Service Principal – Notes

A **Service Principal** is a security identity used by applications, services, or automation tools to access Azure resources securely. It functions as an identity with specific permissions to interact with Azure services without using a user's credentials.

Key Features

- **Secure Authentication**: Provides a way for applications to authenticate without user credentials.
- **Granular Permissions**: Access can be controlled through **Azure Role-Based Access Control (RBAC)**.
- **Used in Automation**: Essential for CI/CD pipelines, infrastructure as code (IaC), and DevOps tasks.
- **Supports Secret Management**: Can use **certificates, client secrets, or managed identities**.

How to Create a Service Principal

1. Using Azure Portal

1. Go to **Azure Active Directory** → **App registrations**.
2. Click on **New registration**.
3. Provide a **name**, select account type, and click **Register**.
4. Navigate to **Certificates & secrets** to generate a client secret.
5. Copy the **Client ID, Tenant ID, and Secret** for authentication.

2. Using Azure CLI

```
az ad sp create-for-rbac --name "MyServicePrincipal" --role Contributor
```

3. Using PowerShell

```
New-AzADServicePrincipal -DisplayName "MyServicePrincipal" -Role Contributor
```

Best Practices

✓ Use **least privilege** access for security. ✓ Rotate **secrets and certificates** regularly. ✓ Use **Managed Identities** when possible. ✓ Monitor service principal activity using **Azure Monitor**.

Use Cases

- Automating deployments in **Azure DevOps**.
- Managing **Azure resources** in a secure manner.

- Enabling authentication for **third-party applications**.
- Running **Terraform, Ansible, or Bicep** scripts securely.

By using a **Service Principal**, organizations can ensure secure and efficient management of Azure resources without relying on user credentials.