Versioniert, automatisiert und sicher - Optimale Bereitstellung von Azure-Ressourcen

Marc Müller
Principal Consultant

marc.mueller@4tecture.ch
@muellermarc
www.4tecture.ch

MVP Microsoft Most Valuable Professional

4tecture
empower your software solutions

About me:

Marc Müller
Principal Consultant
@muellermarc

MVP
Microsoft Most Valuable Professional

4tecture©
empower your software solutions

Our Products:

Multi-Tenant OpenID Connect Identity Provider

ProAuth

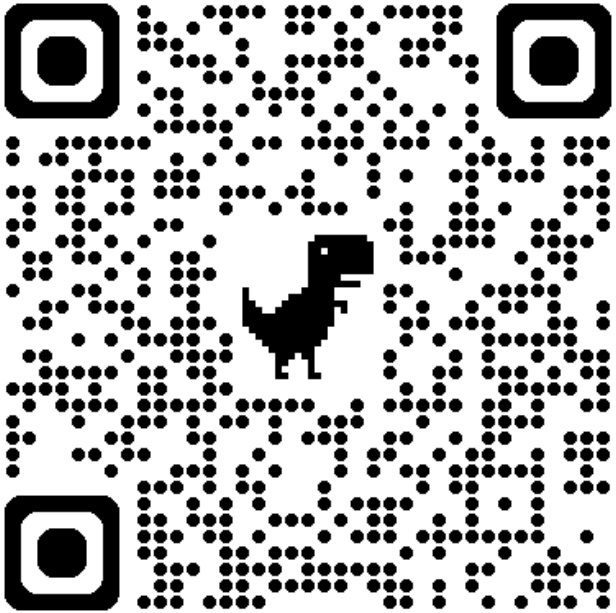
www.proauth.net

Enterprise Application Framework for .NET

ReaFx

www.reafx.net

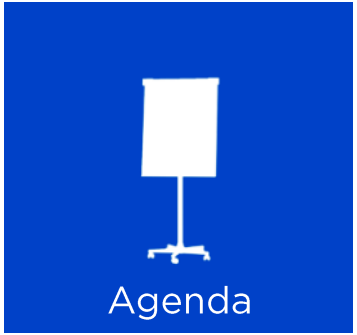
Slide Download



https://www.4tecture.ch/events/ddc24azure

Agenda

- Intro
- Security / Authentication
- Infrastructure as Code / Configuration as Code
- Traditional CI/CD vs GitOps
- Dynamic Resource Deployment
- Conclusion



Azure Deployments

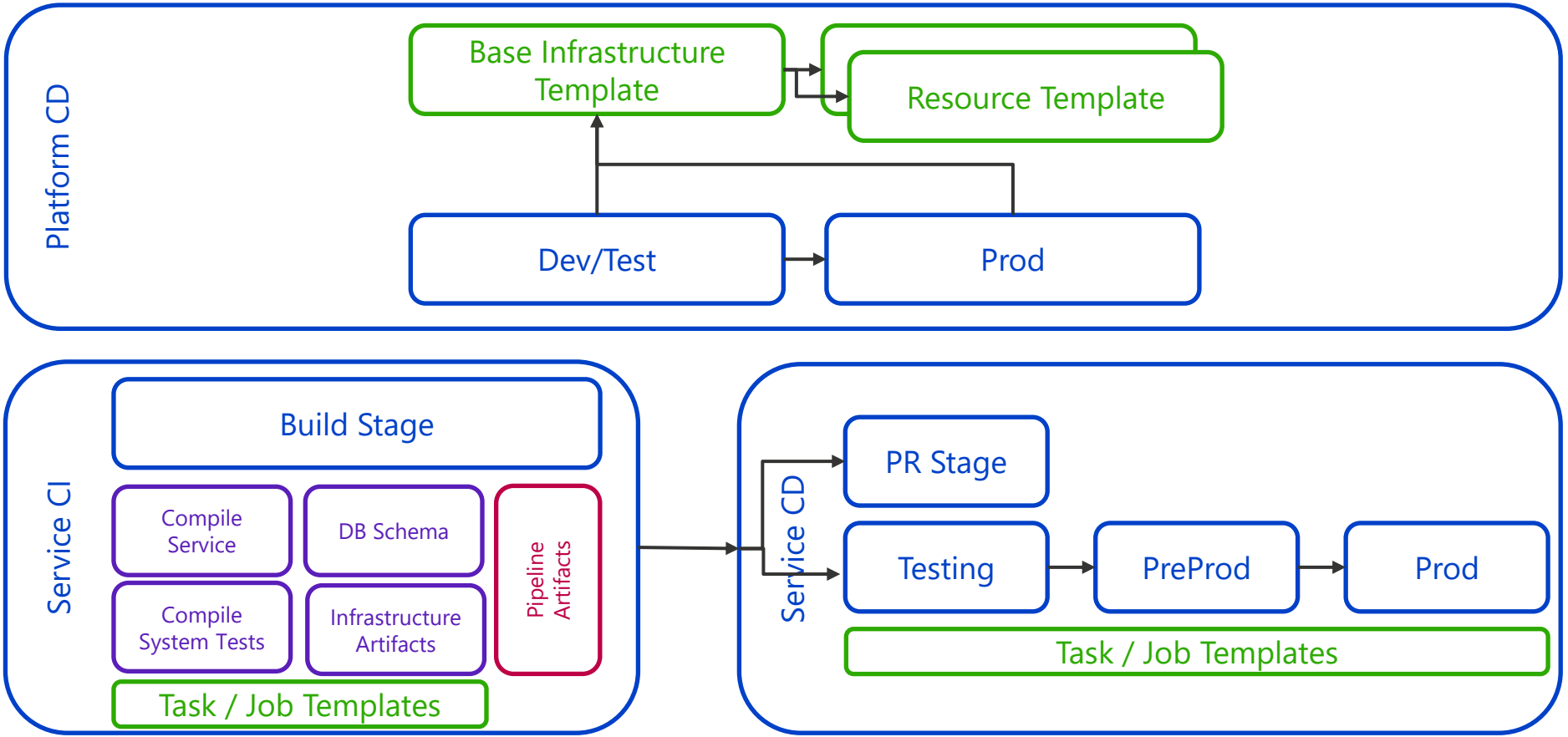
Intro

4tecture
empower your software solutions

Challenges

- Versioned – everything is code
- No manual interaction
- Reusability
- Least Privileged
- Network Access

CI/CD Best Practices



Azure Deployments

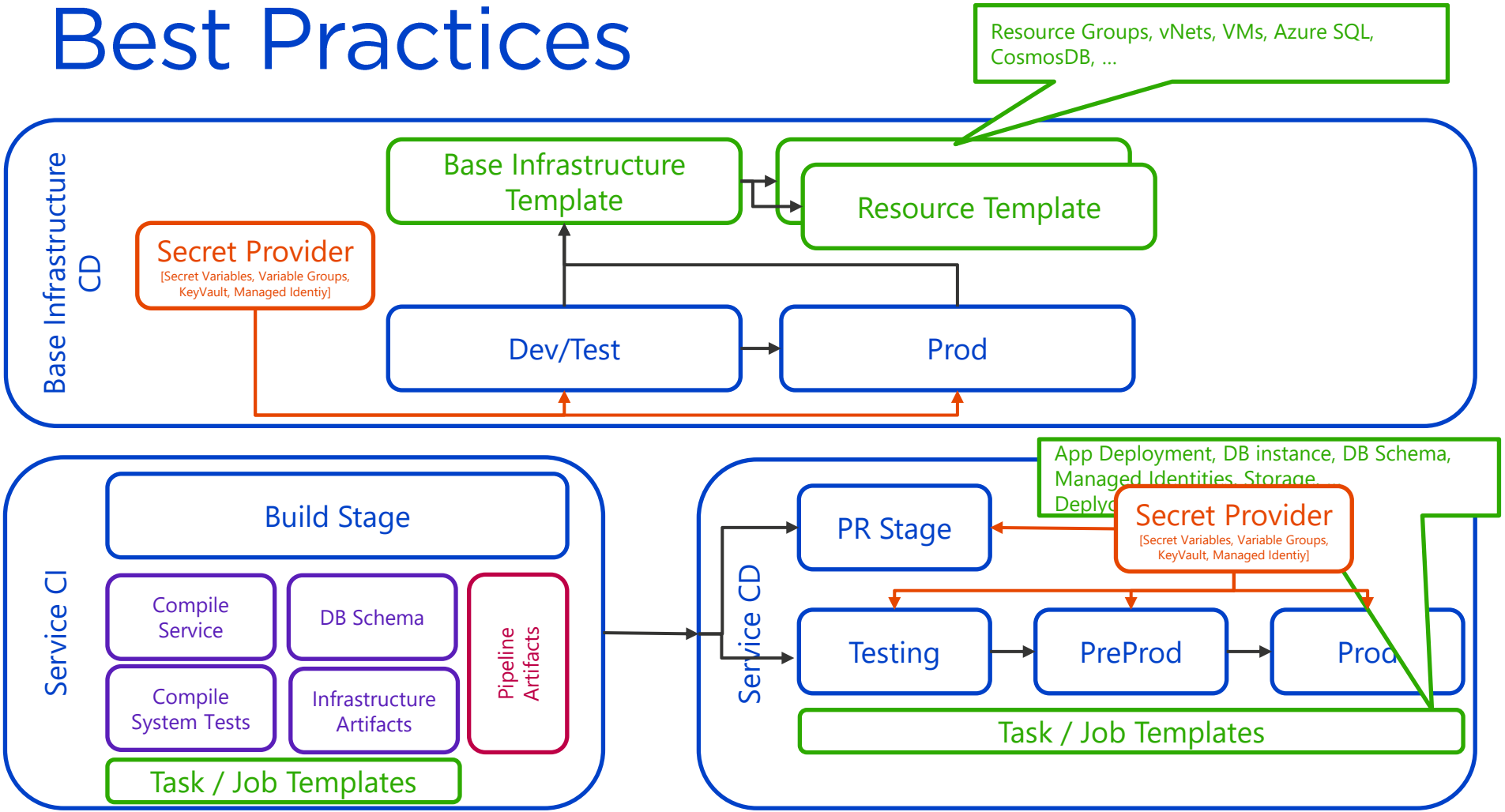
Security / Authentication

4tecture
empower your software solutions

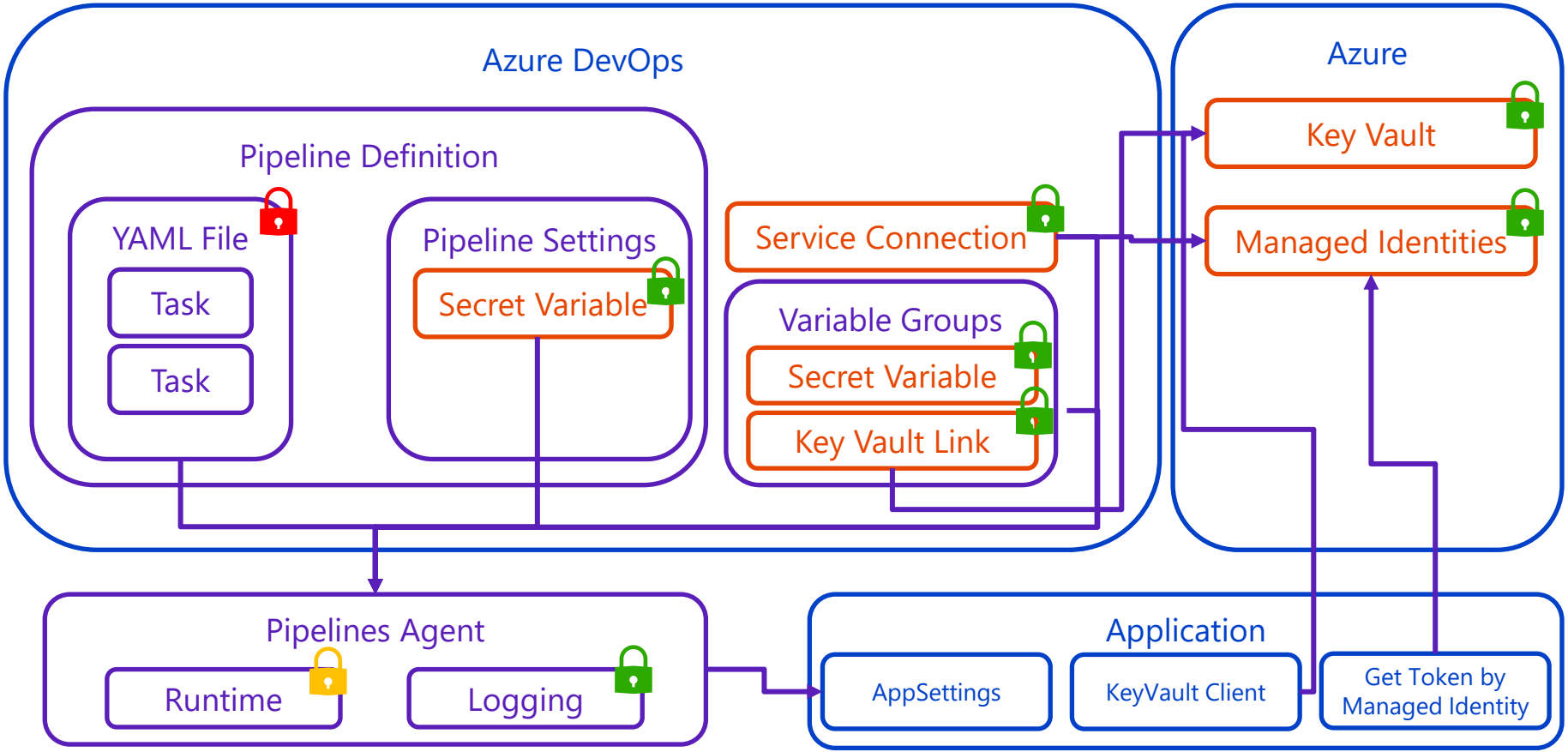
Secrets Challenges

- Configuration as Code
  - Pipeline Definition and Variables are in Source Control
  - Public / Search Index
  - Validate Source Code to not contain any secrets (PR/CI)
  - Just reference secrets in your code / pipelines
- Secret Usage vs. Secret Management
  - Pipeline editors don’t see values in secret variables
  - Pipeline editors only have rights to reference secretes / service connection
  - Additional authorization process for service connections
  - Management of secrets belongs only to dedicated administrators

Best Practices



Simplified Overview




DEMO
Variable Groups / Secret Files

Search

Library > DemoVariableGroup

Variable group | Save | Clone | Security | Pipeline permissions | Approvals and checks | Help

Properties

Variable group name

DemoVariableGroup

Description

Link secrets from an Azure key vault as variables

Variables

Name	Value
GroupSecret1	********
GroupValue1	Value 01
GroupValue2	Value 02

Add

Demo Recap

Search

Library > DemoKeyVaultVariableGroup

Variable group | Save | Clone | Security | Pipeline permissions | Approvals and checks | Help

Properties

Variable group name

DemoKeyVaultVariableGroup

Description

Link secrets from an Azure key vault as variables

Azure subscription * | Manage

Microsoft Azure Sponsorship (redacted)

Scoped to subscription 'Microsoft Azure Sponsorship'

