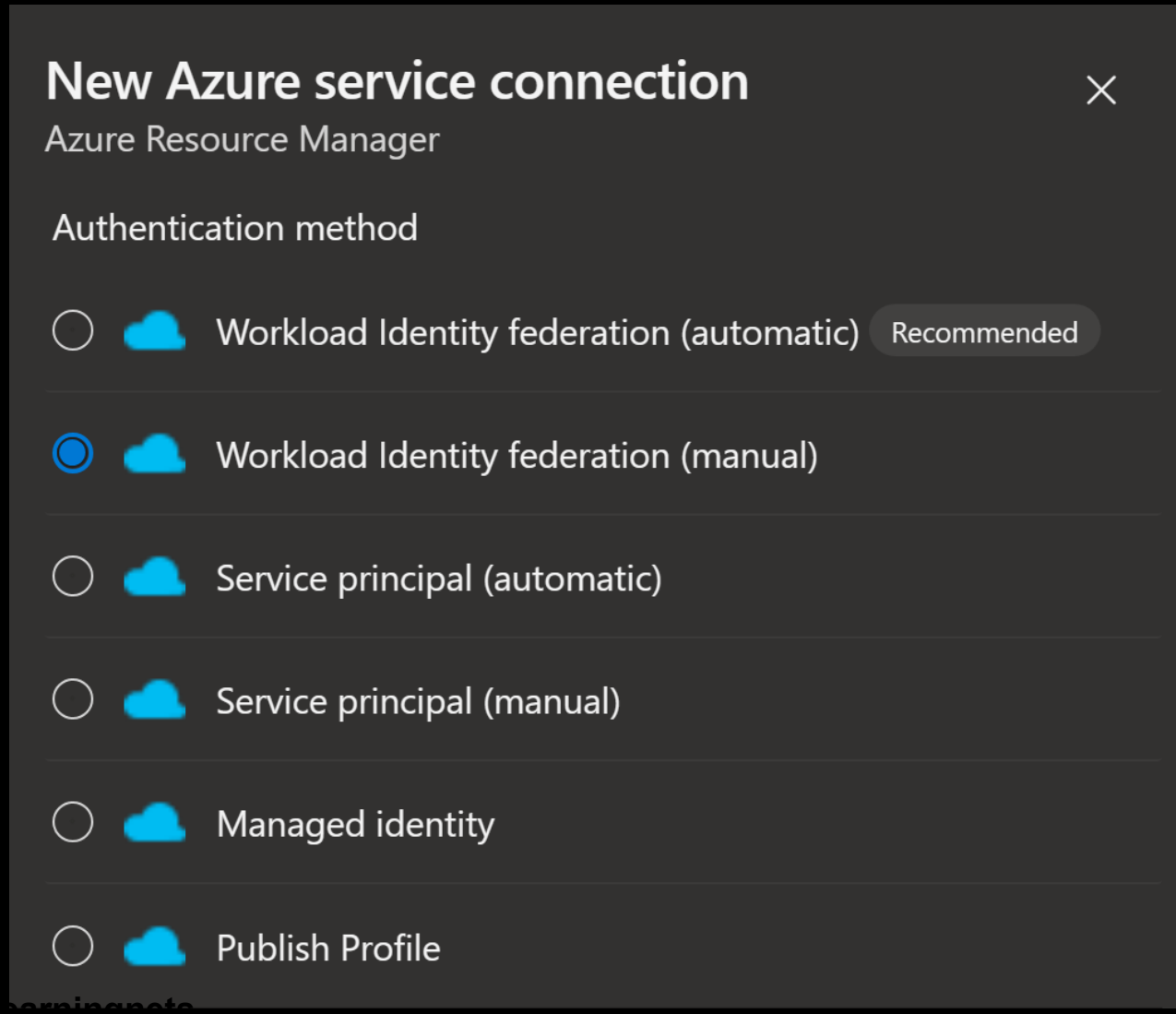
Azure DevOps & Workload Identity (OIDC)

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

Passwordless authentication.

