

# GITHUB ACTIONS

Passwordless workflows  
OIDC on Azure

Housseem Dellai

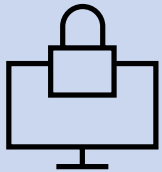


# Github Actions – OIDC on Azure - Identity

How to  
connect  
to Azure  
?

- **User/Human Identity**
  - Works only for humans, based on interactive login with email & pwd
- **Azure Service Principal**
  - AppID & Password
- **User or System Managed Identity (OIDC)**
  - Works only with Azure resources
- **Workload Identity (OIDC)**
  - No password required

# Github Actions – OIDC on Azure – Why Workload Identity ?



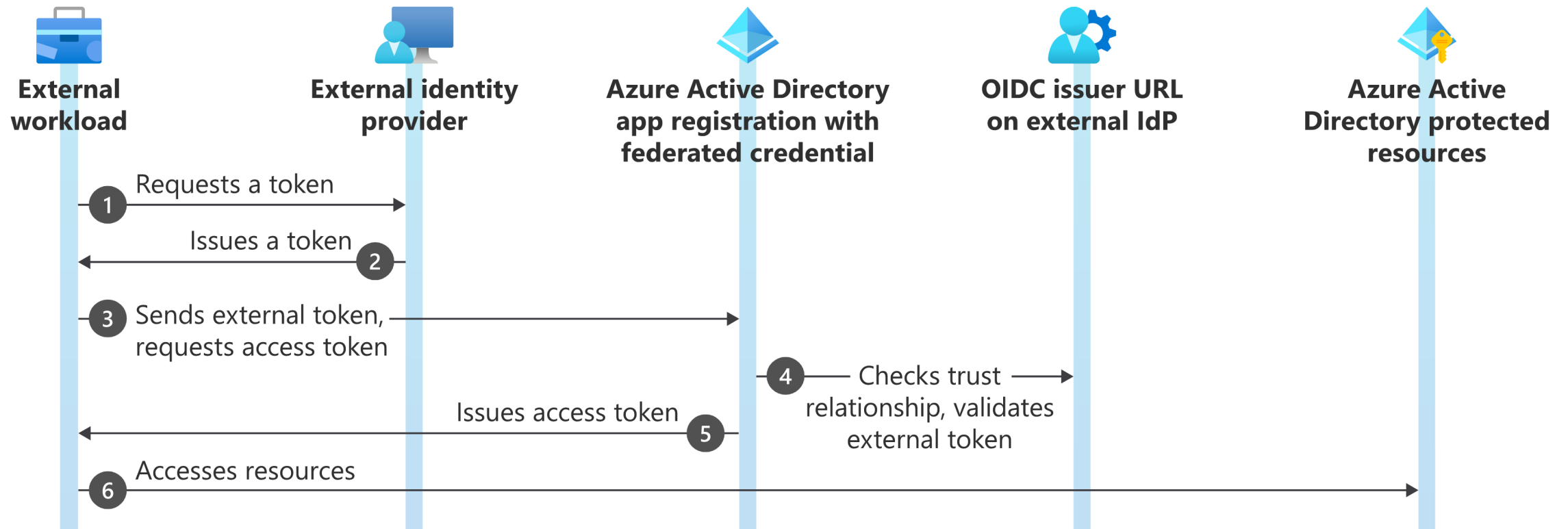
+ No password required



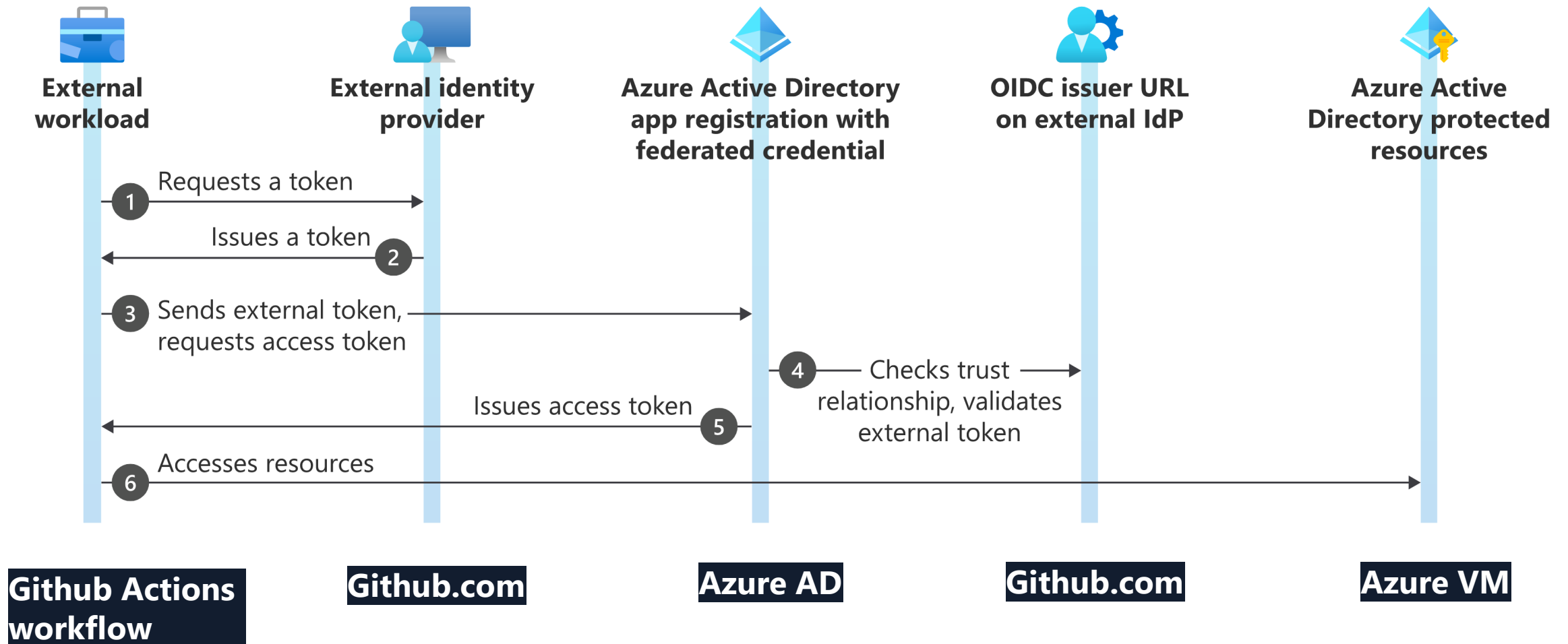
+ Works with Azure resources  
and others:

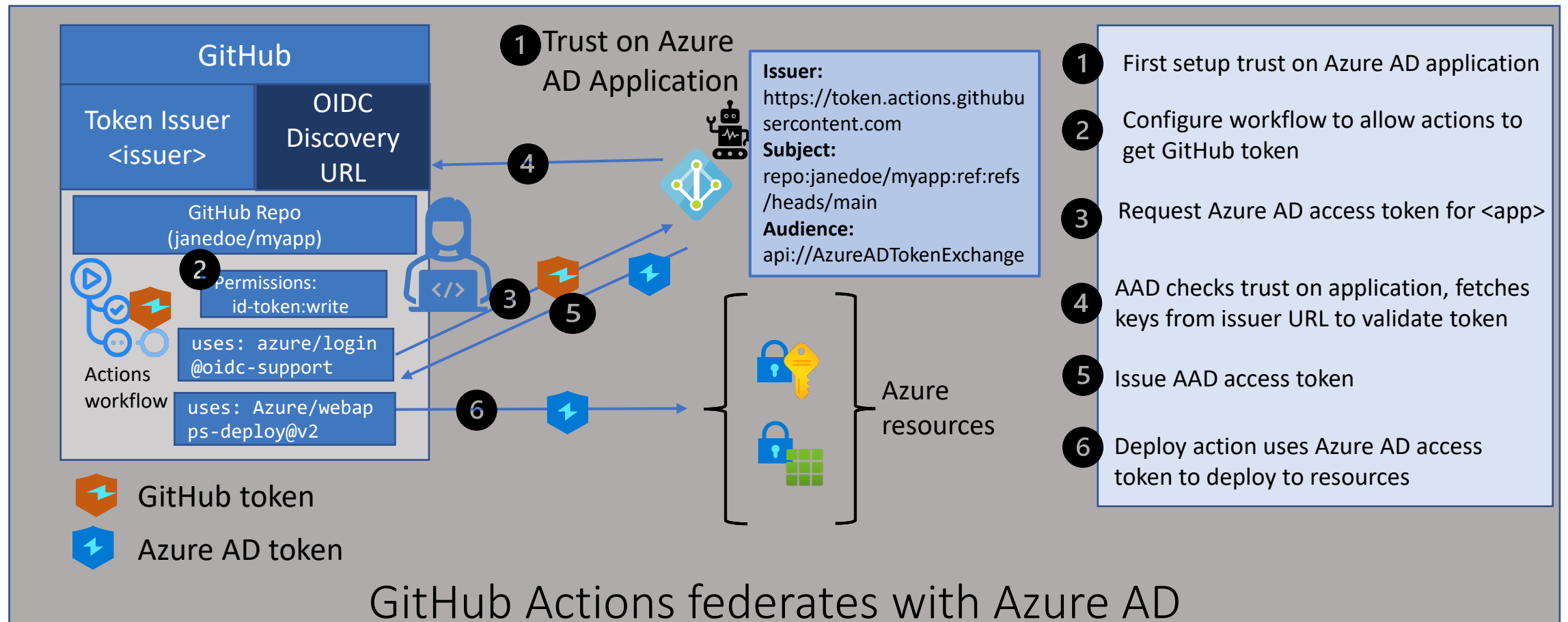
onprem, other cloud, Kubernetes,  
github, etc