Key vault name * Manage

demovaultmizr6qqogvzzw

Variables

Last refreshed: 15.02.2021

Delete	Secret name	Content type	Status	Expiration date
	theSecret		Enabled	Never

+ Add

Demo Recap

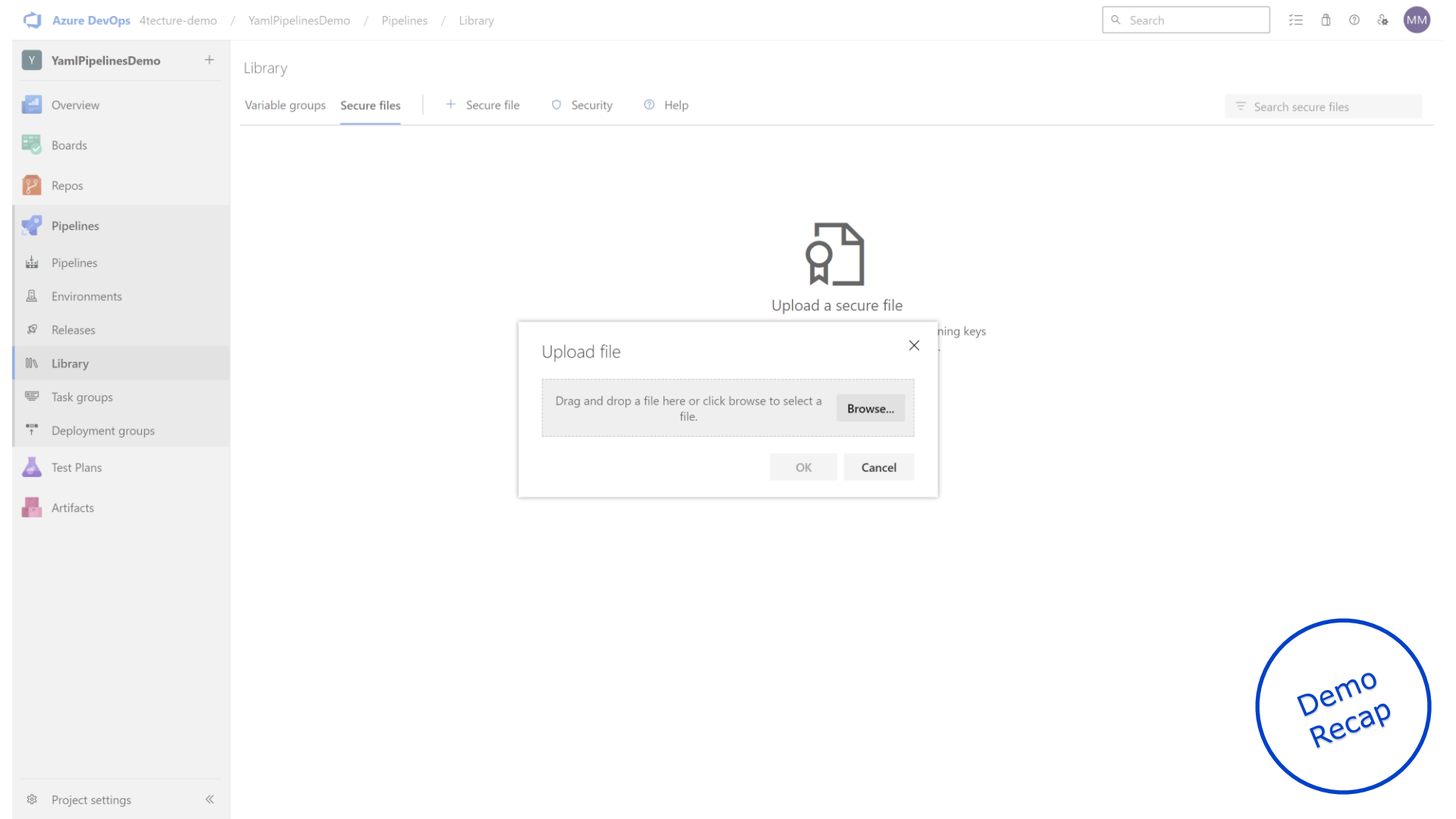
02_SecretVariableGroup

Variables | Run

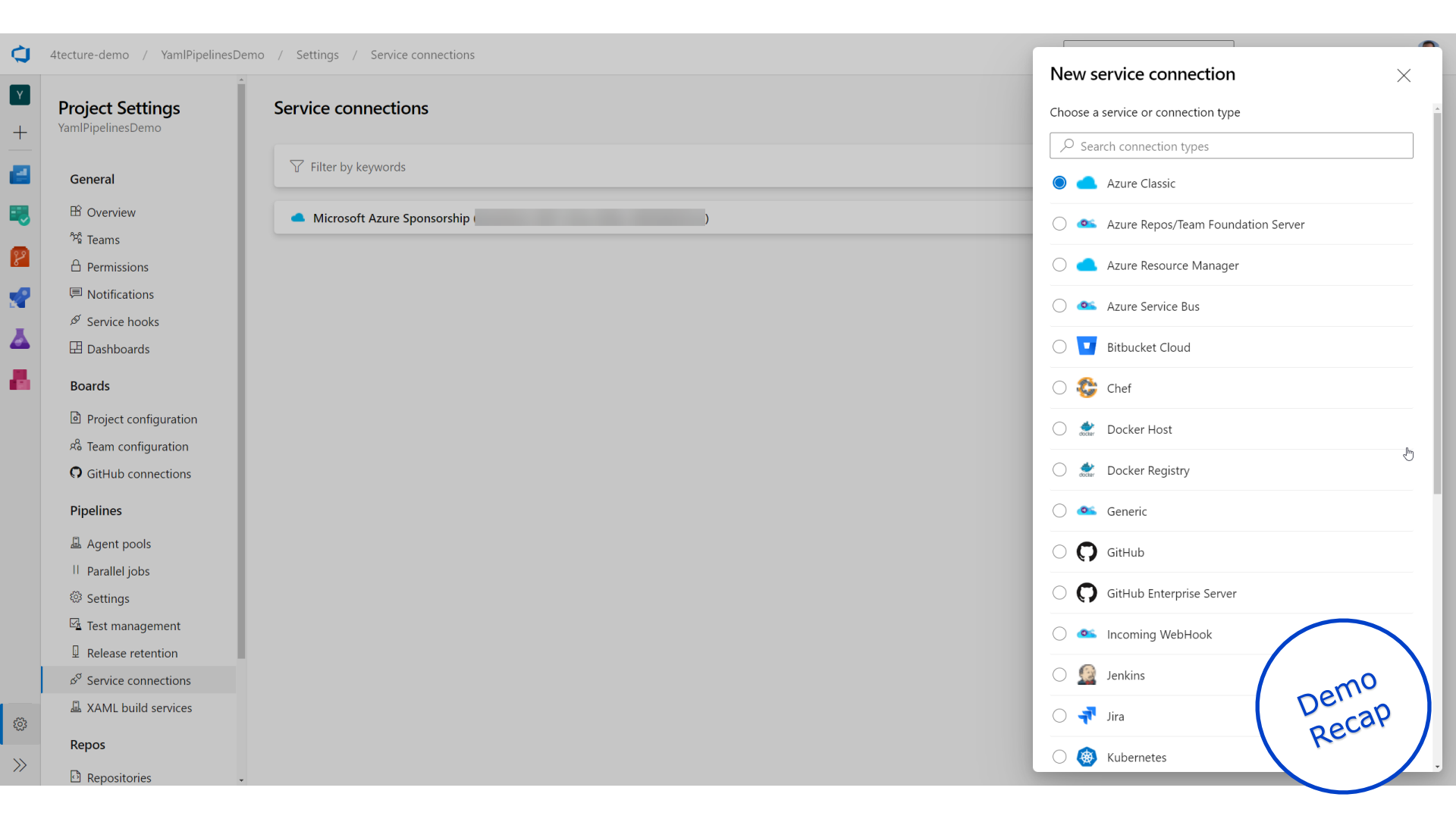
main | SecretsDemo / Pipelines/02_SecretVariableGroup.yml | Show assistant

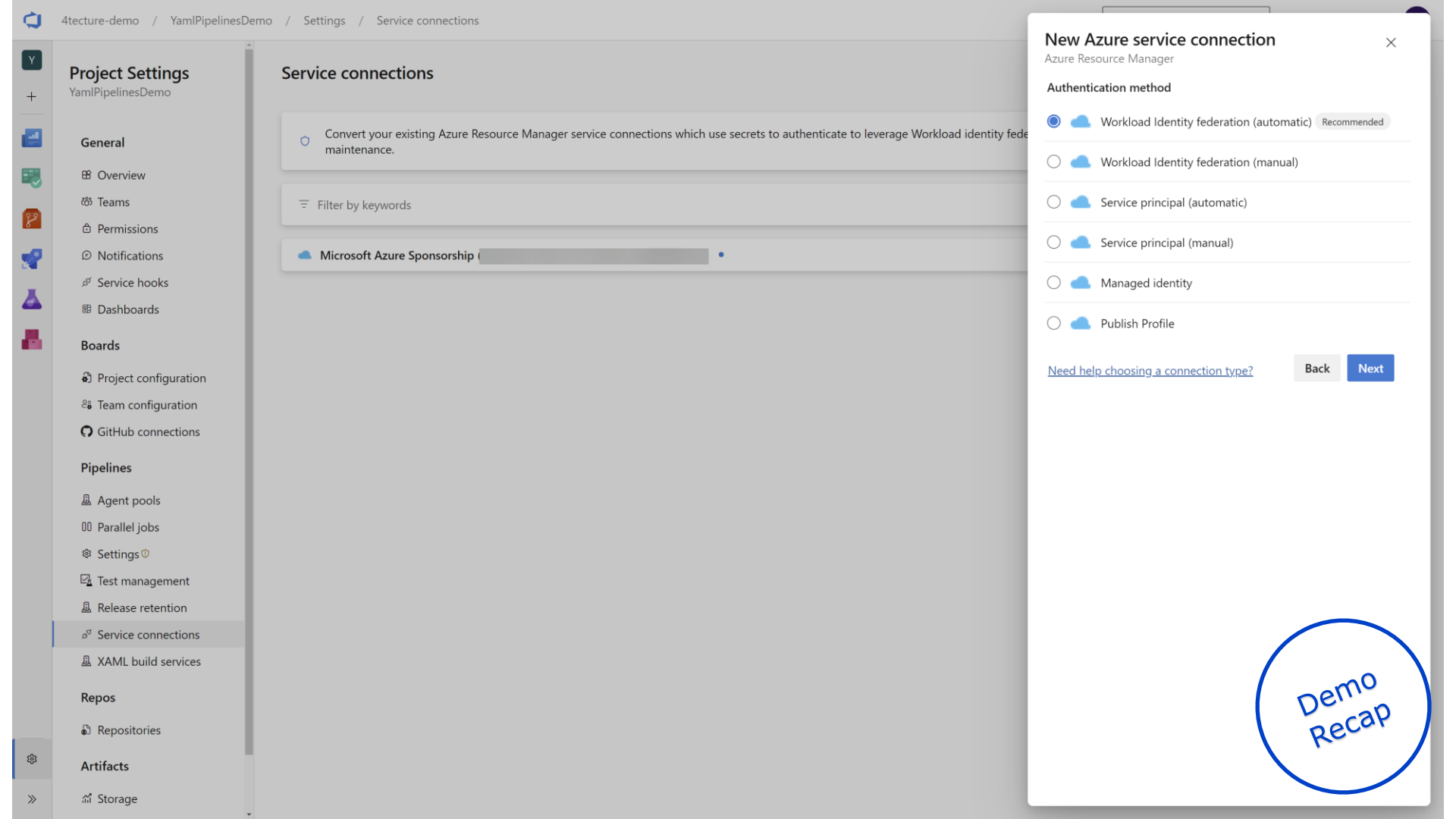
```yaml
trigger:
- main

pool:
  vmImage: ubuntu-latest

variables:
  - name: SampleVariable01
    value: "Some sample content"
  - group: DemoVariableGroup
  - group: DemoKeyVaultVariableGroup

steps:
- pwsh: |
    Write-Host "SampleVariable01: $(SampleVariable01)"
  displayName: "Show a plain text variable"

- pwsh: |
    Write-Host "GroupValue1: $(GroupValue1)"
  displayName: "Show a plain text variable from group"

- pwsh: |
    Write-Host "GroupSecret1: $(GroupSecret1)"
  displayName: "Show a secret variable from group"

- pwsh: |
    Write-Host "theSecret: $(theSecret)"
  displayName: "Show a secret variable from Key Vault by group"

```

Demo Recap


Azure DevOps
4tecture-demo
YamlPipelinesDemo
Pipelines
Library
Search
MM
YamlPipelinesDemo
Overview
Boards
Repos
Pipelines
Pipelines
Environments
Releases
Library
Task groups
Deployment groups
Test Plans
Artifacts
Project settings
Library
Variable groups
Secure files
Secure file
Security
Help
Search secure files
Upload a secure file
ning keys
Upload file
Drag and drop a file here or click browse to select a file.
Browse...
OK
Cancel
Demo Recap


DEMO
Service Connection


4tecture-demo / YamlPipelinesDemo / Settings / Service connections
Project Settings
YamlPipelinesDemo
General
Overview
Teams
Permissions
Notifications
Service hooks
Dashboards
Boards
Project configuration
Team configuration
GitHub connections
Pipelines
Agent pools
Parallel jobs
Settings
Test management
Release retention
Service connections
XAML build services
Repos
Repositories
Service connections
Filter by keywords
Microsoft Azure Sponsorship
New service connection
Choose a service or connection type
Search connection types
Azure Classic
Azure Repos/Team Foundation Server
Azure Resource Manager
Azure Service Bus
Bitbucket Cloud
Chef
Docker Host
Docker Registry
Generic
GitHub
GitHub Enterprise Server
Incoming WebHook
Jenkins
Jira
Kubernetes
Demo Recap


4tecture-demo / YamlPipelinesDemo / Settings / Service connections
Project Settings
YamlPipelinesDemo
General
Overview
Teams
Permissions
Notifications
Service hooks
Dashboards
Boards
Project configuration
Team configuration
GitHub connections
Pipelines
Agent pools
Parallel jobs
Settings
Test management
Release retention
Service connections
XAML build services
Repos
Repositories
Artifacts
Storage
Service connections
Convert your existing Azure Resource Manager service connections which use secrets to authenticate to leverage Workload identity fede
maintenance.
Filter by keywords
Microsoft Azure Sponsorship
New Azure service connection
Azure Resource Manager
Authentication method
Workload Identity federation (automatic)
Recommended
Workload Identity federation (manual)
Service principal (automatic)
Service principal (manual)
Managed identity
Publish Profile
Need help choosing a connection type?
Back
Next
Demo Recap

Project Settings
YamlPipelinesDemo

General
- Overview
- Teams
- Permissions
- Notifications
- Service hooks
- Dashboards

Boards
- Project configuration
- Team configuration
- GitHub connections

Pipelines
- Agent pools
- Parallel jobs
- Settings
- Test management
- Release retention
- Service connections
- XAML build services

Repos
- Repositories

Artifacts
- Storage

Security

Microsoft Azure Sponsorship (8[redacted]2)

User permissions

Project | Organization

+ Add | Undo | Save | Inheritance

User	Role	Access
[YamlPipelinesDemo]\Endpoint Administrators	Administrator	Inherited
MM Marc Müller	Administrator	Assigned

Pipeline permissions

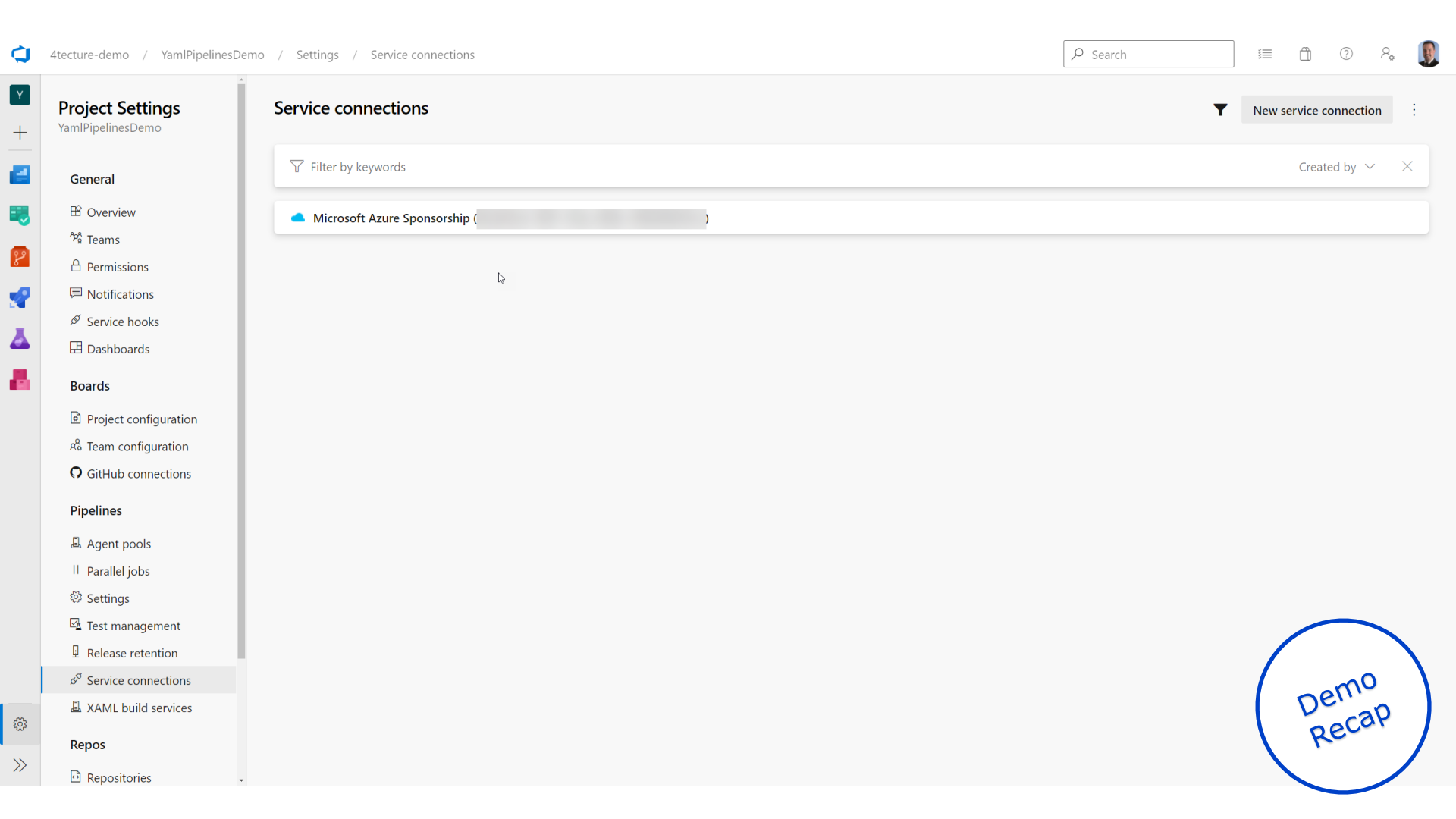
The following YAML pipelines are allowed to use this resource. YAML pipelines from other projects are not shown in this list. All Classic pipelines can use this resource.

Pipeline
04_HelloWorld_MultiStage Pipeline
05_HelloWorld_Trigger_CD Pipeline
03_KeyVaultDemo.yml Pipeline
02_SecretVariableGroup Pipeline

Project permissions

The projects below have access to this service connection.