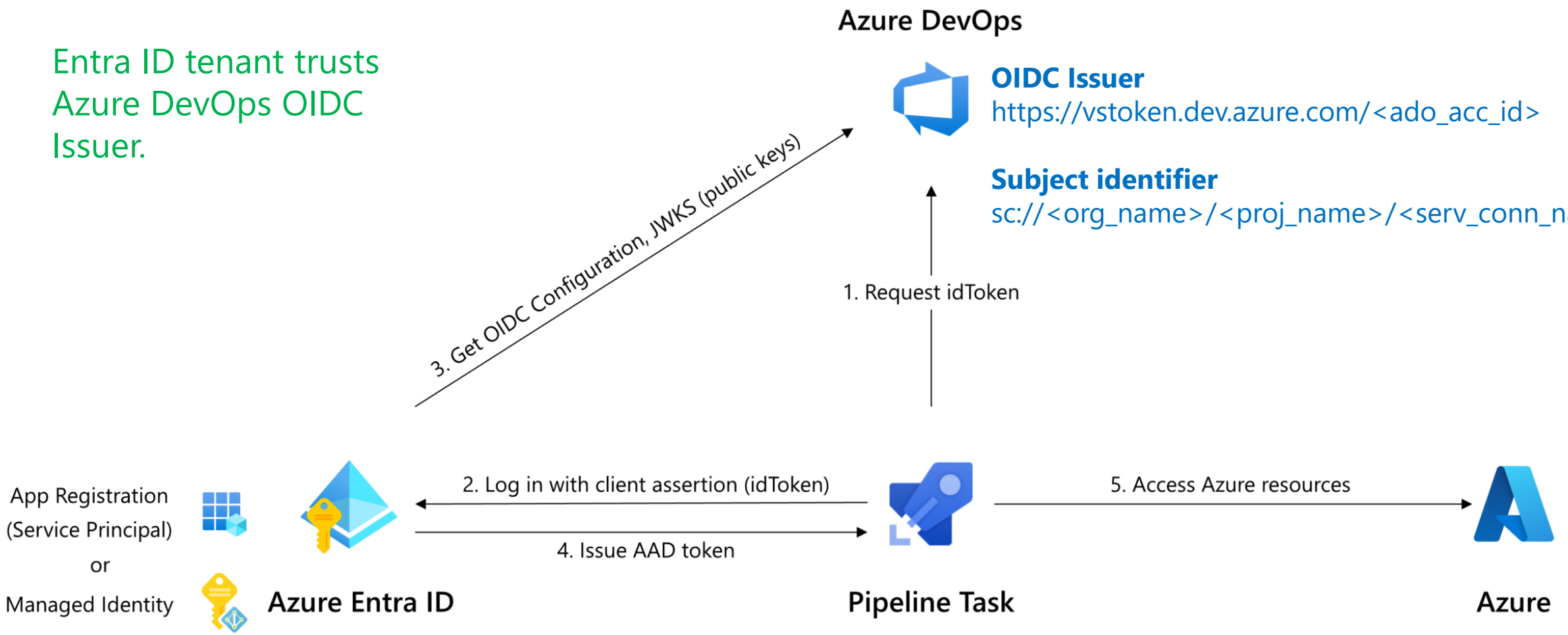
No need to save Service Principal password.

Works also on self hosted build agents where Managed Identity could noy be attached.