# Github Actions – OIDC on Azure – How it works ?




# Github Actions – OIDC on Azure – How it works ?





See <https://blog.identitydigest.com> for detailed walkthrough

# Github Actions – OIDC on Azure – Create App Registration

Houssem Dellai | App registrations

Azure Active Directory

Roles and administrators

Administrative units

Delegated admin partners

Enterprise applications

Devices

App registrations

Identity Governance

+ New registration

Endpoints

Troubleshooting

All applications

Owned applications

Deleted applications

oidc

1 applications found

Display name

github-workflow-oidc

Dashboard > Subscriptions > Microsoft-Azure-2 | Access control (IAM)

Add role assignment

Got feedback?

RoleMembersReview + assign

Selected role

Reader

Assign access to

User, group, or service principal

Managed identity

Members

+ Select members

Name	Object ID
No members selected	

Select

workload

workload-identity-aks

Selected members:

No members selected. Search for and add one or more members you want to assign to the role for this resource.

Learn more about RBAC

Dashboard > Houssem Dellai | App registrations > github-workflow-oidc | Certificates & secrets

Edit a credential

Configure an Azure AD managed identity or an identity from an external OpenID Connect Provider to get tokens as this application and access Azure resources.

Federated credential scenario \*GitHub Actions deploying Azure resources

Connect your GitHub account

Please enter the details of your GitHub Actions workflow that you want to connect with Azure Active Directory. These values will be used by Azure AD to validate the connection and should match your GitHub OIDC configuration. Issuer has a limit of 600 characters. Subject Identifier is a calculated field with a 600 character limit.

Issuerhttps://token.actions.githubusercontent.com

Organization \*HoussemDellai

Repository \*github-actions-course

Entity type \*Branch

Based on selection \*main

Subject identifier \*repo:HoussemDellai/github-actions-course:refs/heads/main

Credential details

Provide a name and description for this credential and review other details.