Demo Recap


4tecture-demo / YamlPipelinesDemo / Settings / Service connections
Search
Project Settings
YamlPipelinesDemo
General
Overview
Teams
Permissions
Notifications
Service hooks
Dashboards
Boards
Project configuration
Team configuration
GitHub connections
Pipelines
Agent pools
Parallel jobs
Settings
Test management
Release retention
Service connections
XAML build services
Repos
Repositories
Service connections
New service connection
Filter by keywords
Created by
Microsoft Azure Sponsorship (
)
Demo Recap

Search

03_KeyVaultDemo.yml

Variables | Run

main | SecretsDemo / Pipelines/03_KeyVaultDemo.yml | Show assistant

```yaml
trigger:
- main

pool:
  vmImage: ubuntu-latest

variables:
  AzureConnection: 'Microsoft Azure Sponsorship (                    )'
  buildConfiguration: 'Release'
  webArtifactName: 'SecretsWebApp'
  infrastructureArtifactName: 'Infrastructure'
stages:
- stage: build ···

- stage: deploy
  displayName: 'Deploy the App'
  jobs:
  - deployment: deployAzure
    displayName: 'Deploy Infrastructure and App'
    environment: secretdemoazure
    strategy:
      runOnce:
        deploy:
          steps:
          - download: current
            artifact: '$(infrastructureArtifactName)'
            displayName: 'Download pipeline artifacts'
          - download: current
            artifact: '$(webArtifactName)'
            displayName: 'Download pipeline artifacts'
```

Settings

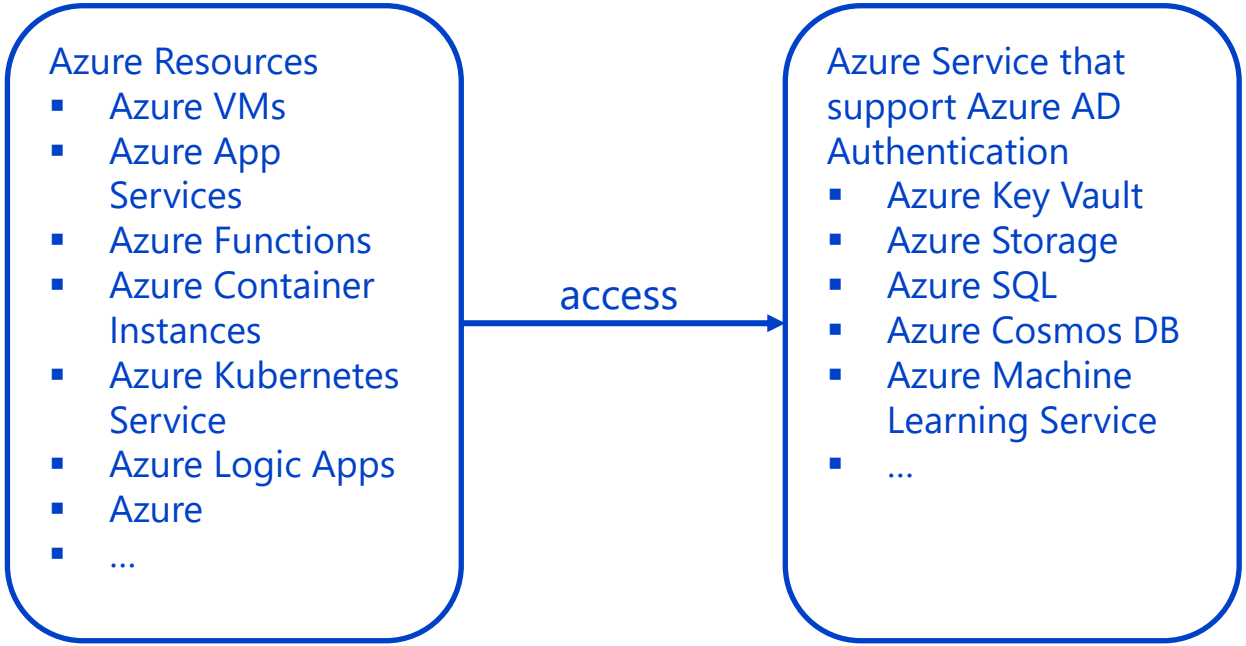
```yaml
          - task: AzureResourceManagerTemplateDeployment@3
            inputs:
              deploymentScope: 'Resource Group'
              azureResourceManagerConnection: $(AzureConnection)
              action: 'Create Or Update Resource Group'
```

Demo Recap

Managed Identities

- Benefits
  - No credentials accessible to the user
  - No management of credentials
  - Used to authenticate to any Azure service that supports Azure AD
  - No additional costs
- Types
  - System-assigned Managed Identities
    - Managed identity directly on the service instance
    - Is tied to the lifecycle of that service instance
  - User-assigned Managed Identities
    - Created as a standalone Azure resource

Use Managed Identities when…



Source: https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

YamlPipelinesDemo

Overview
Boards
Repos
Files
Commits
Pushes
Branches
Tags
Pull requests
Advanced Security
Pipelines
Test Plans
Artifacts

Project settings

SecretsDemo

HelloWorldSecrets
HelloWorldSecrets
.config
Pages
_Host.cshtml
AccessStorage.razor
Error.cshtml
Error.cshtml.cs
Index.razor
ShowSecrets.razor
Properties
ServiceDependencies
Shared
wwwroot
_Imports.razor
App.razor
appsettings.Developme
appsettings.json
HelloWorldSecrets.csproj
Program.cs
Startup.cs
HelloWorldSecrets.sln
Infrastructure

Program.cs

Edit

Contents History Compare Blame

```
1  using Azure.Extensions.AspNetCore.Configuration.Secrets;
2  using Azure.Identity;
3  using Azure.Security.KeyVault.Secrets;
4  using Microsoft.AspNetCore.Hosting;
5  using Microsoft.Extensions.Configuration;
6  using Microsoft.Extensions.Hosting;
7  using System;
8
9  namespace HelloWorldSecrets
10 {
11     public class Program
12     {
13         public static void Main(string[] args)
14         {
15             CreateHostBuilder(args).Build().Run();
16         }
17
18         public static IHostBuilder CreateHostBuilder(string[] args) =>
19             Host.CreateDefaultBuilder(args)
20                 .ConfigureAppConfiguration((context, config) =>
21                 {
22                     var builtConfig = config.Build();
23                     var secretClient = new SecretClient(new Uri($"https://{builtConfig["KeyVaultName"]}.vault.azure.net/"),
24                                                         new DefaultAzureCredential());
25                     config.AddAzureKeyVault(secretClient,
26                                             new AzureKeyVaultConfigurationOptions()
27                                             {
28                                                 ReloadInterval = TimeSpan.FromMinutes(1),
29                                                 Manager = new KeyVaultSecretManager()
30                                             });
31                 })
32                 .ConfigureWebHostDefaults(webBuilder =>
33                 {
34                     webBuilder.UseStartup<Startup>();
35                 });
36     }
37 }
38
```


DEMO
Managed Identity

demovaultmizr6qqogvzzw | Access policies

Key vault

Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Access policies
Events
Objects
Keys
Secrets
Certificates
Settings
Access configuration
Networking
Microsoft Defender for Cloud
Properties
Locks
Monitoring
Automation
Help

Create | Refresh | Delete | Edit

Quickly protect your Key vault from accidental deletion by turning on soft-delete. Please enable soft-delete in 'Properties' page. Click here to learn more. →

Access policies enable you to have fine grained control over access to vault items. Learn more

Search | Permissions : All | Type : All

Showing 1 to 5 of 5 records.

Name	Email	Key Permissions	Secret Permissions	Certificate Permissions
APPLICATION				
[redacted]			Get, List	
secretsdemo-webapp			Get, List	
USER				
[redacted]			All	
[redacted]			Get, List	
[redacted]			All	

< Previous | Page 1 of 1 | Next >

Demo Recap

YamlPipelinesDemo

Overview
Boards
Repos
Files
Commits
Pushes
Branches
Tags
Pull requests
Advanced Security
Pipelines
Test Plans
Artifacts

Project settings

SecretsDemo

HelloWorldSecrets
Infrastructure
storage-and-keyvault.bicep
storage-and-keyvault.paran
webapp.bicep
webapp.parameters.json
Pipelines
.gitignore
README.md

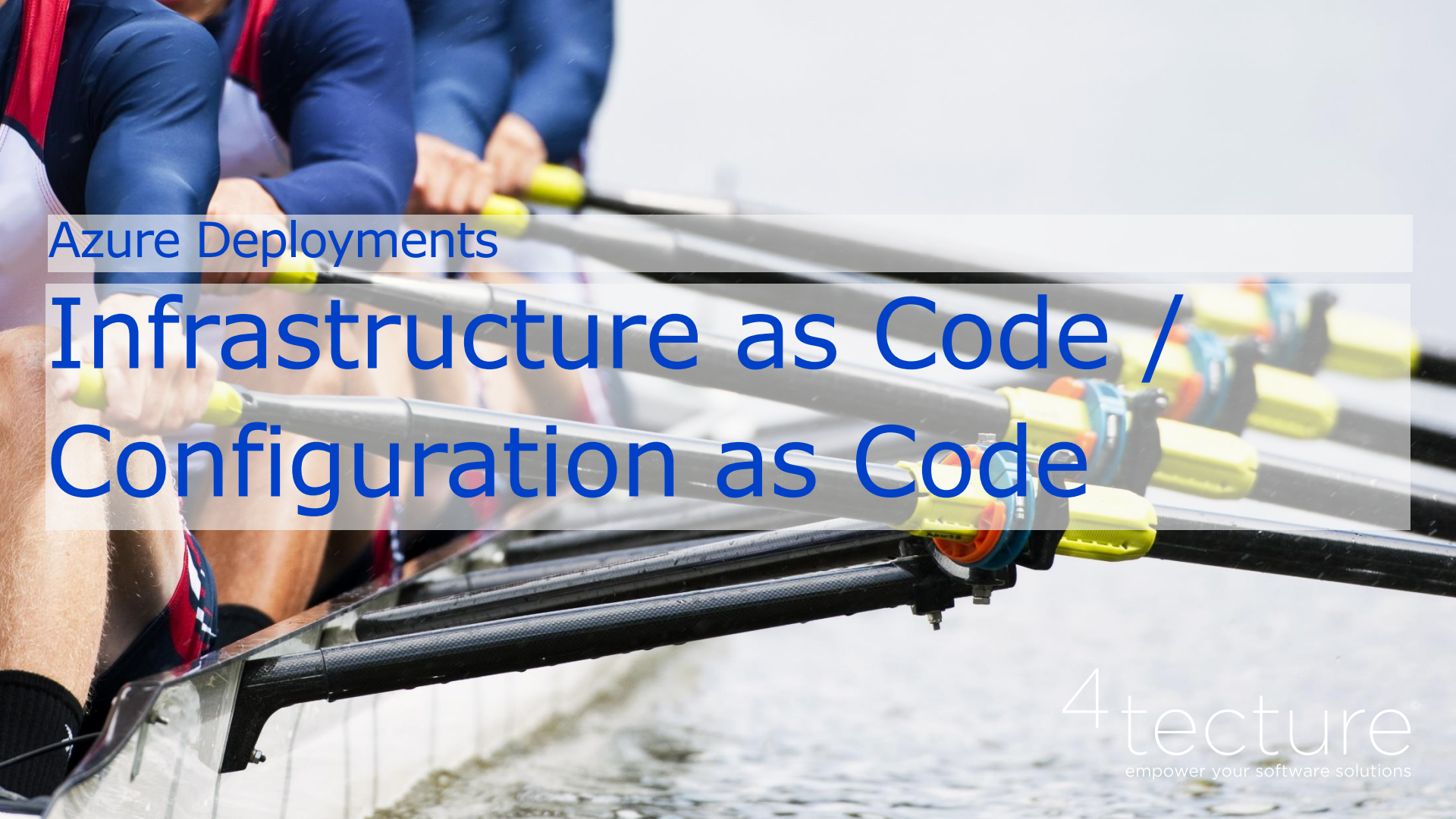
webapp.bicep

Edit

Contents History Compare Blame

```
var keyVaultUniqueName = '${keyVaultName}${uniqueString(resourceGroup().id)}'

resource appServicePlan 'Microsoft.Web/serverfarms@2024-04-01' = {
  name: appServicePlanName
  location: location
  sku: {
    name: sku
  }
  kind: 'linux'
  properties: {
    reserved: true
  }
}

resource webApp 'Microsoft.Web/sites@2024-04-01' = {
  name: webAppPortalName
  location: location
  kind: 'app'
  identity: {
    type: 'SystemAssigned'
  }
  properties: {
    serverFarmId: appServicePlan.id
    siteConfig: {
      linuxFxVersion: linuxFxVersion
      webSocketsEnabled: true
    }
  }
}

resource keyVault 'Microsoft.KeyVault/vaults/accessPolicies@2023-07-01' = {
  name: '${keyVaultUniqueName}/add'
  properties: {
    accessPolicies: [
      {
        tenantId: subscription().tenantId
        objectId: reference(webApp.id, '2019-08-01', 'full').identity.principalId
        permissions: {
          secrets: [
            'get'
            'list'
          ]
        }
      }
    ]
  }
}
```

Demo Recap



Azure Deployments

Infrastructure as Code / Configuration as Code

4tecture
empower your software solutions

Configuration as Code

- Pipelines, Templates, Variables / Values files stored in Git
- Do not store secrets in Git!
- Mono-Repo / Repo per Service
- Staging is implemented by
  - Feature Branches → PR → PR Deployment with QA → PR Approval / Integration
  - Main Branch → Pre Production → Production (checks and approvals, deployment rings)


DEMO
Simple Deployment

YamlPipelinesDemo

Overview
Boards
Repos
Files
Commits
Pushes
Branches
Tags
Pull requests
Advanced Security
Pipelines
Test Plans
Artifacts

Project settings

SecretsDemo

HelloWorldSecrets
HelloWorldSecrets
HelloWorldSecrets.sln
Infrastructure
storage-and-keyvault.bicep
storage-and-keyvault.paran
webapp.bicep
webapp.parameters.json
Pipelines
.gitignore
README.md

webapp.bicep

Edit

Contents History Compare Blame

```bicep
@description('Base name of the resource such as web app name and app service plan ')
@minLength(2)
param webAppName string = 'secretsdemo'

@description('The SKU of App Service Plan ')
param sku string = 'F1'

@description('The Runtime stack of current web app')
param linuxFxVersion string = 'DOTNETCORE|9.0'

@description('Location for all resources.')
param location string = resourceGroup().location

@description('Specifies the name of the key vault.')
@minLength(1)
@maxLength(11)
param keyVaultName string

var webAppPortalName = '${webAppName}-webapp'
var appServicePlanName = 'AppServicePlan-${webAppName}'
var keyVaultUniqueName = '${keyVaultName}${uniqueString(resourceGroup().id)}'

resource appServicePlan 'Microsoft.Web/serverfarms@2024-04-01' = {
  name: appServicePlanName
  location: location
  sku: {
    name: sku
  }
  kind: 'linux'
  properties: {
    reserved: true
  }
}

resource webApp 'Microsoft.Web/sites@2024-04-01' = {
  name: webAppPortalName
  location: location
  kind: 'app'
  identity: {
    type: 'SystemAssigned'
  }
  properties: {
    serverFarmId: appServicePlan.id
    siteConfig: {
      linuxFxVersion: linuxFxVersion
      webSocketsEnabled: true
    }
  }
```

Demo Recap

YamlPipelinesDemo

Overview
Boards
Repos
Pipelines
Pipelines
Environments
Releases
Library
Task groups
Deployment groups
Test Plans
Artifacts

Project settings

03_KeyVaultDemo.yml

Variables | Run

main | SecretsDemo / Pipelines/03_KeyVaultDemo.yml | Show assistant

```yaml
48          steps:
49          - download: current
50            artifact: '$(infrastructureArtifactName)'
51            displayName: 'Download pipeline artifacts'
52          - download: current
53            artifact: '$(webArtifactName)'
54            displayName: 'Download pipeline artifacts'
            Settings
55          - task: AzureCLI@2
56            inputs:
57              azureSubscription: $(AzureConnection)
58              scriptType: bash
59              scriptLocation: inlineScript
60              inlineScript: |
61                az group create --name $(resourceGroupName) --location $(location)
62                az deployment group create --resource-group $(resourceGroupName) --template-file $(Pipeline.Workspace)/Infrastructure/storage-and-keyvault.bicep
63            displayName: "Deploy Storage and KeyVault Infrastructure"
            Settings
64          - task: AzureCLI@2
65            inputs:
66              azureSubscription: $(AzureConnection)
67              scriptType: bash
68              scriptLocation: inlineScript
69              inlineScript: |
70                az group create --name $(resourceGroupName) --location $(location)
71                az deployment group create --resource-group $(resourceGroupName) --template-file $(Pipeline.Workspace)/Infrastructure/webapp.bicep --parameters @
72            displayName: "Deploy WebApp Infrastructure"
            Settings
73          - task: AzureWebApp@1
74            displayName: 'Deploy app to azure web app'
75            inputs:
76              azureSubscription: '$(AzureConnection)'
77              appType: 'webAppLinux'
78              appName: 'secretsdemo-webapp'
79              package: '$(Pipeline.Workspace)/**/HelloWorldSecrets.zip'
80
81
```

Demo Recap


DEMO
Complex Deployment

Deploy Cluster Services

- Cluster setup has a lot of Helm chart deployments
- Configuration as Code
- Pipeline automation on configuration object

- Runtime Parameters / Parameters support objects
- Define your cluster configuration as object

k8sDemo

Overview
Boards
Repos
Files
Commits
Pushes
Branches
Tags
Pull requests
Advanced Security
Pipelines
Test Plans
Artifacts