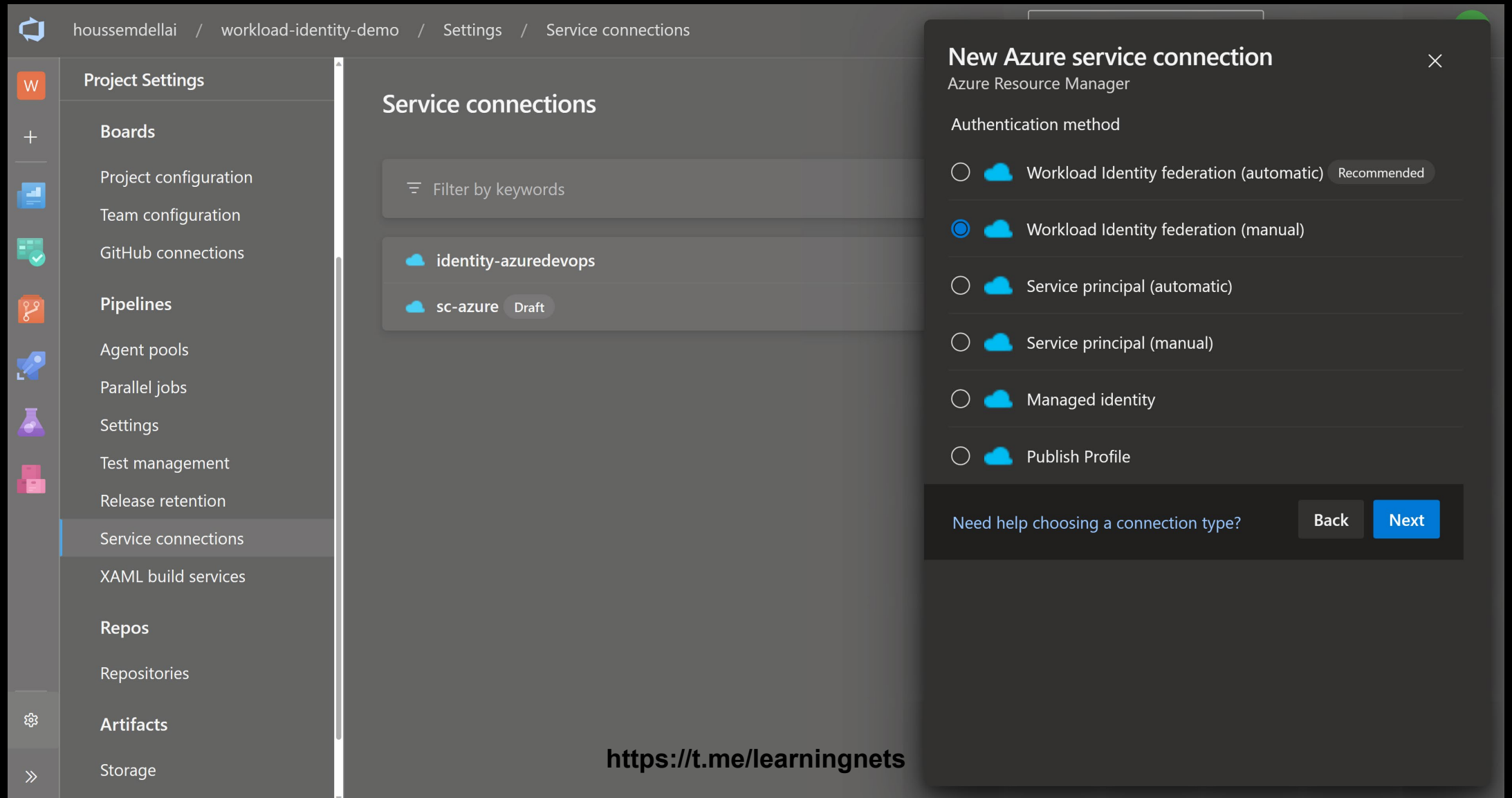


Azure DevOps & Workload Identity (OIDC)