Namegithub-workflow-oidc

DescriptionLimit of 600 characters

Audienceapi://AzureADTokenExchange

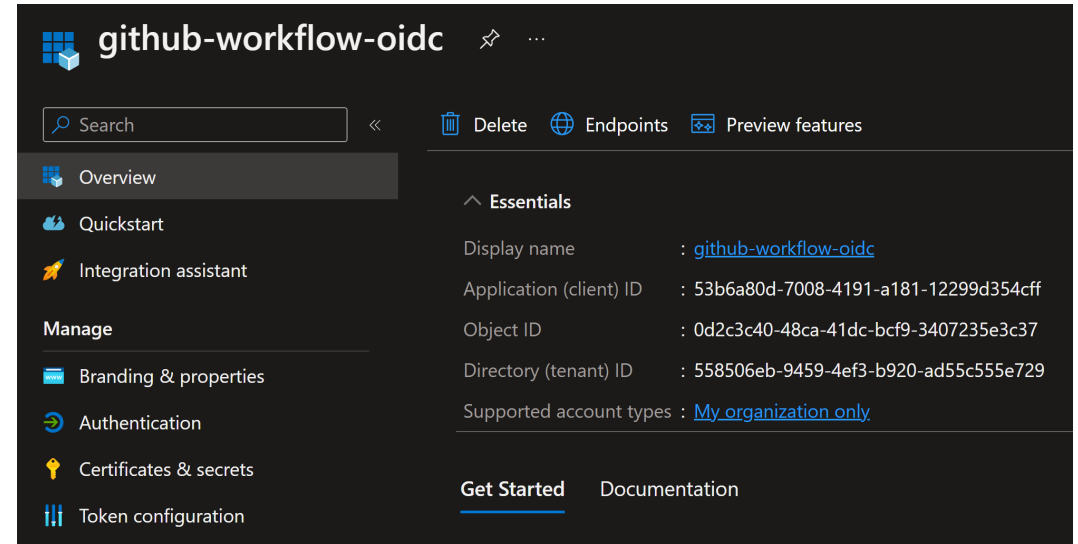
Update

Cancel

# Github Actions – OIDC on Azure – Create workflow

```
on:
  push:
    branches: main
permissions:
  id-token: write
  contents: read
jobs:
  build-and-deploy:
    runs-on: ubuntu-latest
    steps:
      - name: 'Az CLI login'
        uses: azure/login@v1
        with:
          client-id: ${ secrets.AZURE_CLIENT_ID }
          tenant-id: ${ secrets.AZURE_TENANT_ID }
          subscription-id: ${ secrets.AZURE_SUBSCRIPTION_ID }

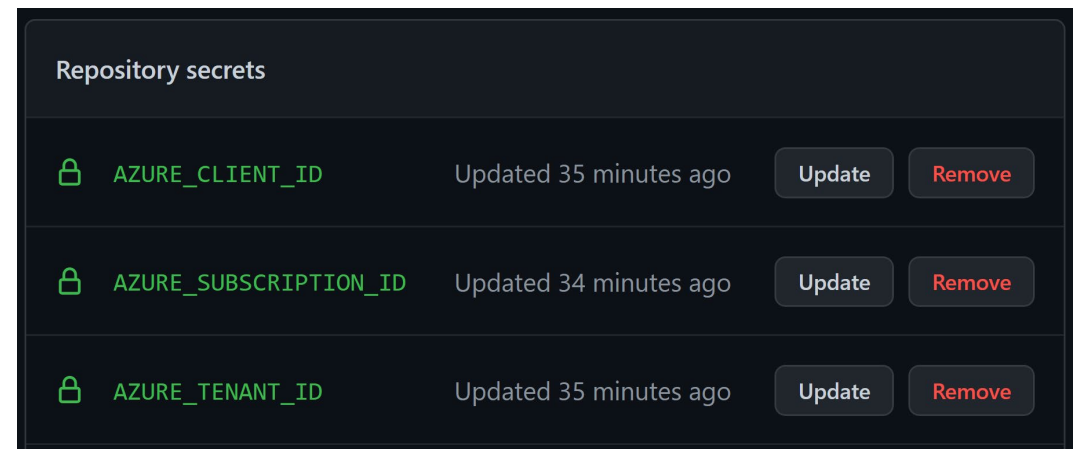
      - name: 'Run az commands'
        run: |
          az account show
          az group list
```



The screenshot shows the GitHub Actions workflow configuration page for a workflow named 'github-workflow-oidc'. The page has a dark theme and includes a sidebar with navigation links: Overview (selected), Quickstart, Integration assistant, Manage, Branding & properties, Authentication, Certificates & secrets, and Token configuration. The main content area displays the 'Essentials' section with the following details:

- Display name: `github-workflow-oidc`
- Application (client) ID: `53b6a80d-7008-4191-a181-12299d354cff`
- Object ID: `0d2c3c40-48ca-41dc-bcf9-3407235e3c37`
- Directory (tenant) ID: `558506eb-9459-4ef3-b920-ad55c555e729`
- Supported account types: [My organization only](#)

At the bottom of the Essentials section, there are links for 'Get Started' and 'Documentation'.



The screenshot shows the 'Repository secrets' page in GitHub Actions. It displays a list of secrets that have been added to the repository:

Secret Name	Updated	Actions
<code>AZURE_CLIENT_ID</code>	Updated 35 minutes ago	<a href="#">Update</a> <a href="#">Remove</a>
<code>AZURE_SUBSCRIPTION_ID</code>	Updated 34 minutes ago	<a href="#">Update</a> <a href="#">Remove</a>
<code>AZURE_TENANT_ID</code>	Updated 35 minutes ago	<a href="#">Update</a> <a href="#">Remove</a>



# Github Actions – OIDC on Azure - Resources

Official documentation: <https://docs.github.com/en/actions/deployment/security-hardening-your-deployments/configuring-openid-connect-in-azure>

Sample: <https://learn.microsoft.com/en-us/azure/developer/github/connect-from-azure?tabs=azure-portal%2Cwindows>