4. Security and compliance

└ 4.1 Authentication and authorization

└ 4.1.1 Choose: Service Principals, Managed Identity

---

1. What is a Service Principal in Azure and when should it be used?
2. What is a Managed Identity and what types are available?
3. What are the main differences between Service Principals and Managed Identities?
4. In which scenarios is a Service Principal preferred over Managed Identity?
5. When should you use a Managed Identity instead of a Service Principal?
6. How are credentials managed for Service Principals versus Managed Identities?
7. What are the security best practices for Service Principals?
8. What are the security advantages of Managed Identities?
9. How do you grant permissions to a Service Principal and a Managed Identity?
10. What is the process to rotate credentials for Service Principals and Managed Identities?

---

1. **What is a Service Principal in Azure and when should it be used?**

A Service Principal is an identity created for use

- with applications,
- hosted services,
- and automation tools

to access Azure resources. Use it when you need an application or script to authenticate and operate independently of user context.

---

2. **What is a Managed Identity and what types are available?**

An automatically managed identity in Azure AD for Azure resources. Two types exist:

- *system-assigned* (tied to a single resource)
- and *user-assigned* (independent, reusable across resources).

---

3. **What are the main differences between Service Principals and Managed Identities?**

- Service Principals require manual credential management (client secrets or certificates) and can be used outside Azure.
- Managed Identities have automatic credential rotation, no secret exposure, and only work within supported Azure services.

---

4. **In which scenarios is a Service Principal preferred over Managed Identity?**

Use a Service Principal

- when accessing Azure resources from outside Azure,
- in cross-cloud or on-premises scenarios,
- or when granular control over authentication lifecycle is required.

---

5. **When should you use a Managed Identity instead of a Service Principal?**

Use a Managed Identity when your workload runs entirely on Azure and needs secure, automated authentication to Azure resources—eliminating secret management.

6. **How are credentials managed for Service Principals versus Managed Identities?**
   - Service Principals require explicit secret/certificate creation, storage, and rotation.
   - Managed Identities handle credential mgmt. & rotation automatically, exposing no secrets.

---

7. **What are the security best practices for Service Principals?**
   - Use the least-privilege principle,
   - regularly rotate secrets/certificates,
   - use certificate-based authentication over client secrets,
   - restrict access with conditional access policies,
   - and store secrets in Azure Key Vault.

---

8. **What are the security advantages of Managed Identities?**
Managed Identities
   - remove the need to handle credentials,
   - provide automatic credential rotation,
   - and limit exposure of secrets,
   - reducing the risk of leaks or misuse.

---

9. **How do you grant permissions to a Service Principal and a Managed Identity?**
Assign the required Azure RBAC role to the Service Principal or Managed Identity at the correct scope (subscription, resource group, or resource level) via the Azure portal, CLI, or PowerShell.

---

10. **What is the process to rotate credentials for Service Principals and Managed Identities?**
For Service Principals, manually update secrets or certificates and update applications to use the new credentials. For Managed Identities, Azure handles rotation automatically—no manual action required.