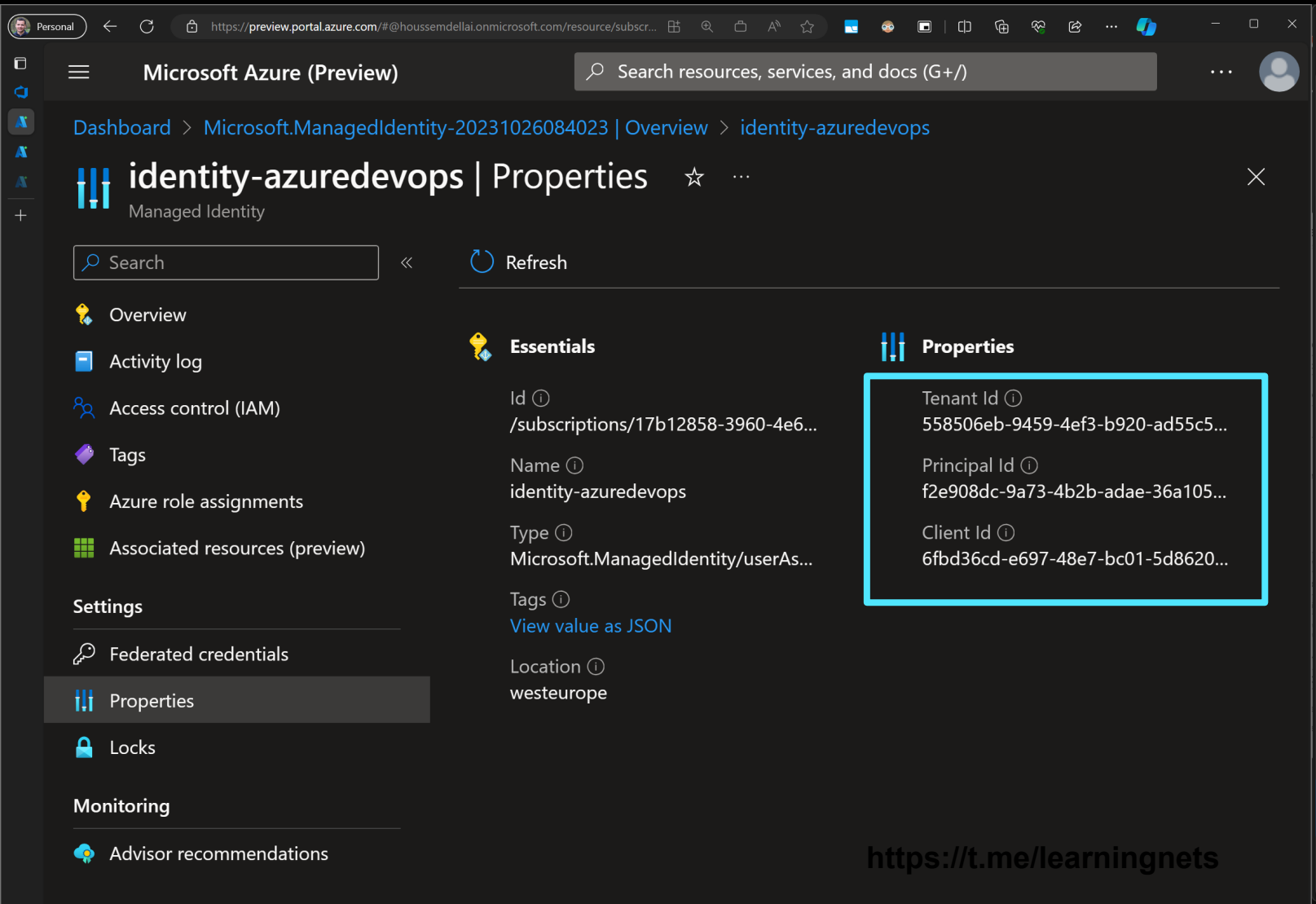
Entra ID tenant trusts Azure DevOps OIDC Issuer.