Project settings

Infrastructure

azure
aks.bicep
aksidentity.bicep
azdoagentvm.bicep
k8senvironment-dev.param
k8senvironment.bicep
k8senvironment.parameters
privatedns.bicep
rbac.bicep
registry.bicep
sql.bicep
vnet.bicep
deploymentagent
kubernetes-config
linuxworker
scripts
.gitignore
azure-pipelines.yml
README.md

feature/privateEndpoints / azure / k8senvironment.bicep

k8senvironment.bicep

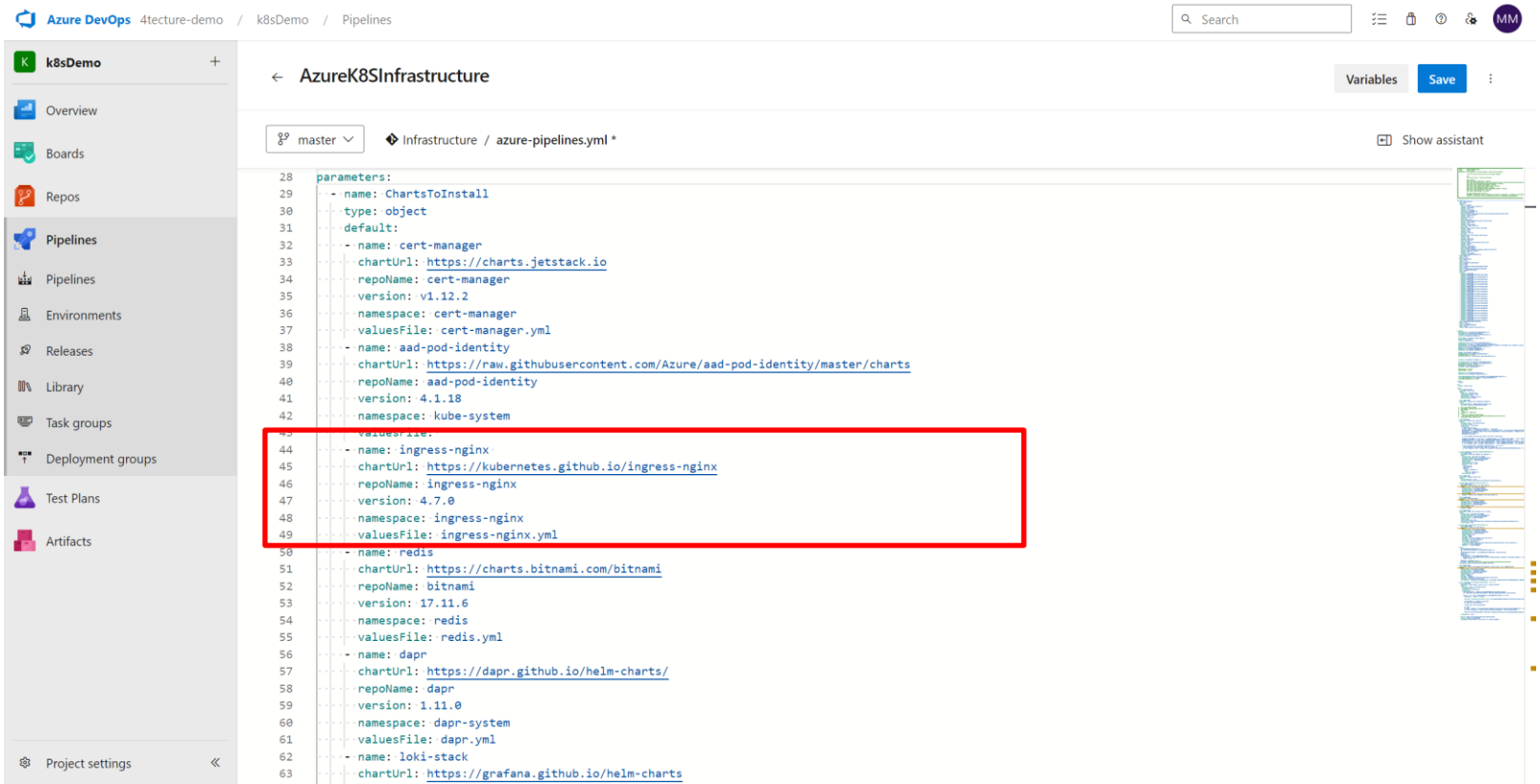
Edit

Contents History Compare Blame

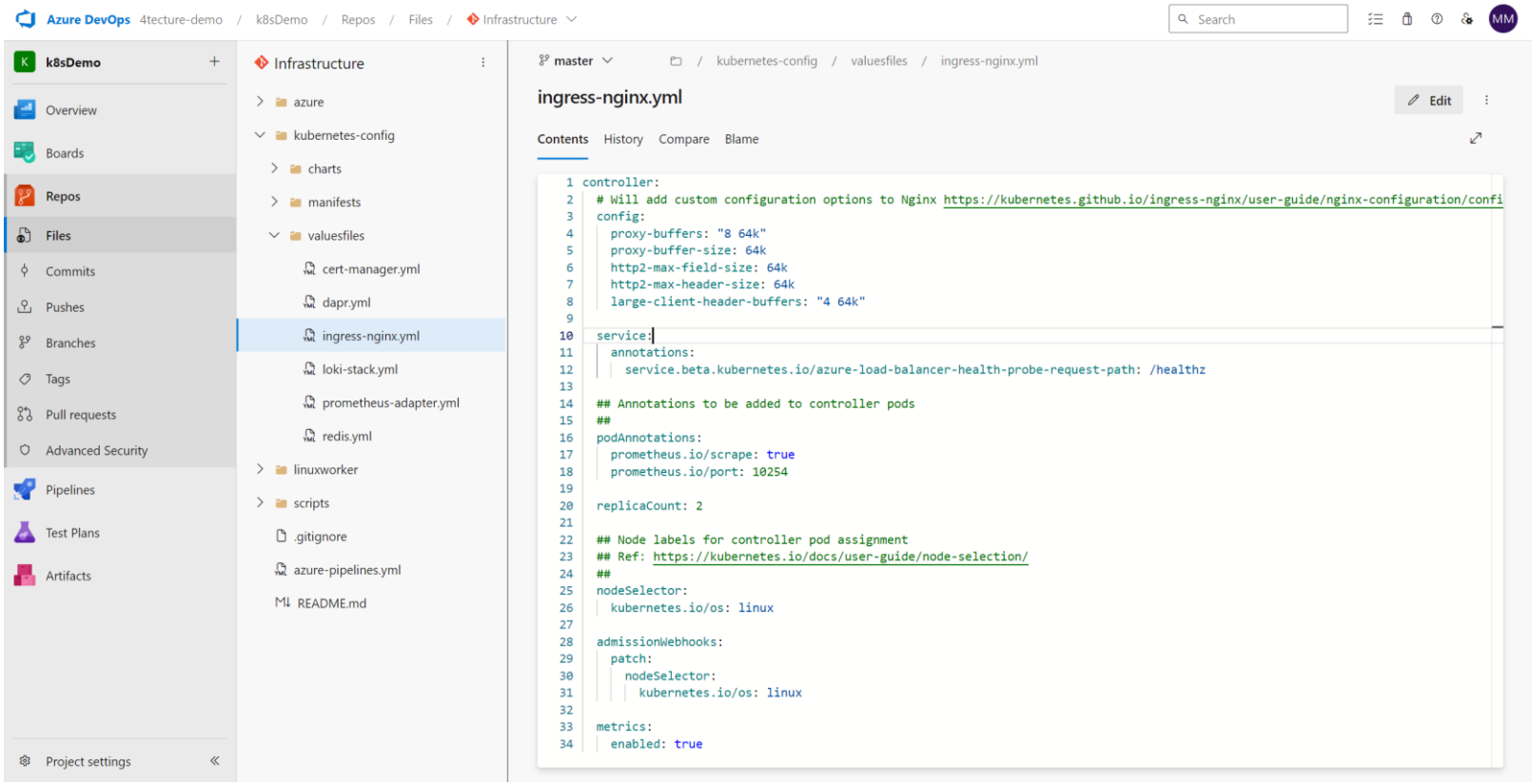
```
64 param agentVmPatToken string
65
66
67 module vnet 'vnet.bicep' = {
68   name: 'vnetDeploy'
69   params: {
70     vnetName: '${prefix}-vnet-${clusterName}-${location}'
71     subnetName: '${prefix}-snet-${clusterName}-${location}'
72     vnetAddressPrefixes: vnetAddressPrefixes
73     subnetAddressPrefix: subnetAddressPrefix
74     tags: tags
75     location: location
76   }
77   scope: resourceGroup()
78 }
79
80 module privateDNS 'privatedns.bicep' = {
81   name: 'privateDNSDeploy'
82   params: {
83     vnetId: vnet.outputs.vnetId
84     tags: tags
85     userAssignedIdentityPrincipalId: aksidentity.outputs.identityPrincipalId
86   }
87   dependsOn: [
88     vnet
89   ]
90 }
91
92 module aksidentity 'aksidentity.bicep' = {
93   name: 'aksidentityDeploy'
94   params: {
95     clusterName: clusterName
96     prefix: prefix
97     tags: tags
98     location: location
99   }
100 }
101
102
103 module aks 'aks.bicep' = {
104   name: 'aksDeploy'
105   params: {
106     prefix: prefix
107     clusterName: clusterName
108     subnetId: vnet.outputs.subnetId
109     nodeAdminUsername: nodeAdminUsername
110     adminGroupObjectIDs: adminGroupObjectIDs
```


DEMO
K8s Cluster Configuration

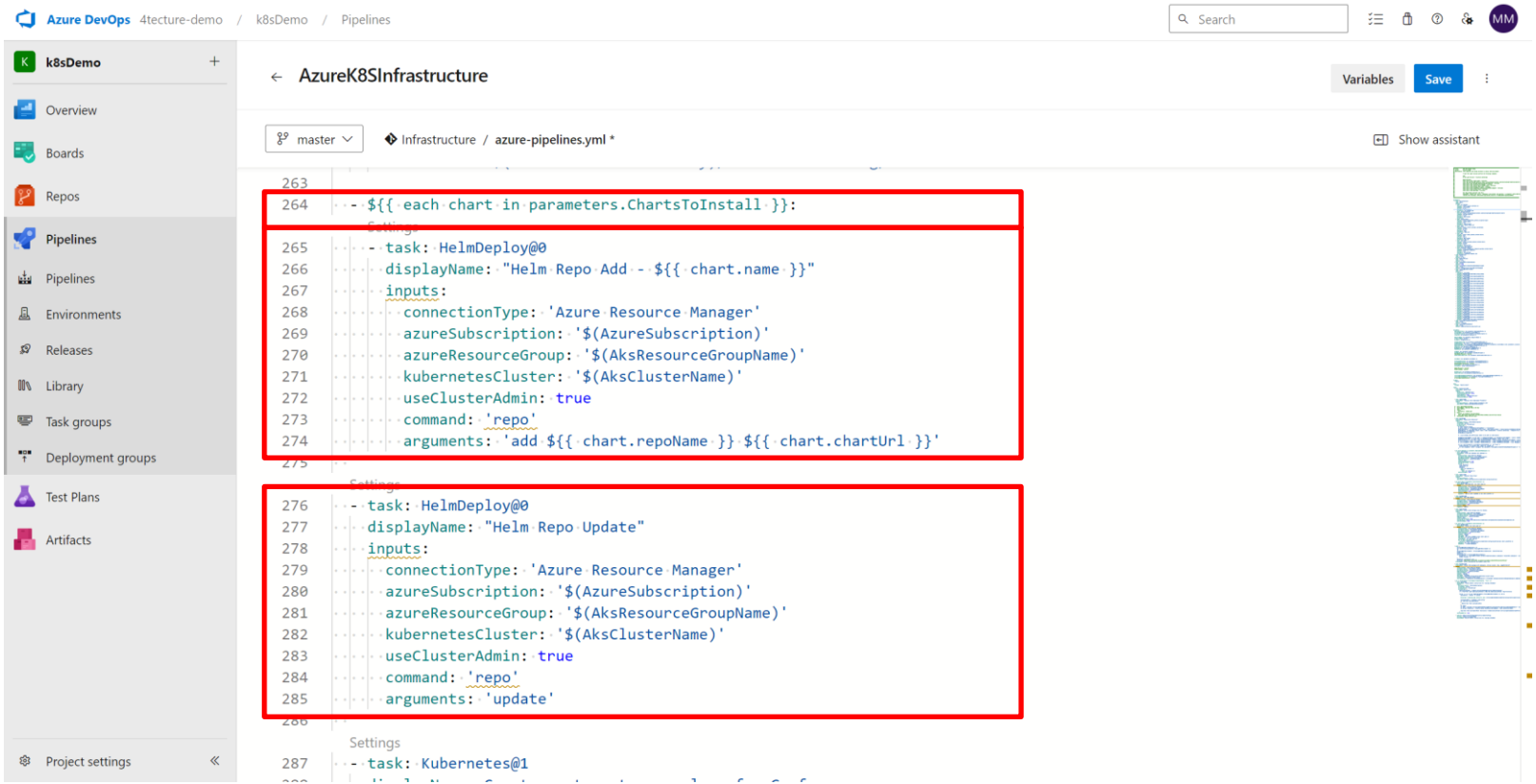
Parameter with all charts



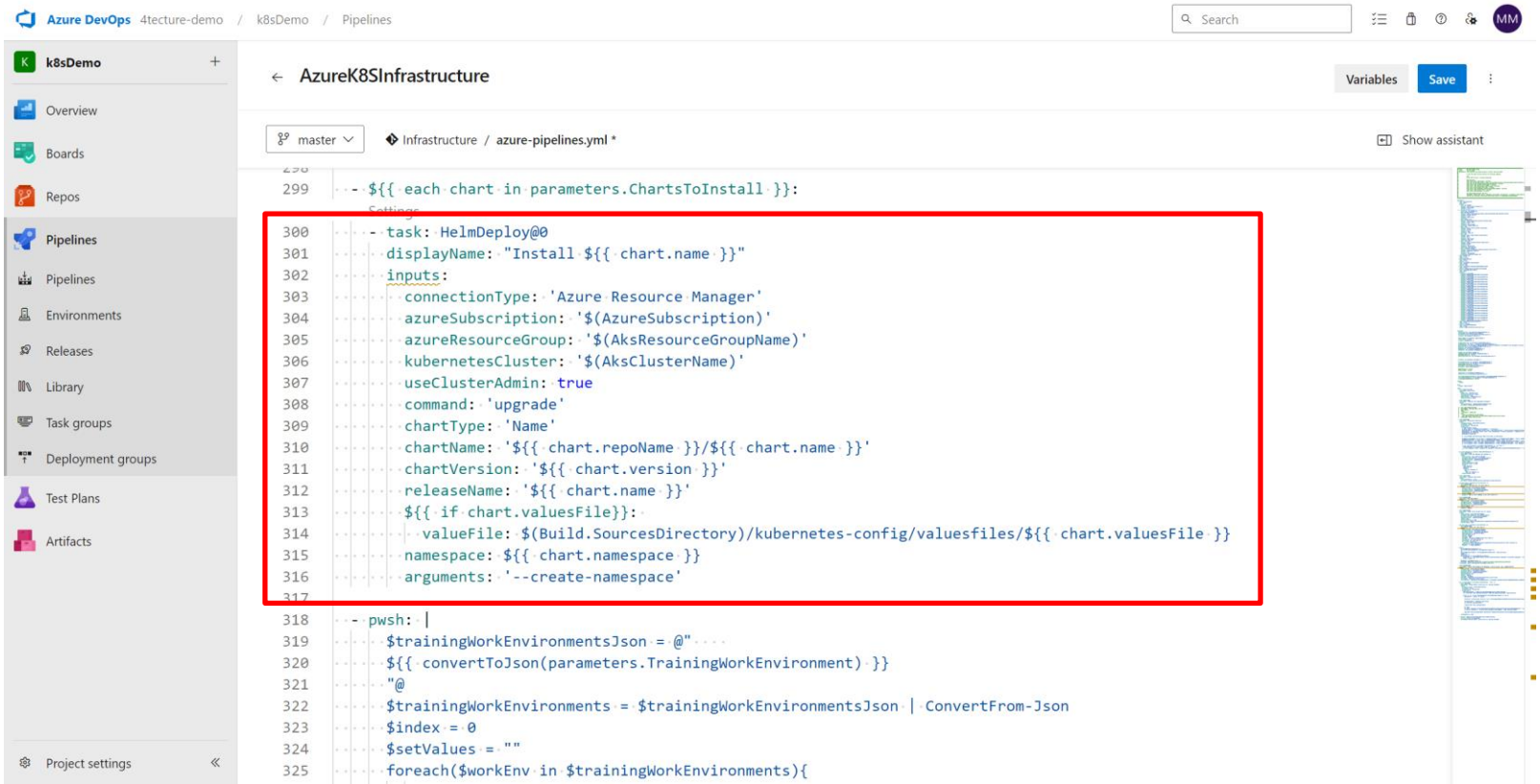
Configuration as Code



Add and update Helm Repos



Install helm charts



Azure Deployments

Traditional CI/CD vs. GitOps

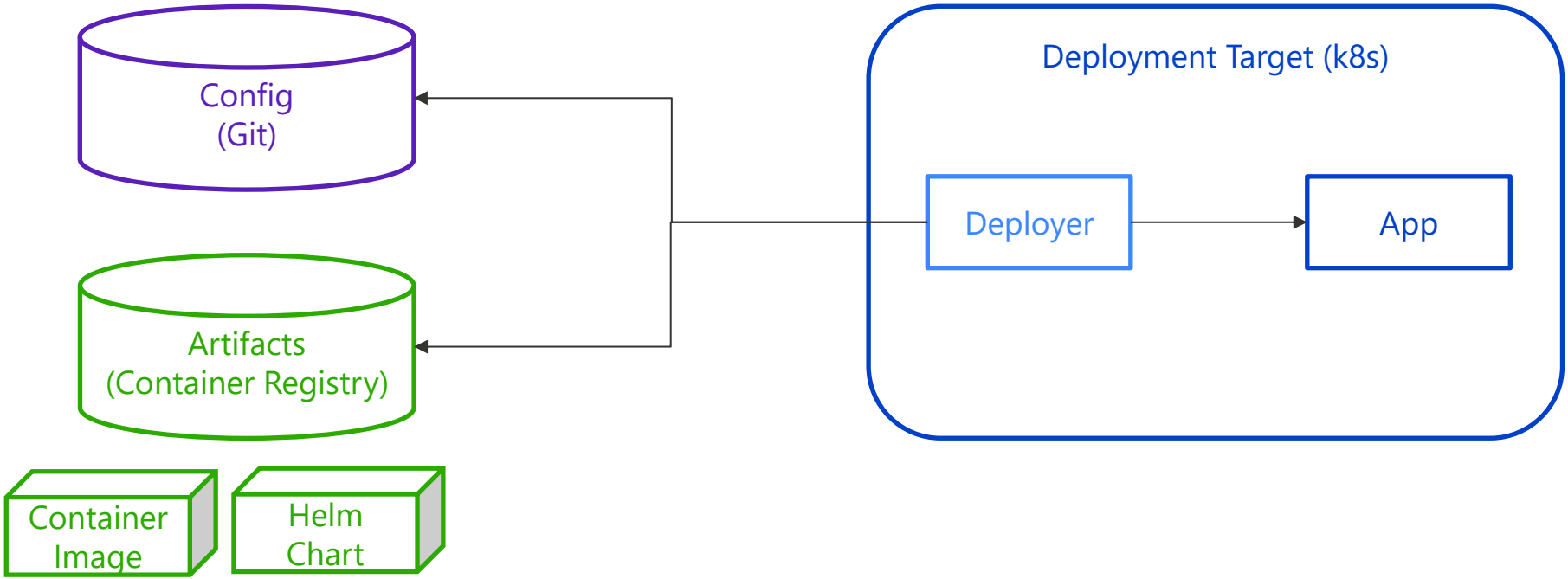
4tecture
empower your software solutions


