

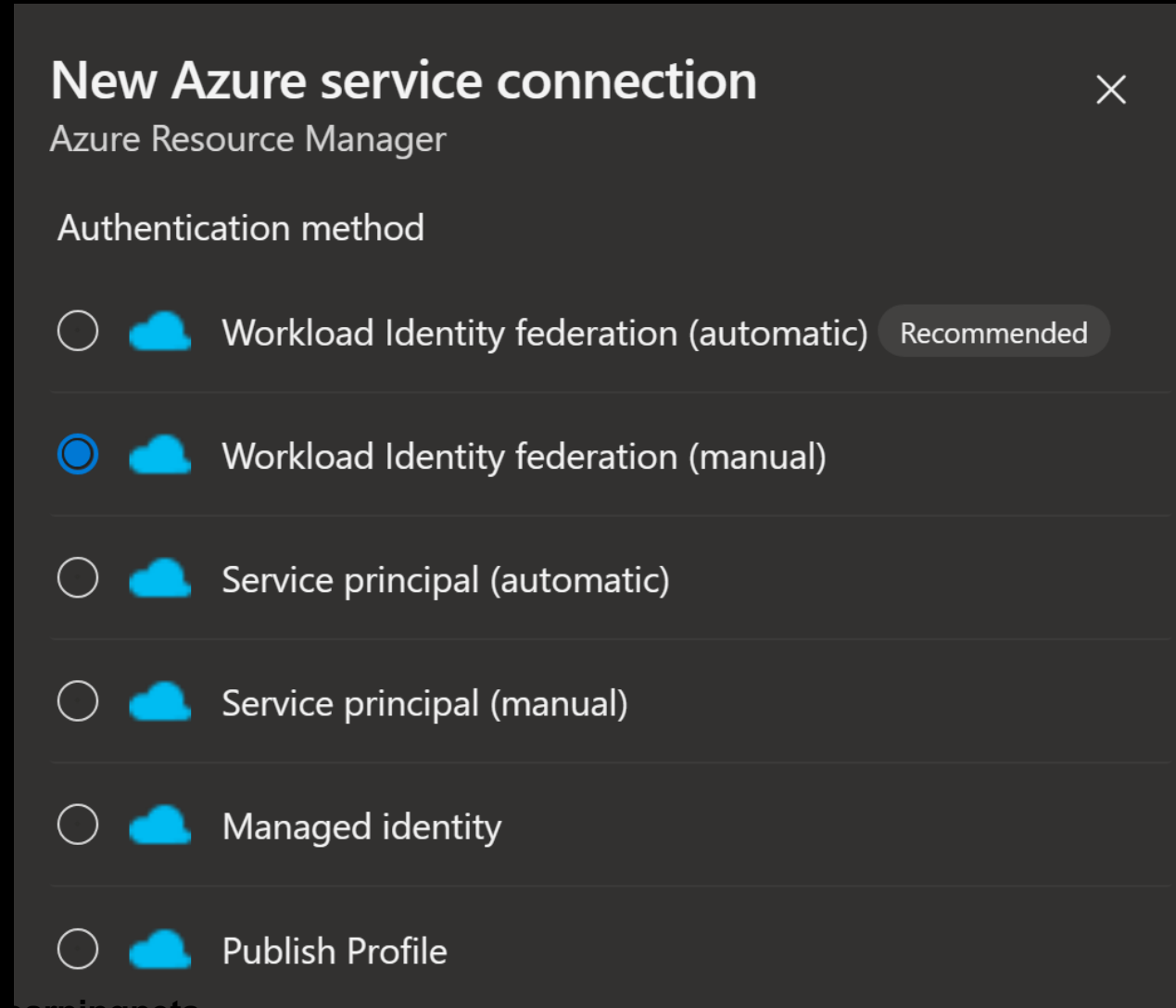
Azure DevOps & Workload Identity (OIDC)

Connect securely to Azure services through **Managed Identity** or **Service Principal** without managing a password.

Passwordless authentication.