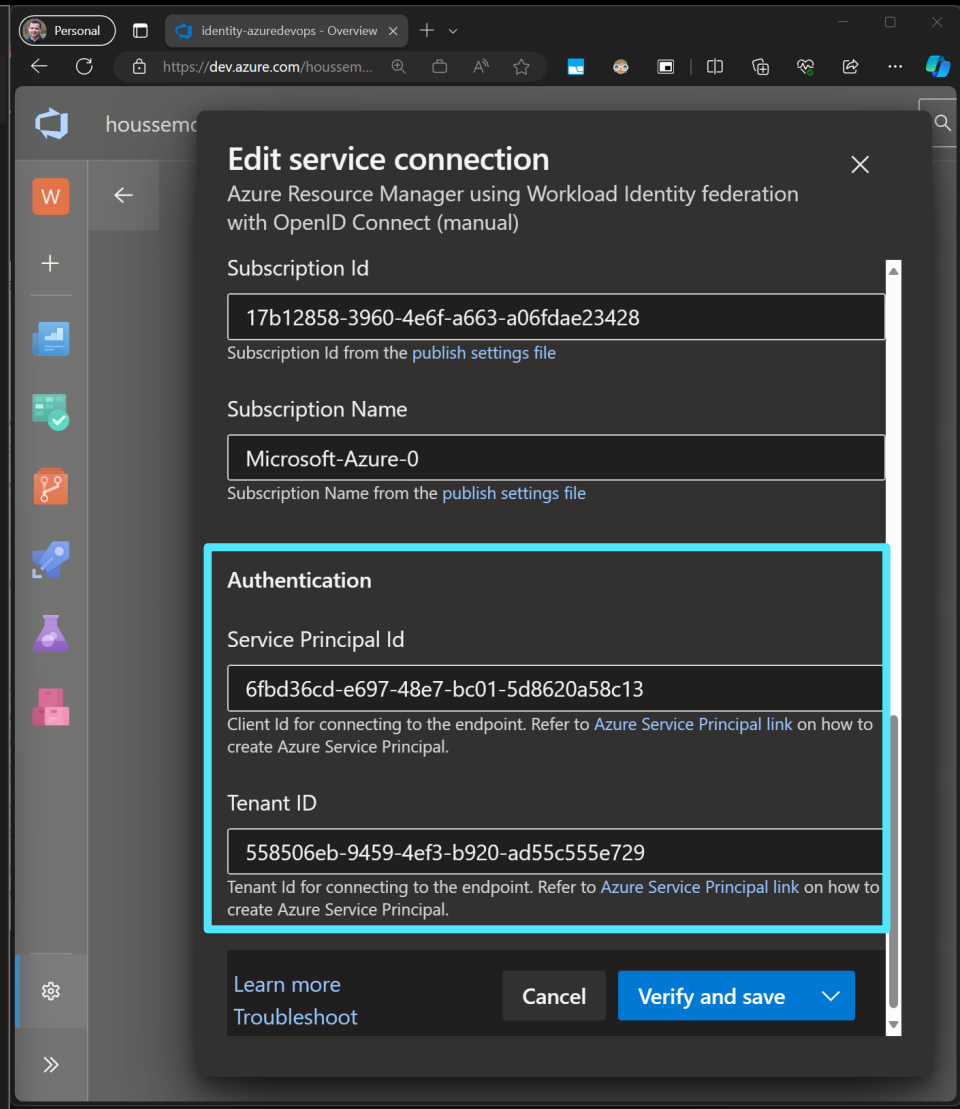


Configuring Workload Identity (OIDC)

