**What is Service principle**

**Service Principal** is an application within Microsoft Entra ID, which is authorized to access resources in Azure. This access is restricted by the roles assigned to the service principal, giving you control over which resources can be accessed and at which level.

**Key Concepts of a Service Principal**

1. **Identity for Applications and Services**: Service principals are used by applications or automated processes to authenticate and interact with Azure resources. Instead of using a user's credentials, which is not secure or scalable, a service principal provides a secure mechanism to control access.
2. **Role-Based Access Control (RBAC)**: Service principals are assigned roles that determine their level of access to Azure resources. This ensures that the principle of least privilege is enforced, limiting the actions the service principal can perform based on the assigned role.
3. **Credentials**: A service principal has credentials that the application or service uses to authenticate. These credentials include:
   * **Client ID (Application ID)**: A unique identifier for the service principal.
   * **Client Secret (Password)**: A password or key associated with the service principal.
   * **Tenant ID**: The Azure Active Directory (AAD) tenant in which the service principal is created.
4. **Security**: Using service principals enhances security by enabling fine-grained access control and auditing of what the application or service is doing. Credentials can be rotated without affecting the users and their access.

**Step 1: Set Up an Azure Service Principal**

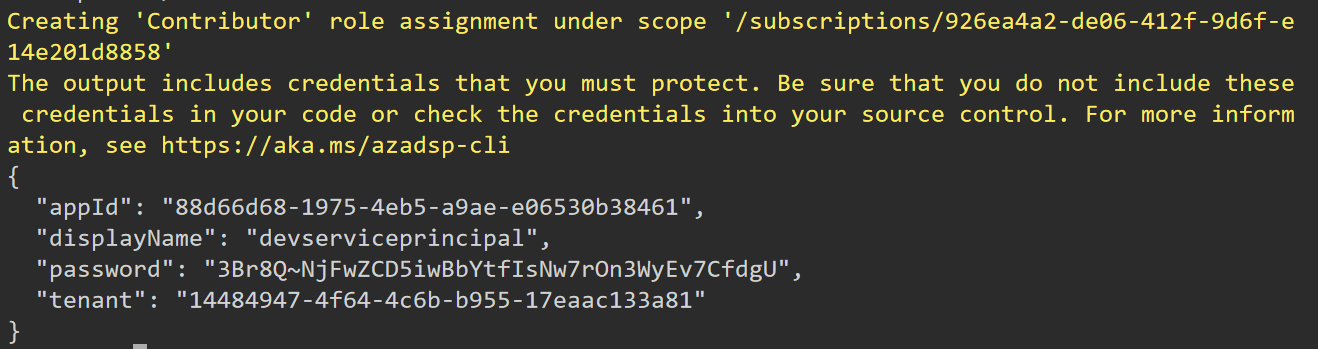
To establish a secure connection, you'll need a service principal in your Azure Active Directory (AAD) with the necessary permissions.

**Using Azure CLI**

1. **Open Azure Cloud Shell** or your local terminal with Azure CLI installed.
2. **Create a Service Principal**:

az ad sp create-for-rbac --name <service-principal-name> --role Contributor --scopes /subscriptions/<subscription-id>

az ad sp create-for-rbac --name devserviceprincipal --role Contributor --scopes /subscriptions/926ea4a2-de06-412f-9d6f-e14e201d8858



**Step 2: Create a Service Connection in Azure DevOps**

1. **Navigate to your Azure DevOps Project**: Open your Azure DevOps project.
2. **Go to Project Settings**: Located at the bottom left corner of the page.
3. **Select Service Connections**: Under the Pipelines section.
4. **New Service Connection**: Click on "New service connection" and choose "Azure Resource Manager".
5. **Service Principal (manual)**: Select the option to manually enter the service principal details.
6. **Fill in the Details**:
   * **Subscription ID**: Your Azure subscription ID.
   * **Subscription Name**: Your Azure subscription name.
   * **Service Principal ID**: The appId from the service principal creation.
   * **Service Principal Key**: The password from the service principal creation.
   * **Tenant ID**: The tenant from the service principal creation.
   * **Service Connection Name**: A name for your service connection.
   * **Verify and Save**: Optionally verify the connection and then save.

**Step 3: Use the Service Connection in Your Pipeline**

1. **Edit or Create a Pipeline**: Go to Pipelines in Azure DevOps and either create a new pipeline or edit an existing one.
2. **Configure Tasks to Use the Service Connection**:
   * When adding or editing a task that requires azure connection (e.g., Azure CLI, Azure PowerShell, or ARM template deployment), select the service connection you created from the "Azure subscription" dropdown.