KEEP
CALM
AND
GIT COMMIT
GIT PUSH ORIGIN MAIN
imgflip.com

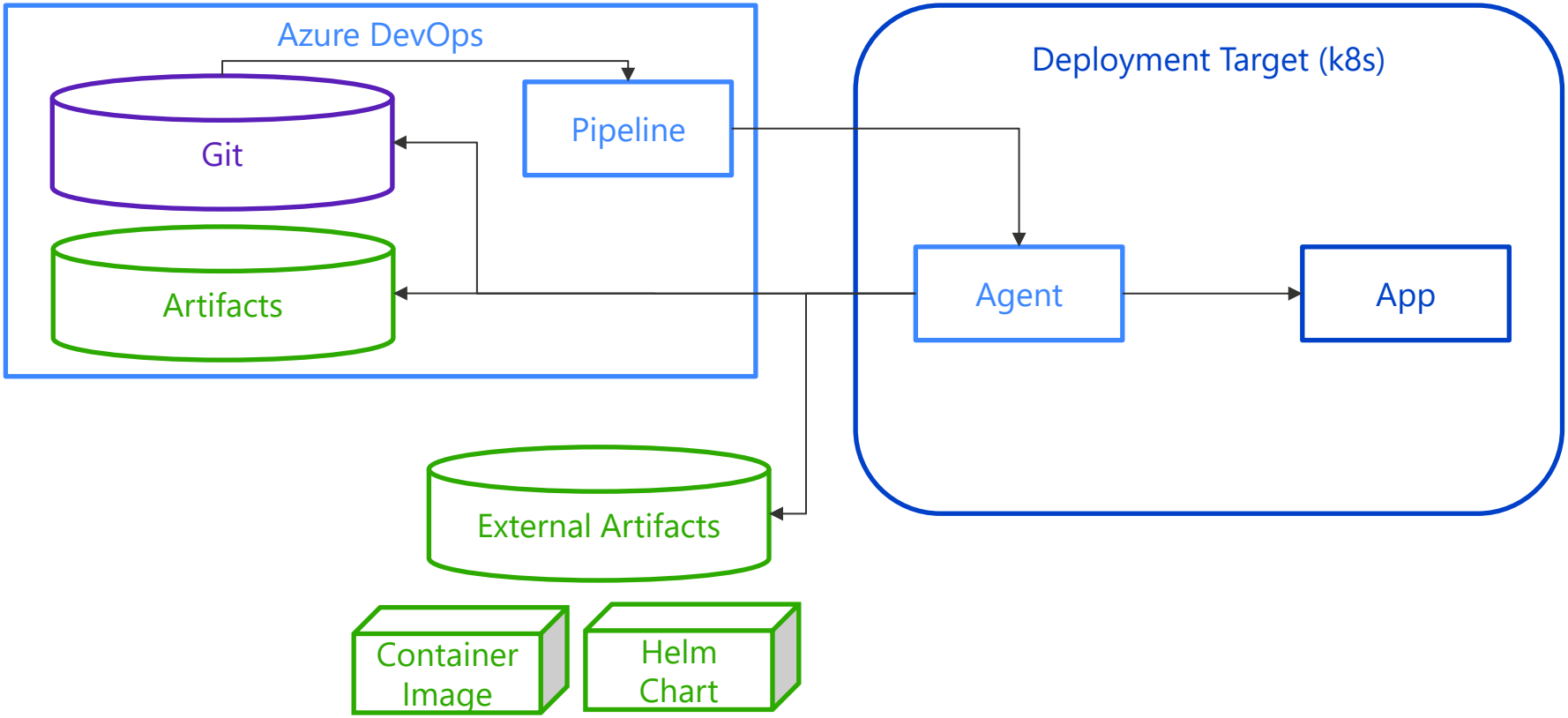
GitOps

By following these principles, GitOps aims to make operations and deployment more consistent, repeatable, and secure.

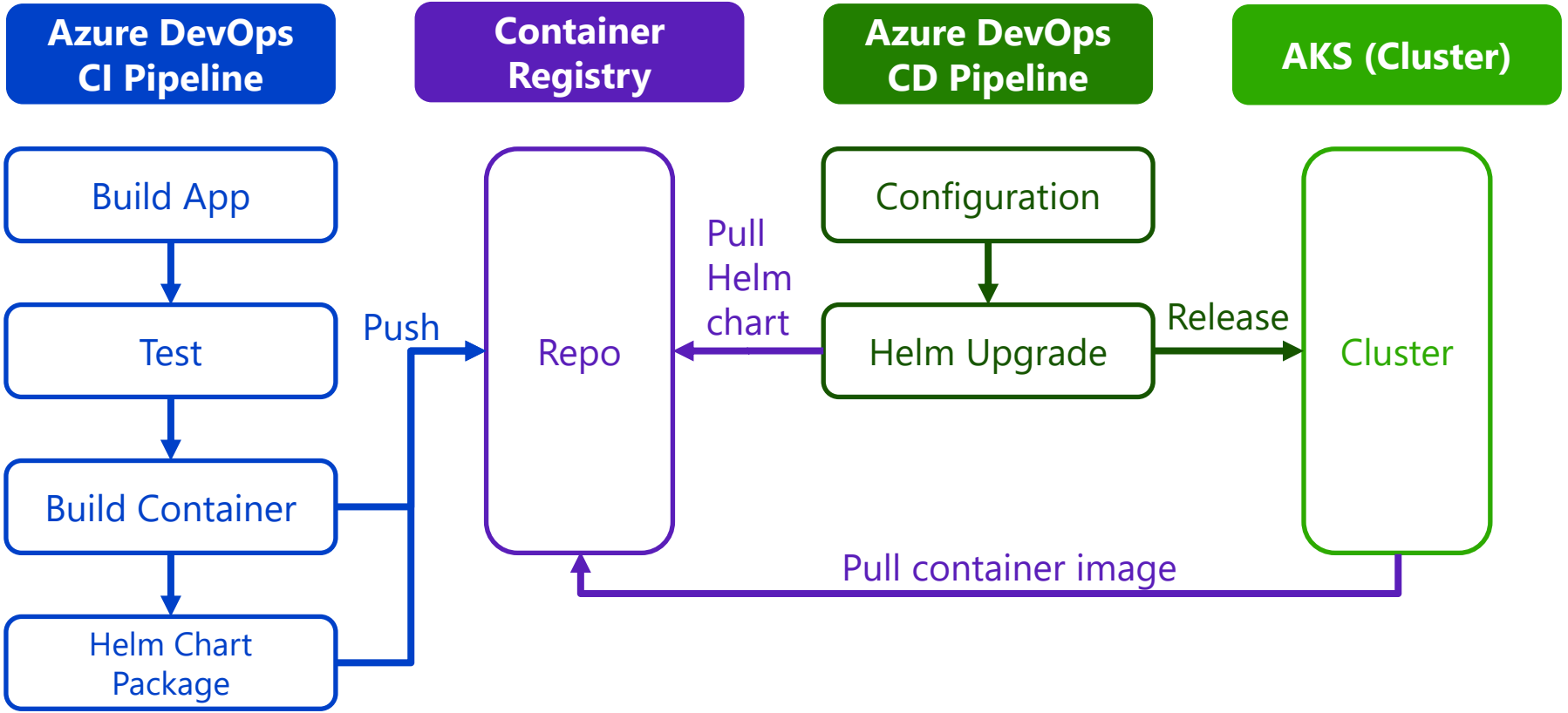
General Setup



Azure DevOps

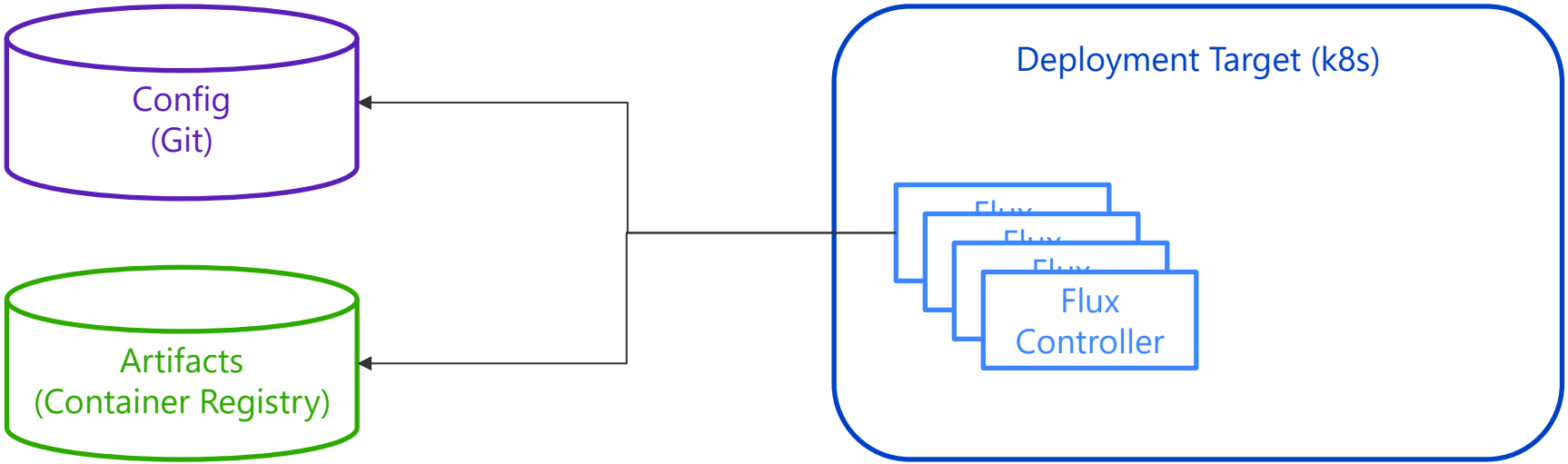


Azure DevOps & AKS CI / CD

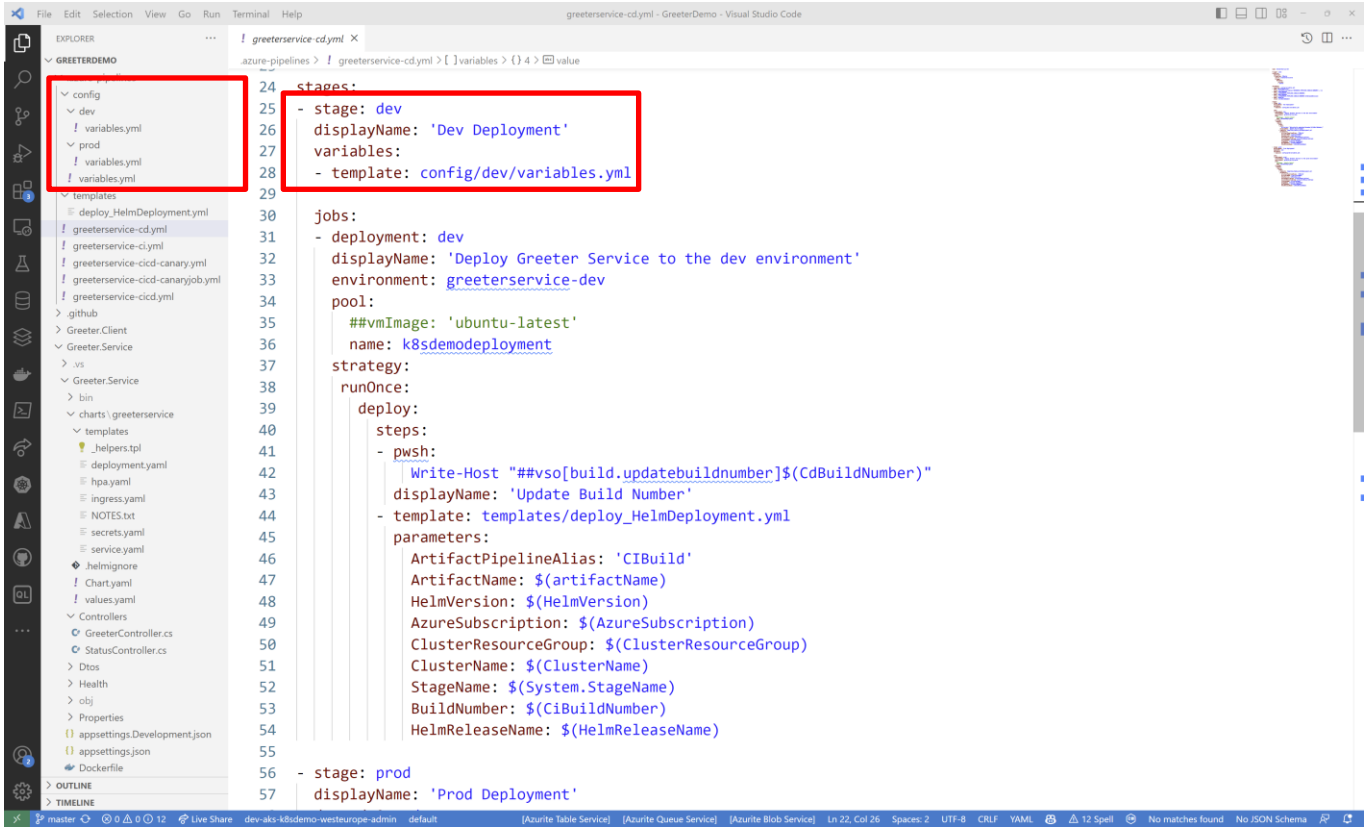


FluxCD

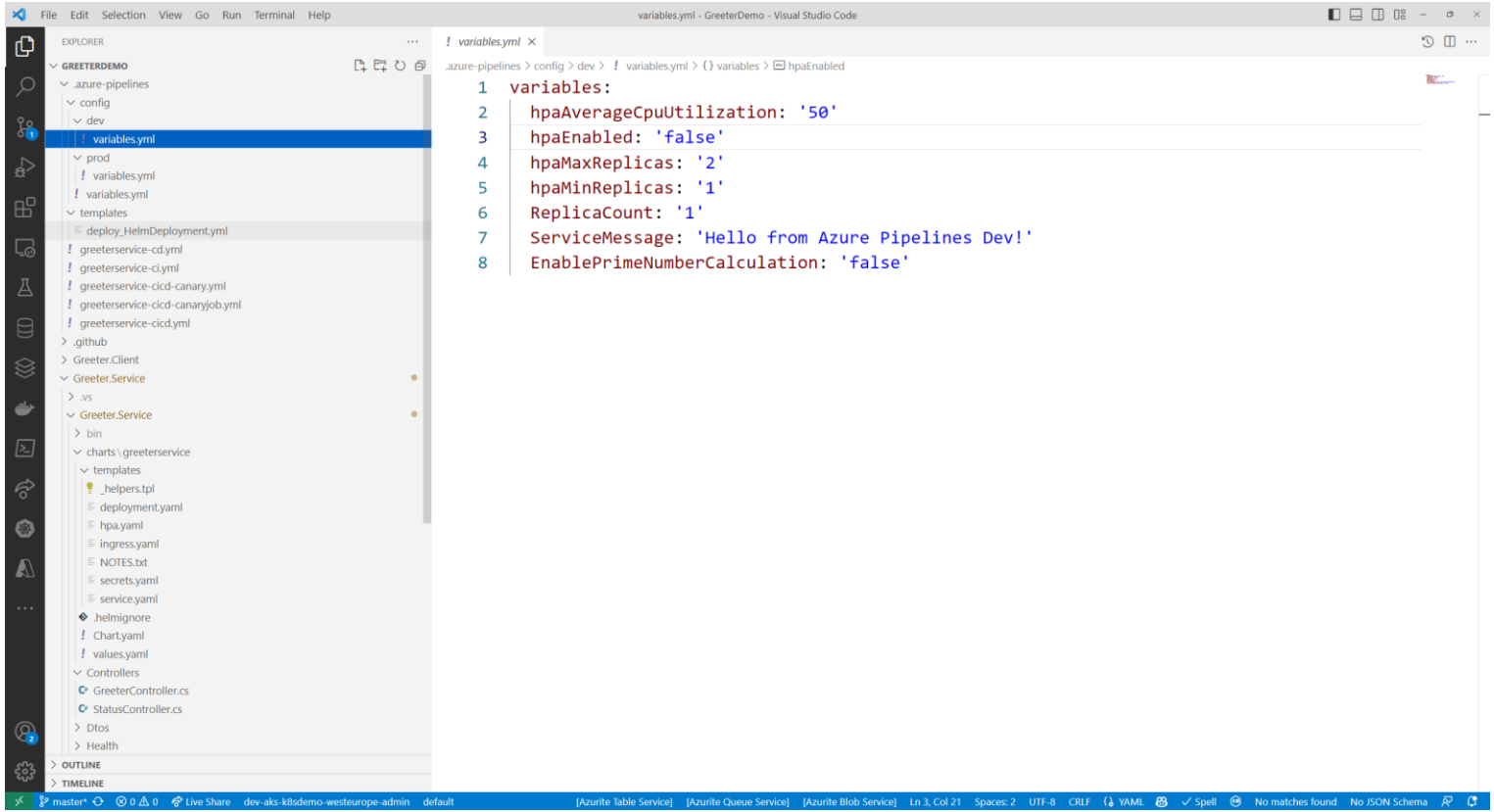
- Install the CLI
- Installation in k8s
  - flux bootstrap
  - flux install
  - Add kustomizations, sources, …



