, including managed identities, which the interactive user sign-in log does not show. Audit logs record directory changes, and provisioning logs record account synchronization activity. Those logs do not show token requests from workloads.