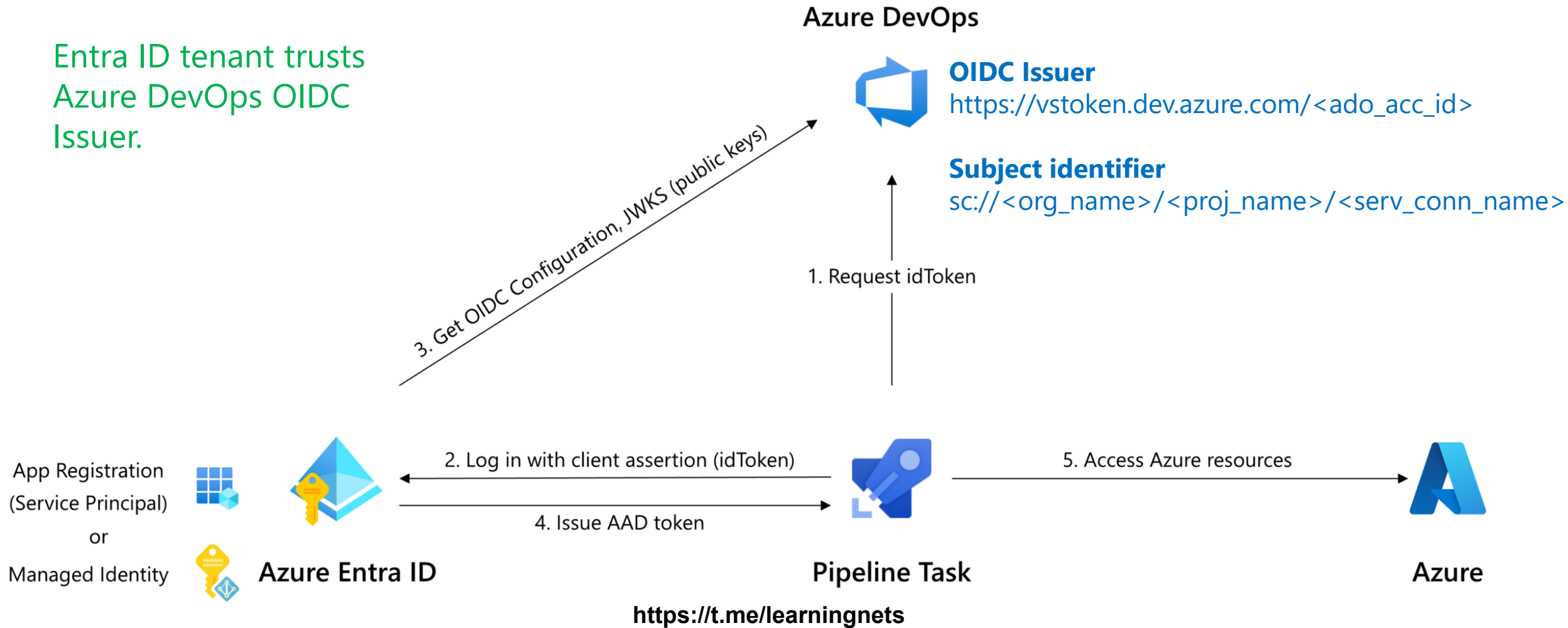
No need to save Service Principal password.

Works also on **self hosted build agents** where Managed Identity could not be attached.



Azure DevOps & Workload Identity (OIDC)

Entra ID tenant trusts
Azure DevOps OIDC
Issuer.



Configuring Workload Identity (OIDC)

The screenshot displays the Azure DevOps interface for configuring service connections. The breadcrumb path is 'houssemdellai / workload-identity-demo / Settings / Service connections'. The left sidebar shows the 'Service connections' menu item selected. The main content area shows a list of service connections: 'identity-azuredevops' and 'sc-azure' (marked as Draft). A modal dialog titled 'New Azure service connection' is open, showing the 'Authentication method' options:

- Workload Identity federation (automatic) Recommended
- Workload Identity federation (manual)
- Service principal (automatic)
- Service principal (manual)
- Managed identity
- Publish Profile

At the bottom of the dialog, there is a link 'Need help choosing a connection type?' and two buttons: 'Back' and 'Next'.