Dedicated Settings per Stage



Dedicated Settings per Stage



Comparison

Pipelines

- Everything in Git
- Versatile
- Full DevOps Lifecycle
- End-to-end Traceability
- Integrated Test Automation

Flux

- Everything in Git
- K8s Deployments
- Focus on Continuous Deployment
- Independent / Various Sources

Azure Deployments

Agents

4tecture
empower your software solutions

The Agent

- Multi-purpose task executer
- Executes any task
- Orchestration by Azure Pipelines

Considerations / Challenges

- Tool Dependencies
- Build old and new states of the repo
- Network access / restrictions
- Scaling
- Caching

Agent Hosting Options

Hosted Agent

- Cloud-Only
- Fixed image for Windows, Linux, Mac
- Monthly fee per parallel agent instance
- Job duration limits

Virtual Machine Scale Set Pool

- Cloud-Only
- Run agents in your VMSS resource
- Scaled by Azure DevOps Services
- You provide VM images
- Configurable VM resources

Managed DevOps Pool

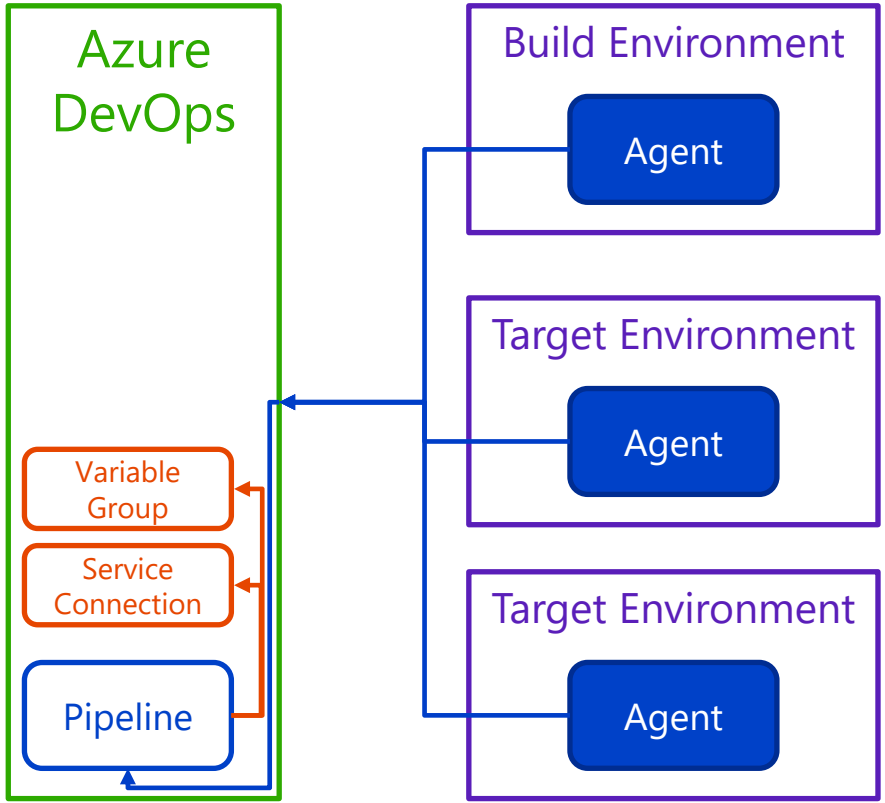
- Cloud-Only
- Hosted on your behalf
- Quick-starter images and custom images
- Stateful agents
- Private networking
- Configurable VM resources

Private Agent

- Runs everywhere
- Self-installed
- Self-scaled

Agent Deployment

- Agent per Purpose (build, deploy target)
- Agent as near as possible to deployment target
- Connectivity from inside-out, no hole punching, isolate networking
- Least privileged
- Use secret from Azure DevOps, per environment vault instance
- Permit resource usage per pipeline




DEMO
Private Agent in VM

azdoagentvm.bicep

Edit

Contents History Compare Blame

```bicep
@description('The environment prefix of the Managed Cluster resource e.g. dev, prod, etc.')
param prefix string
@description('The name of the Managed Cluster resource')
param clusterName string
@description('Tags for the resources')
param tags object
@description('Location')
param location string = resourceGroup().location
param adminUsername string
@secure()
param adminPassword string
param vmSize string = 'Standard_B2s'
param subnetId string
param agentPool string
param agentName string
param azdoUrl string
@secure()
param patToken string

resource publicIP 'Microsoft.Network/publicIPAddresses@2020-11-01' = {
  name: '${prefix}-agentvm-${clusterName}-${location}-pip'
  location: location
  properties: {
    publicIPAllocationMethod: 'Dynamic'
  }
}

resource networkInterface 'Microsoft.Network/networkInterfaces@2020-11-01' = {
  name: '${prefix}-agentvm-${clusterName}-${location}-nic'
  location: location
  properties: {
    ipConfigurations: [
      {
        name: 'ipconfig1'
        properties: {
          privateIPAllocationMethod: 'Dynamic'
          subnet: {
            id: subnetId
          }
          publicIPAddress: {
            id: publicIP.id
          }
        }
      }
    ]
  }
}
```

Demo Recap

k8sDemo

Overview
Boards
Repos
Files
Commits
Pushes
Branches
Tags
Pull requests
Advanced Security
Pipelines
Test Plans
Artifacts

Project settings

Infrastructure

azure
aks.bicep
aksidentity.bicep
azdoagentvm.bicep
k8senvironment-dev.param
k8senvironment.bicep
k8senvironment.parameters
privatedns.bicep
rbac.bicep
registry.bicep
sql.bicep
vnet.bicep
deploymentagent
kubernetes-config
linuxworker
scripts
.gitignore
azure-pipelines.yml
README.md

feature/privateEndpoints / azure / azdoagentvm.bicep

azdoagentvm.bicep

Edit

Contents History Compare Blame

```
48
49 resource virtualMachine 'Microsoft.Compute/virtualMachines@2021-04-01' = {
50   name: '${prefix}-agentvm-${clusterName}-${location}'
51   location: location
52   properties: {
53     hardwareProfile: {
54       vmSize: vmSize
55     }
56     osProfile: {
57       computerName: 'agentvm'
58       adminUsername: adminUsername
59       adminPassword: adminPassword
60       linuxConfiguration: {
61         disablePasswordAuthentication: false
62       }
63     }
64     storageProfile: {
65       imageReference: {
66         publisher: 'Canonical'
67         offer: 'UbuntuServer'
68         sku: '18.04-LTS'
69         version: 'latest'
70       }
71       osDisk: {
72         createOption: 'FromImage'
73       }
74     }
75     networkProfile: {
76       networkInterfaces: [
77         {
78           id: networkInterface.id
79         }
80       ]
81     }
82   }
83   tags: tags
84 }
85
86 resource customScriptExtension 'Microsoft.Compute/virtualMachines/extensions@2021-04-01' = {
87   parent: virtualMachine
88   name: 'installAgent'
89   location: location
90   properties: {
91     publisher: 'Microsoft.Azure.Extensions'
92     type: 'CustomScript'
93     typeHandlerVersion: '2.0'
94     autoUpgradeMinorVersion: true
```

Demo Recap

azdoagentvm.bicep

Edit

Contents History Compare Blame

```
  tags: tags
}

resource customScriptExtension 'Microsoft.Compute/virtualMachines/extensions@2021-04-01' = {
  parent: virtualMachine
  name: 'installAgent'
  location: location
  properties: {
    publisher: 'Microsoft.Azure.Extensions'
    type: 'CustomScript'
    typeHandlerVersion: '2.0'
    autoUpgradeMinorVersion: true
    settings: {
      script: base64(concat('''
        #!/bin/bash

        # Variables
        AGENT_POOL="''', agentPool, '''"
        AGENT_NAME="''', agentName, '''"
        AZDO_URL="''', azdoUrl, '''"
        PAT_TOKEN="''', patToken, '''"

        # Update the system
        apt-get update
        apt-get upgrade -y

        # Install prerequisites
        apt-get install -y liblttng-ust0 libkrb5-3 zlib1g libicu60 libssl1.0.0 libssl1.0.2 libssl1.1 unzip

        # Download the Azure DevOps agent
        wget https://vstsagentpackage.azureedge.net/agent/3.227.2/vsts-agent-linux-x64-3.227.2.tar.gz
        mkdir myagent && cd myagent
        tar zxvf ../vsts-agent-linux-x64-3.227.2.tar.gz

        # Allow running as root
        export AGENT_ALLOW_RUNASROOT="1"

        # Configure the agent
        ./config.sh --url $AZDO_URL --auth pat --token $PAT_TOKEN --pool $AGENT_POOL --agent $AGENT_NAME --replace --acceptTeeEula --runAsService --unatt

        # Install the agent service
        ./svc.sh install
        ./svc.sh start
      '''))
    }
  }
}
```


DEMO
Managed DevOps Pool

Subscriptions

4tecture Demo Environment

Add | Advanced options

Global administrators can manage all subscriptions in this list by updating their policy setting here.

View list of subscriptions for which you have role-based access control (RBAC) permissions to manage Azure resources. To view subscriptions for which you have billing access, click here
Showing subscriptions in 4tecture Demo Environment directory. Don't see a subscription? Switch directories

S... | Subscriptions : **Filtered (1 of 1)** | My role == **all** | Status == **all** | Add filter

Subscription name

Microsoft Azure Sponsorship

Microsoft Azure Sponsorship | Resource providers

Subscription

Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Security
- Events
- Billing
- Settings
  - Programmatic deployment
  - Resource groups
  - Resources
  - Preview features
  - Usage + quotas
  - Policies
  - My permissions
  - Resource providers
  - Deployments
  - Deployment stacks
  - Properties
  - Resource locks
- Help

Register | Unregister | Refresh | Feedback

devops | Status : **All** | Registration Policy : **All**

Provider	Status	Registration Policy
Microsoft.DevOpsInfrastructure	Registering	RegistrationRequired

Demo Recap

Create a Managed DevOps Pool

Managed DevOps Pools that meet your team needs.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Microsoft Azure Sponsorship

Resource group * : DemoMDP

Create new

Instance details

Dev Center * : (New) DemoDevCenter

Dev Center project * : (New) Demo

Create new Dev Center and project

Azure DevOps organization * : https://dev.azure.com/ 4t[redacted]no

Pool name * : DemoMDP

This pool will be created in every project in the Azure DevOps organization that is selected. If you want to add this pool only to specific projects, use the security tab to limit the projects it will be visble in.

Region * : (Europe) West Europe

Maximum agents * : 2

Agent size * :

Name	Cores	RAM	
Standard D2ads v5	2	8	Change size

Demo Recap

Create a Managed DevOps Pool

Managed DevOps Pools that meet your team needs.

Basics | Scaling | Networking | Storage | Security | Tags | Review

Pool name * DemoMDP

This pool will be created in every project in the Azu that is selected. If you want to add this pool only t the security tab to limit the projects it will be visble

Region * (Europe) West Europe

Maximum agents * 2

Agent size *

	Name	Cores	RAM
	Standard D2ads v5	2	8

OS disk type Standard

Images

Pick one or more from Images with which to create our CI/CD agents.

+ Add from Image Library

Name	Version	Aliases
Ubuntu Server 20.04 LTS - x64 Gen 2	latest	

Previous | Next | Review + create

Image Library

Azure Pipelines Images | Selected marketplace images | Azure Compute Gallery images

These are Quickstarter VM images that contain the most commonly used software. They are the same VM images used by the Microsoft Hosted Azure Pipelines agents. These images can be used to get started quickly but we recommend creating a VM image with exactly the software your CI/CD pipelines need. All of these images are Gen 1(V1) and x64 architecture.

Name & plan	Description
Azure Pipelines - Windows Server 2022	VM Image used by Microsoft Hosted Agents. View full list of software.
Azure Pipelines - Windows Server 2019	VM Image used by Microsoft Hosted Agents. View full list of software.
Azure Pipelines - Ubuntu 22.04	VM Image used by Microsoft Hosted Agents. View full list of software.
Azure Pipelines - Ubuntu 20.04	VM Image used by Microsoft Hosted Agents. View full list of software.

Add | Cancel

Demo Recap

Create a Managed DevOps Pool

Managed DevOps Pools that meet your team needs.

Defaults are selected to keep your total cost low. If you want your agents to be more powerful or to be assigned to your pipelines faster, you will have to chose the right option to balance cost and performance.

Agent state

- ○ Fresh agent every time
- ◉ Same agent can be reused by multiple builds

Standby agent mode

- ◉ Off
  Standby agent mode off.
- ○ Manual
  If you know your workloads' usage patterns, you can configure standby agents as per the scale conditions.
- ○ Automatic
  If you don't know your usage patterns, you can rely on automatic forecasting based on past data.

Max time to live * 7.00:00:00

Grace period * 0.00:15:00

Demo Recap

Create a Managed DevOps Pool

Managed DevOps Pools that meet your team needs.

You can use features in this section to control networking settings of your agents.

Virtual network type

- ○ Isolated virtual network
- ◉ Agents injected into existing virtual network

Subnet resource

Subscription Id:
Resource group:
Virtual network:
Subnet:
Configure

Subnet resource

Subscription * Microsoft Azure Sponsorship

Virtual Network * ServiceCluster-VNet

Subnet * ServiceCluster-AksSubnet

Demo Recap

Ok Cancel

Create a Managed DevOps Pool

Managed DevOps Pools that meet your team needs.

You can use features in this section to improve security of your agents.

Use pool in multiple organizations ☐

Add pool to all projects
- ◉ Yes
- ○ No

Enable Interactive Mode ☐

Pool Administration Permissions

Choose who will be able to administer the pool that will be created

Pool Administration Permissions
- ◉ Creator only
- ○ Inherit permissions from project
- ○ Specific accounts

DemoMDP

Managed DevOps Pool

Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Monitoring
Automation
Help

Delete Refresh

Essentials

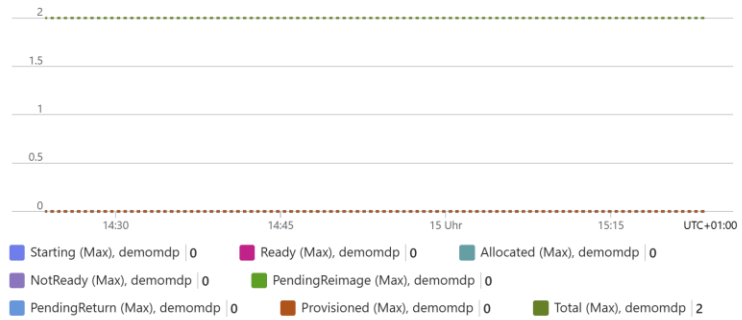
JSON View

Resource group (move)	: DemoMDP	Name	: DemoMDP
Location	: West Europe	Azure DevOps organizati...	: https://dev.azure.com/4tecture-demo
Subscription (move)	: Microsoft Azure Sponsorship	Agent state	: Stateful
Subscription ID	: 82d445a5-0bf3-454a-804b-2fd0286650c2	Maximum agents	: 2
Tags (edit)	: Add tags		

Metrics

1h 1d 7d 30d

Pool Usage



Pool Usage Chart Legend

Starting: Number of Azure DevOps Agents being prepared
Ready: Number of Azure DevOps Agents present that are prepared to accept a job
Allocated: Number of Azure DevOps Agents with jobs currently running
NotReady: Number of Azure DevOps Agents present that are not yet completely set up for testing
PendingReimage: Number of Azure DevOps Agents in the process of being reimaged
PendingReturn: [Azure only] Number of Azure DevOps Agents that are post-cleanup, waiting to be deleted (which occurs in batc...
Provisioned: Number of Azure DevOps Agents currently up
Total: Total number of Azure DevOps Agents

Pool Provisioning Health

Request Durations

Demo Recap

Search

MM

Project Settings

k8sDemo

General

- Overview
- Teams
- Permissions
- Notifications
- Service hooks
- Dashboards

Boards

- Project configuration
- Team configuration
- GitHub connections

Pipelines

- Agent pools
- Parallel jobs
- Settings
- Test management
- Release retention
- Service connections
- XAML build services