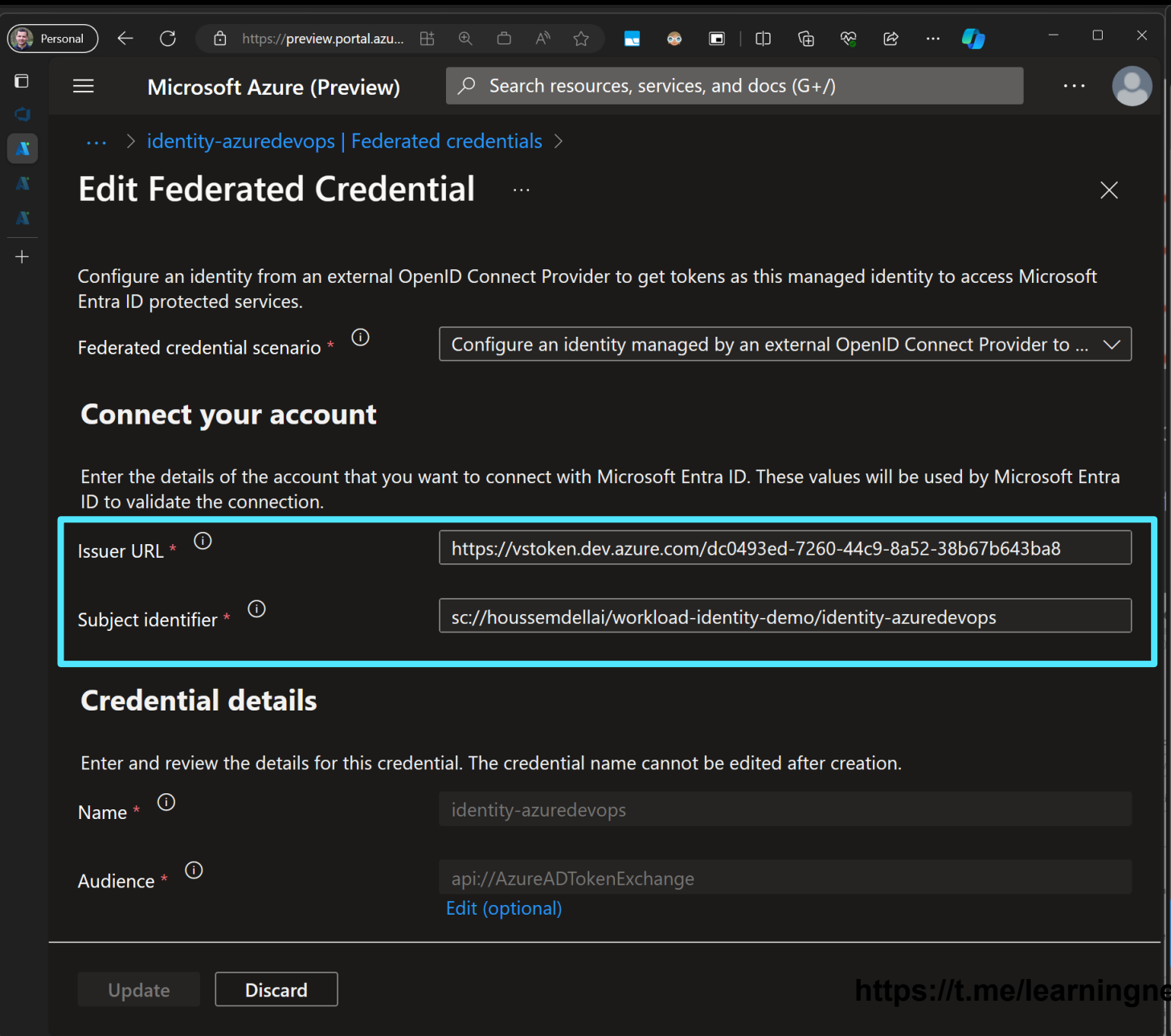


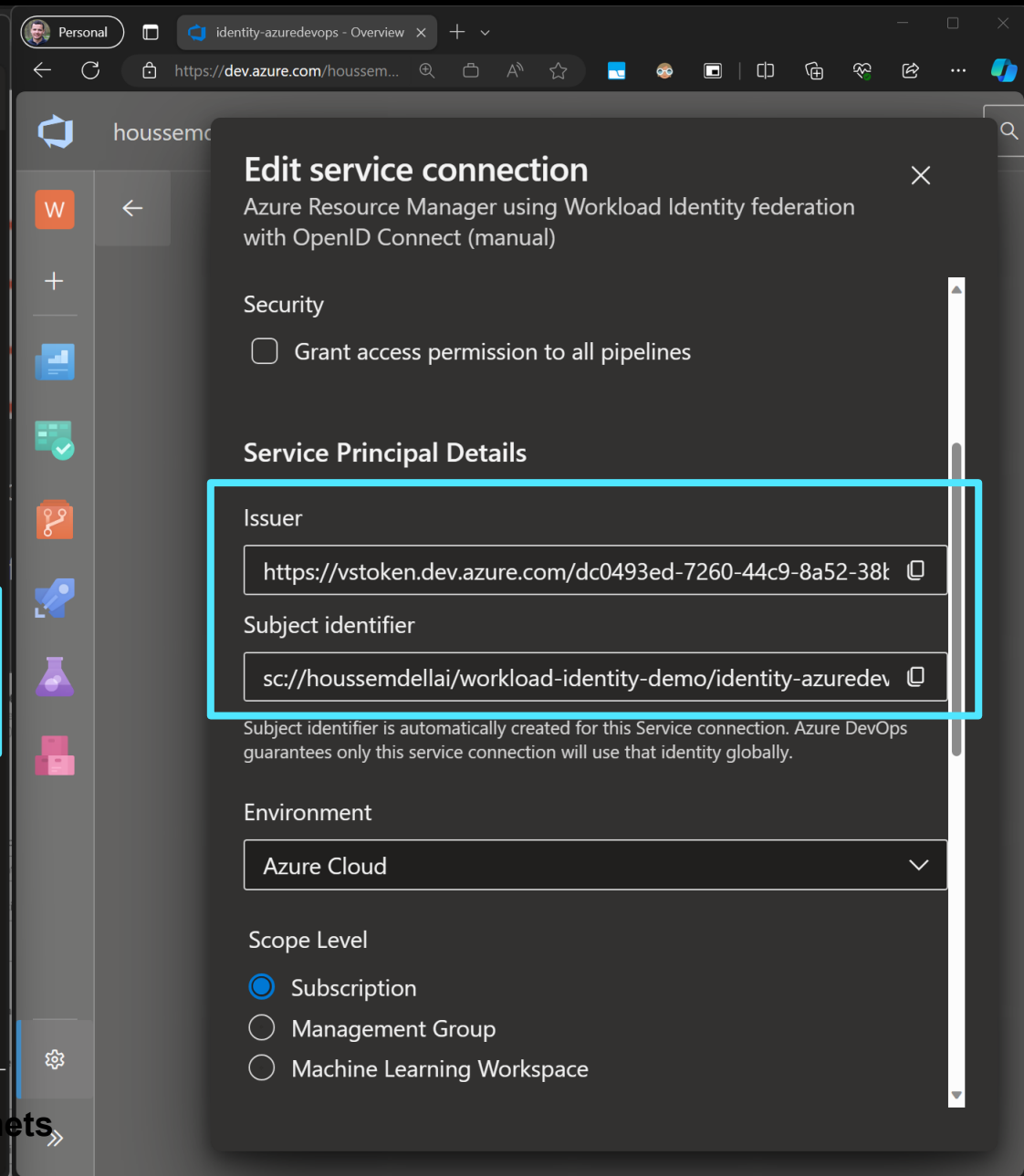
Configuring Workload Identity (OIDC)





Configuring Workload Identity (OIDC)





Using Workload Identity (OIDC) in pipeline

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

```yaml
trigger:
- main

pool:
  vmImage: ubuntu-latest

steps:

Settings
- task: AzureCLI@2
  inputs:
    azureSubscription: 'identity-azuredevops'
    scriptType: 'bash'
    scriptLocation: 'inlineScript'
    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

```yaml
- 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
```

devblogs.microsoft.com/devops/public-preview-of-workload-identity-federation-for-azure-pipelines/