Configuring Workload Identity (OIDC)

Microsoft Azure (Preview) Search resources, services, and docs (G+)

Dashboard > Microsoft.ManagedIdentity-20231026084023 | Overview > identity-azuredevops

identity-azuredevops | Properties

Managed Identity

Search Refresh

- Overview
- Activity log
- Access control (IAM)
- Tags
- Azure role assignments
- Associated resources (preview)

Settings

- Federated credentials
- Properties**
- Locks

Monitoring

- Advisor recommendations

Essentials

- Id: /subscriptions/17b12858-3960-4e6f-a663-a06fdae23428
- Name: identity-azuredevops
- Type: Microsoft.ManagedIdentity/userAs...
- Tags: View value as JSON
- Location: westeurope

Properties

- Tenant Id: 558506eb-9459-4ef3-b920-ad55c5...
- Principal Id: f2e908dc-9a73-4b2b-adae-36a105...
- Client Id: 6fbd36cd-e697-48e7-bc01-5d8620...

identity-azuredevops - Overview

Edit service connection

Azure Resource Manager using Workload Identity federation with OpenID Connect (manual)

Subscription Id: 17b12858-3960-4e6f-a663-a06fdae23428
Subscription Id from the publish settings file

Subscription Name: Microsoft-Azure-0
Subscription Name from the publish settings file

Authentication

Service Principal Id: 6fbd36cd-e697-48e7-bc01-5d8620a58c13
Client Id for connecting to the endpoint. Refer to Azure Service Principal link on how to create Azure Service Principal.

Tenant ID: 558506eb-9459-4ef3-b920-ad55c555e729
Tenant Id for connecting to the endpoint. Refer to Azure Service Principal link on how to create Azure Service Principal.

Learn more Troubleshoot

Cancel **Verify and save**

Configuring Workload Identity (OIDC)

Microsoft Azure (Preview) Search resources, services, and docs (G+)

identity-azuredevops | Federated credentials

Edit Federated Credential

Configure an identity from an external OpenID Connect Provider to get tokens as this managed identity to access Microsoft Entra ID protected services.

Federated credential scenario *

Connect your account

Enter the details of the account that you want to connect with Microsoft Entra ID. These values will be used by Microsoft Entra ID to validate the connection.

Issuer URL *

Subject identifier *

Credential details

Enter and review the details for this credential. The credential name cannot be edited after creation.

Name *

Audience *
[Edit \(optional\)](#)

identity-azuredevops - Overview

housemc

Edit service connection

Azure Resource Manager using Workload Identity federation with OpenID Connect (manual)

Security

Grant access permission to all pipelines

Service Principal Details

Issuer

Subject identifier

Subject identifier is automatically created for this Service connection. Azure DevOps guarantees only this service connection will use that identity globally.

Environment

Scope Level

Subscription

Management Group

Machine Learning Workspace

Using Workload Identity (OIDC) in pipeline

main workload-identity-demo / azure-pipelines.yml *

```
1 trigger:
2   - main
3
4 pool:
5   vmImage: ubuntu-latest
6
7 steps:
8
9   Settings
10  - task: AzureCLI@2
11    inputs:
12      azureSubscription: 'identity-azuredevops'
13      scriptType: 'bash'
14      scriptLocation: 'inlineScript'
15      inlineScript: 'az group create -n rg-demo -l westeurope'
```

← Azure CLI ⓘ

Azure Resource Manager connection * ⓘ

identity-azuredevops

Script Type * ⓘ

Shell

Script Location * ⓘ

Inline script

Inline Script * ⓘ

az group create -n rg-demo -l westeurope

Script Arguments ⓘ

Advanced

Workload Identity in pipeline for Terraform

```
- task: AzureCLI@2
  inputs:
    addSpnToEnvironment: true
    azureSubscription: 'my-azure-service-connection'
    scriptType: bash
    scriptLocation: inlineScript
    inlineScript: |
      # Inherit Azure CLI service connection
      export ARM_CLIENT_ID=$servicePrincipalId
      export ARM_OIDC_TOKEN=$idToken
      export ARM_TENANT_ID=$tenantId
      export ARM_SUBSCRIPTION_ID=$(az account show --query id -o tsv)
      export ARM_USE_OIDC=true

      terraform init
      terraform apply -auto-approve
```