Repos

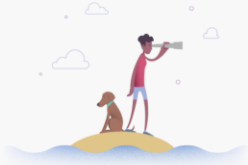
- Repositories

Artifacts

- Storage

DemoMDP

Jobs | Details | Security | Approvals and checks | Analytics



No jobs have run on this agent pool

Run a pipeline on this agent pool to see more details

Demo Recap

Azure Deployments

Dynamic Deployments

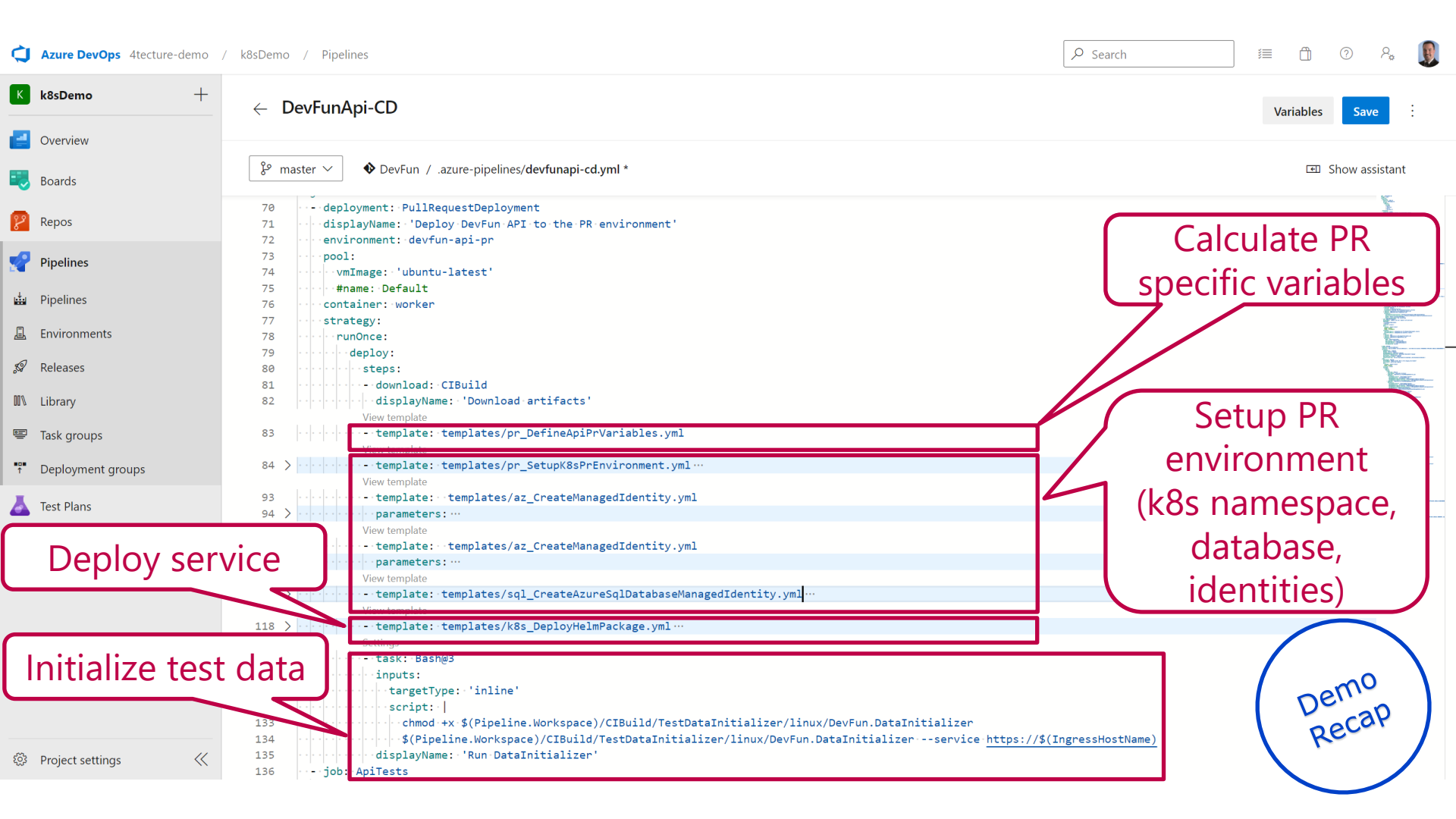
4tecture
empower your software solutions

PR Resources

Why Pull Request Deployments?

- Fail fast – learn fast & fix fast
- Only an integrated change provides clarity if it runs successfully in production
- Pull Request is single point of interaction / status for developers, testers and product owners
- Pipelines with conditions, templates and integration in PR API provide all the tools you need


DEMO
PR Deployment (Resources)


Azure DevOps 4tecture-demo / k8sDemo / Pipelines
Search
k8sDemo
Overview
Boards
Repos
Pipelines
Pipelines
Environments
Releases
Library
Task groups
Deployment groups
Test Plans
Project settings
DevFunApi-CD
Variables
Save
master
DevFun / .azure-pipelines/devfunapi-cd.yml *
Show assistant
- deployment: PullRequestDeployment
displayName: 'Deploy DevFun API to the PR environment'
environment: devfun-api-pr
pool:
vmImage: 'ubuntu-latest'
#name: Default
container: worker
strategy:
runOnce:
deploy:
steps:
- download: CIBuild
displayName: 'Download artifacts'
View template
- template: templates/pr_DefineApiPrVariables.yml
- template: templates/pr_SetupK8sPrEnvironment.yml
View template
- template: templates/az_CreateManagedIdentity.yml
parameters:
View template
- template: templates/az_CreateManagedIdentity.yml
parameters:
View template
- template: templates/sql_CreateAzureSqlDatabaseManagedIdentity.yml
- template: templates/k8s_DeployHelmPackage.yml
- task: Bash@3
inputs:
targetType: 'inline'
script: |
chmod +x $(Pipeline.Workspace)/CIBuild/TestDataInitializer/linux/DevFun.DataInitializer
$(Pipeline.Workspace)/CIBuild/TestDataInitializer/linux/DevFun.DataInitializer --service https://$(IngressHostName)
displayName: 'Run DataInitializer'
- job: ApiTests
Calculate PR specific variables
Setup PR environment (k8s namespace, database, identities)
Deploy service
Initialize test data
Demo Recap

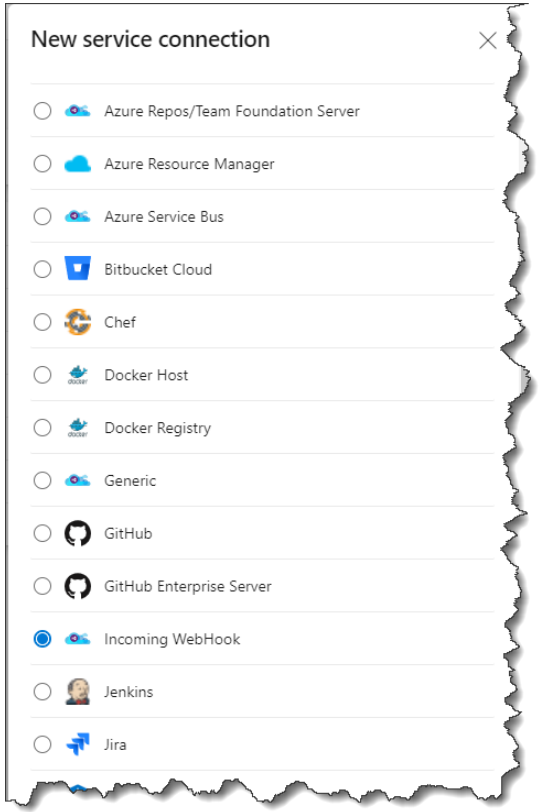
Cleanup

Trigger

- Main triggers are repository / code related
- Many automation scenarios trigger from other events
  - Work Item Update
  - Pull Request Update

Incoming Webhook Service Connection

- Incoming webhook can be defined as service connection
- Generic webhook trigger in pipelines
- Payload can be filtered



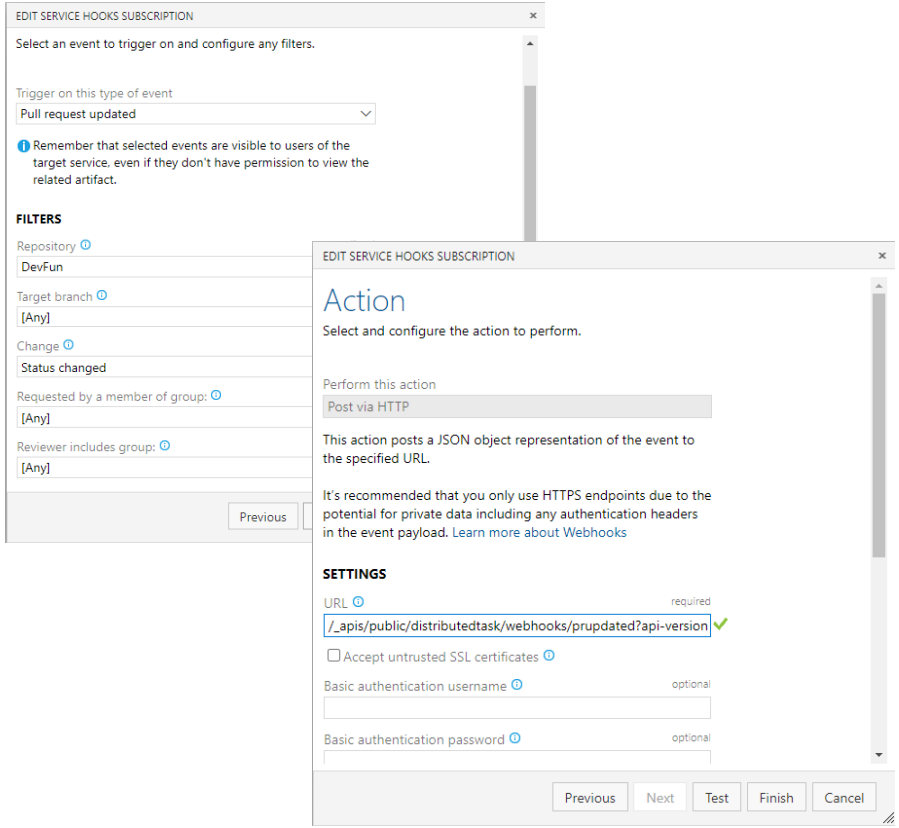
Pipeline Resource

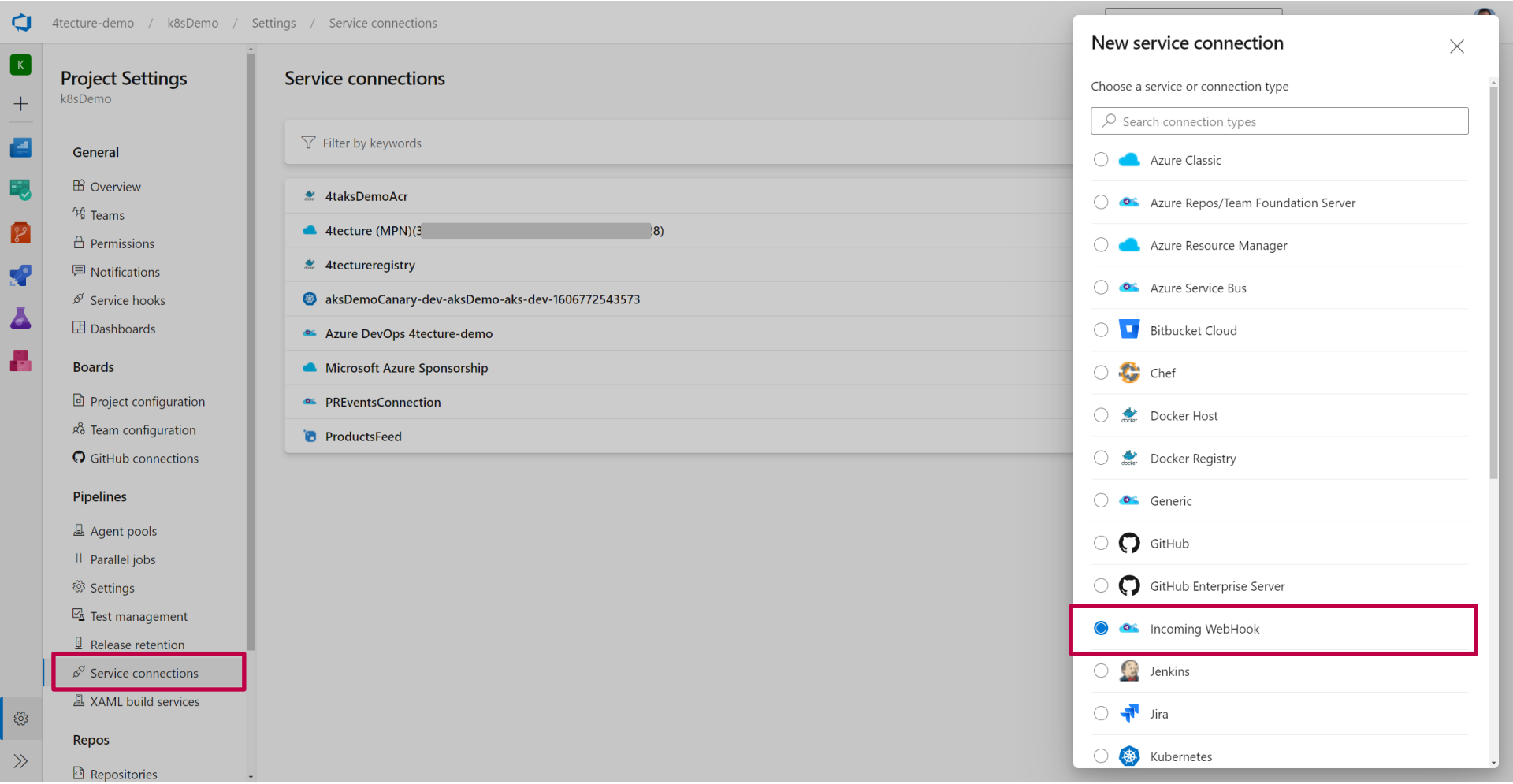
- Azure DevOps creates webhook endpoint based on alias
- Pipeline resource triggers pipeline
- Filters can be applied to trigger

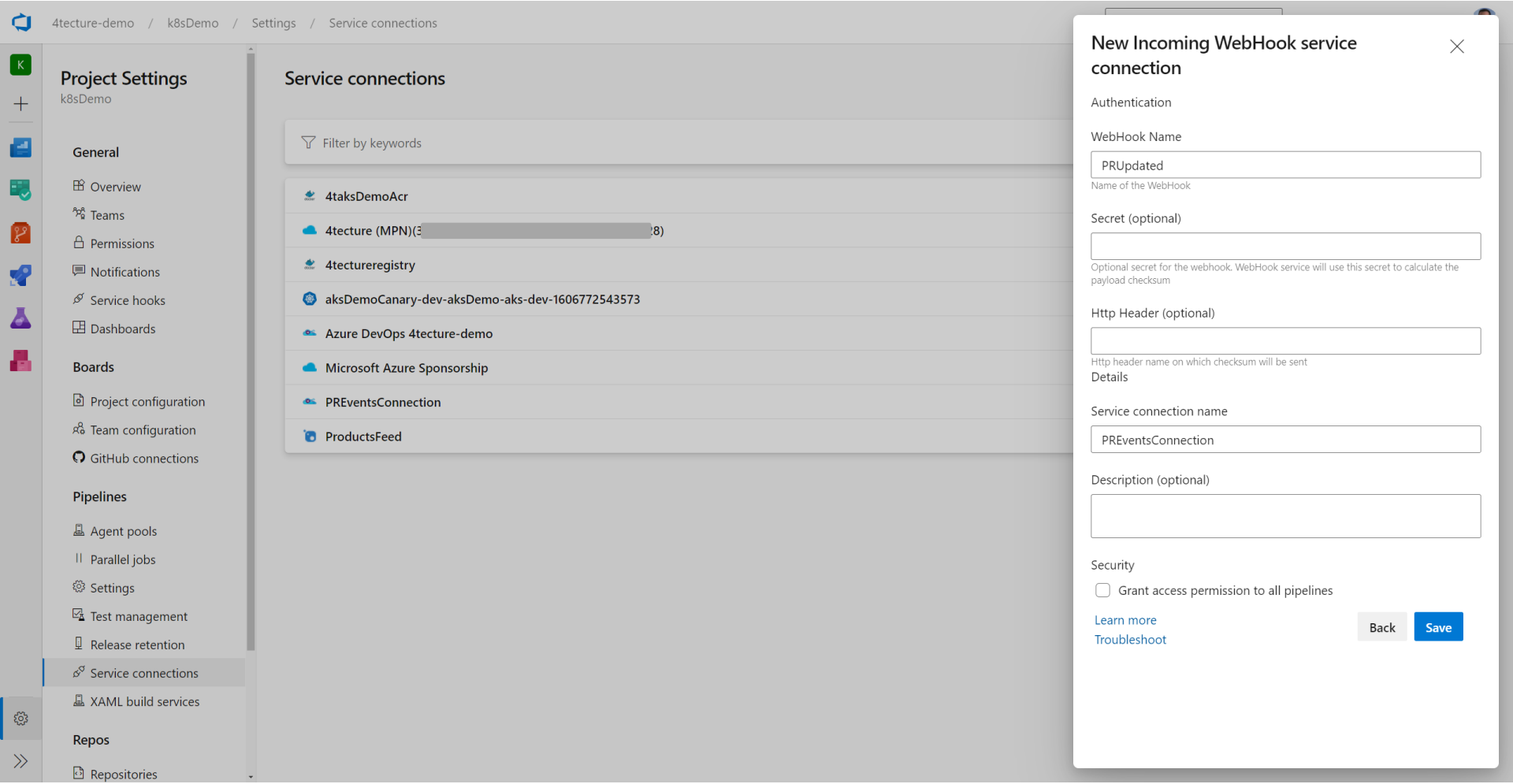
```yaml
trigger: none

pool:
  vmImage: ubuntu-latest

resources:
  # https://dev.azure.com/4tecture-demo/_apis/public/distributedtask/webhooks/prupdated?api-version=6.0-preview
  webhooks:
    - webhook: PRUpdated                ### Webhook alias
      connection: PREventsConnection    ### Incoming webhook service connection
      filters:
      - path: eventType
        value: git.pullrequest.updated
      - path: publisherId
        value: tfs
      - path: resource.repository.name
        value: DevFun

variables:
View template
- template: templates/common_variables.yml
View template
```

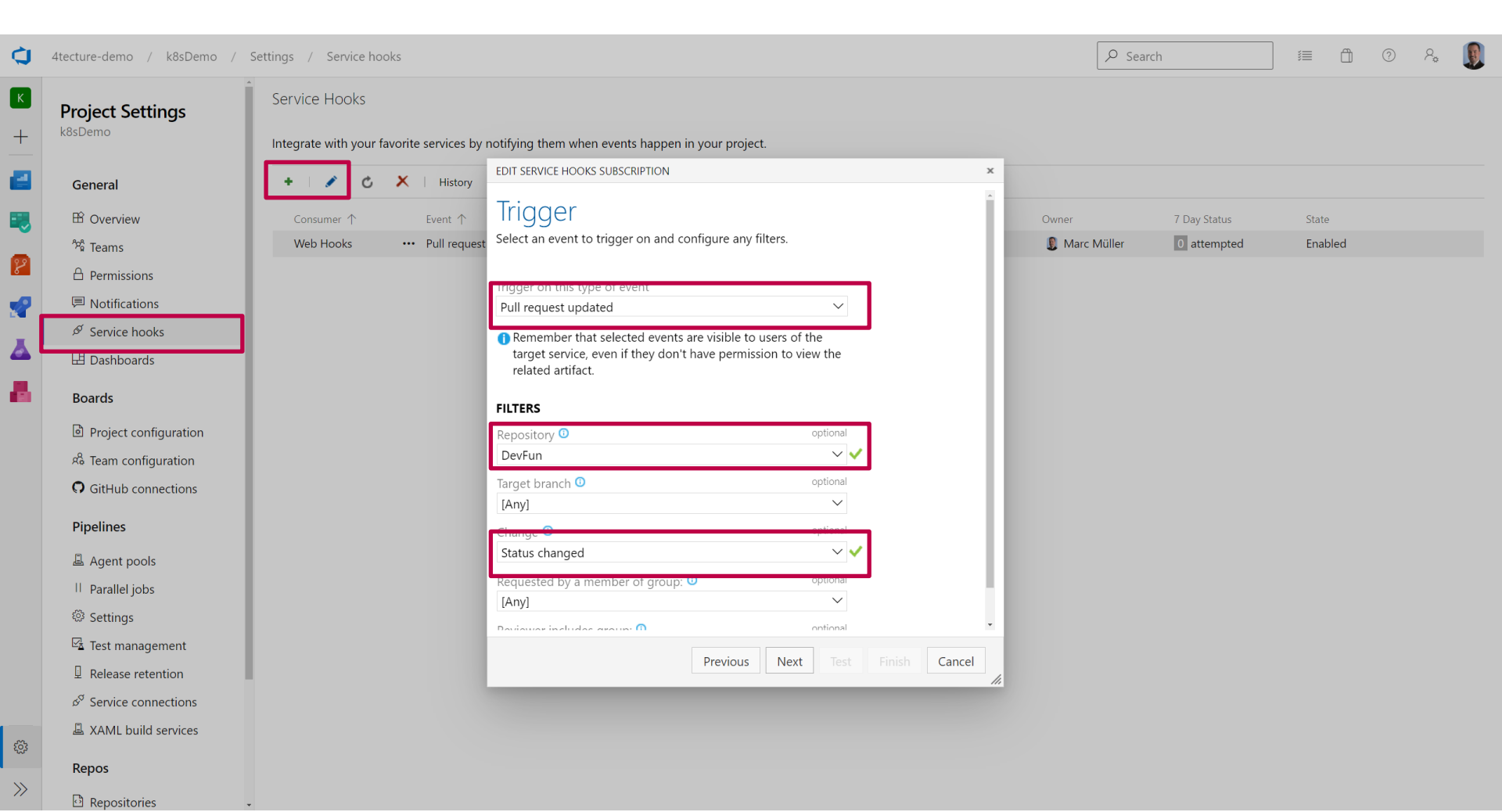
Service Hook & Incoming Webhook

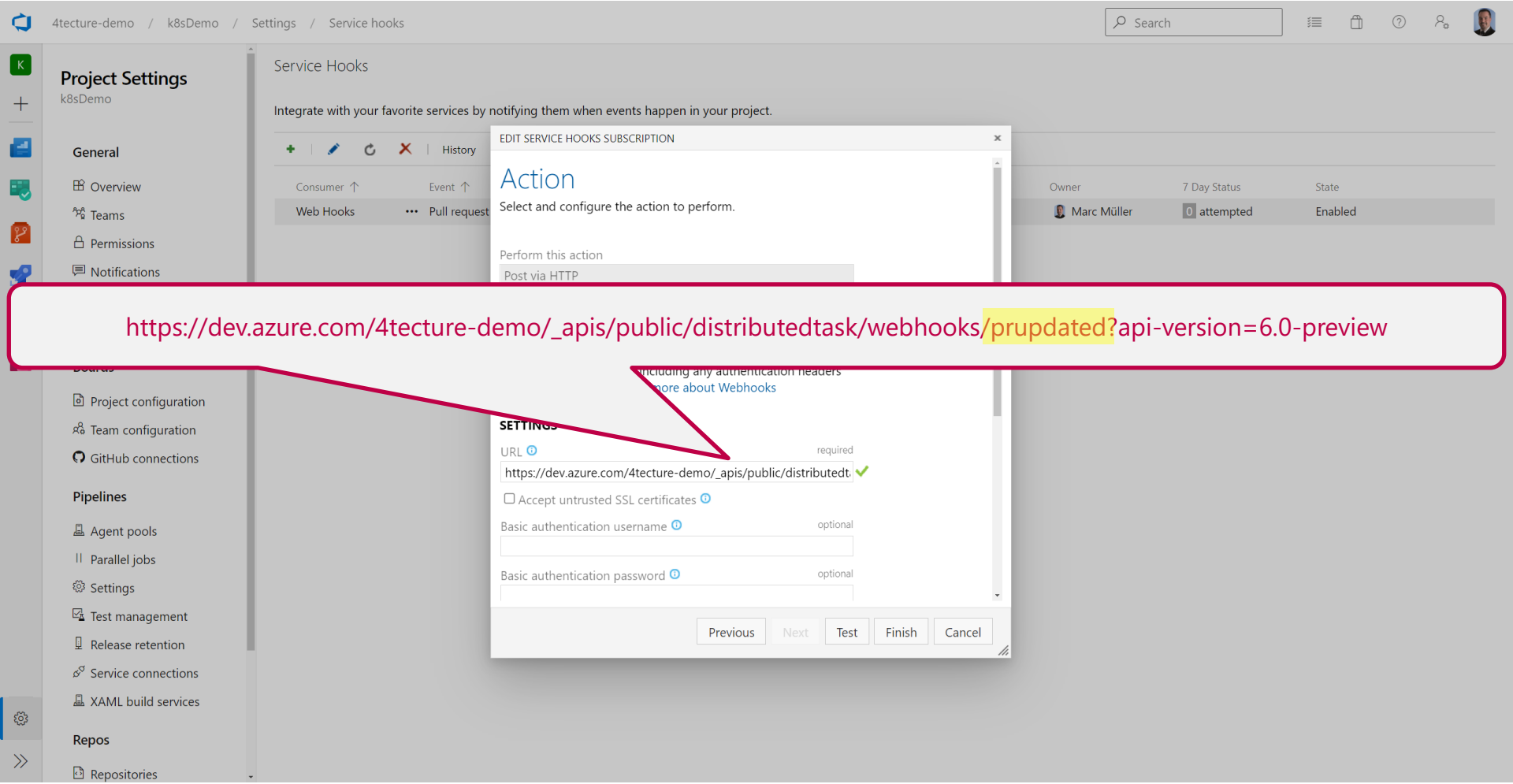
- Service hooks can trigger webhooks for many Azure DevOps Events
  - Build completed
  - Code pushed
  - Elastic agent pool resized
  - Pull request commented on
  - Pull request created
  - Pull request merge attempted
  - Pull request updated
  - Release abandoned
  - Release created
  - Release deployment approval completed
  - Release deployment approval pending
  - Release deployment completed
  - Release deployment started
  - Run stage approval completed
  - Run stage state changed
  - Run stage waiting for approval
  - Run state changed
  - Work item commented on
  - Work item created
  - Work item deleted
  - Work item restored
  - Work item updated

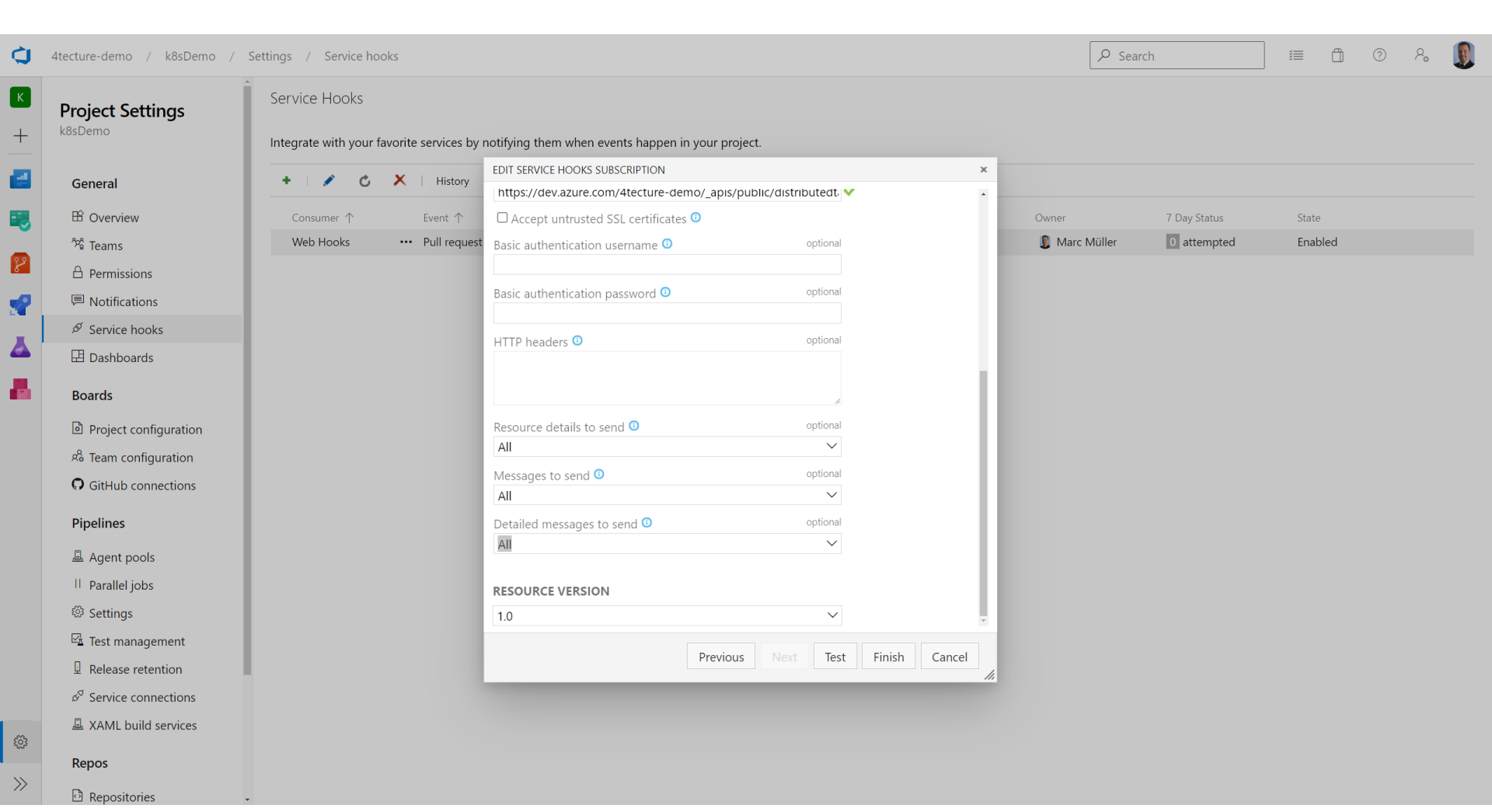



4tecture-demo / k8sDemo / Settings / Service connections
Project Settings
k8sDemo
General
Overview
Teams
Permissions
Notifications
Service hooks
Dashboards
Boards
Project configuration
Team configuration
GitHub connections
Pipelines
Agent pools
Parallel jobs
Settings
Test management
Release retention
Service connections
XAML build services
Repos
Repositories
Service connections
Filter by keywords
4taksDemoAcr
4tecture (MPN)(
8)
4tectureregistry
aksDemoCanary-dev-aksDemo-aks-dev-1606772543573
Azure DevOps 4tecture-demo
Microsoft Azure Sponsorship
PREventsConnection
ProductsFeed
New service connection
Choose a service or connection type
Search connection types
Azure Classic
Azure Repos/Team Foundation Server
Azure Resource Manager
Azure Service Bus
Bitbucket Cloud
Chef
Docker Host
Docker Registry
Generic
GitHub
GitHub Enterprise Server
Incoming WebHook
Jenkins
Jira
Kubernetes

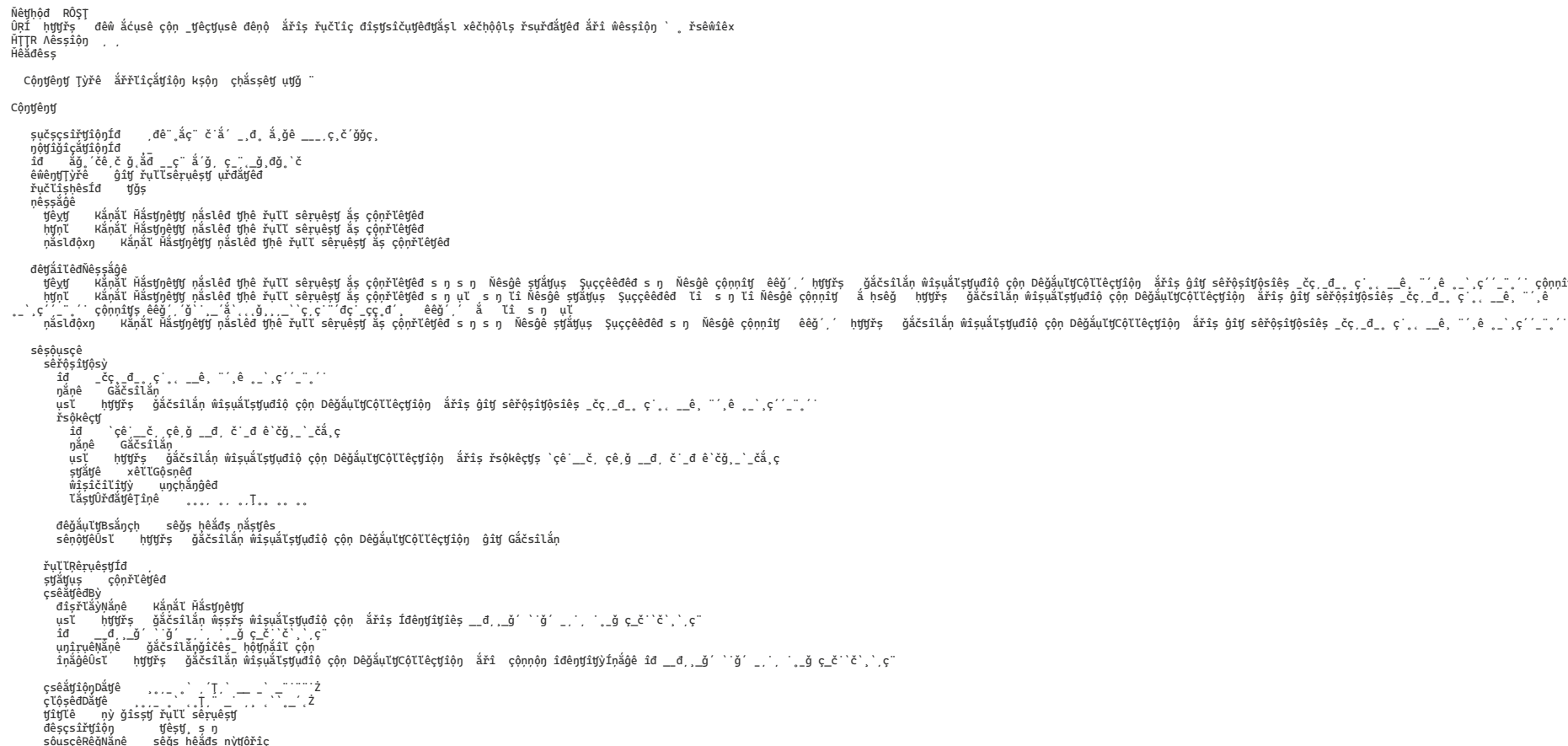

4tecture-demo / k8sDemo / Settings / Service connections
Project Settings
k8sDemo
General
Overview
Teams
Permissions
Notifications
Service hooks
Dashboards
Boards
Project configuration
Team configuration
GitHub connections
Pipelines
Agent pools
Parallel jobs
Settings
Test management
Release retention
Service connections
XAML build services
Repos
Repositories
Service connections
Filter by keywords
4taksDemoAcr
4tecture (MPN)(
8)
4tectureregistry
aksDemoCanary-dev-aksDemo-aks-dev-1606772543573
Azure DevOps 4tecture-demo
Microsoft Azure Sponsorship
PREventsConnection
ProductsFeed
New Incoming WebHook service connection
Authentication
WebHook Name
PRUpdated
Name of the WebHook
Secret (optional)
Optional secret for the webhook. WebHook service will use this secret to calculate the payload checksum
Http Header (optional)
Http header name on which checksum will be sent
Details
Service connection name
PREventsConnection
Description (optional)
Security
Grant access permission to all pipelines
Learn more
Troubleshoot
Back
Save


4tecture-demo / k8sDemo / Settings / Service hooks
Search
Project Settings
k8sDemo
General
Overview
Teams
Permissions
Notifications
Service hooks
Dashboards
Boards
Project configuration
Team configuration
GitHub connections
Pipelines
Agent pools
Parallel jobs
Settings
Test management
Release retention
Service connections
XAML build services
Repos
Repositories
Service Hooks
Integrate with your favorite services by notifying them when events happen in your project.
History
Consumer
Event
Owner
7 Day Status
State
Web Hooks
Pull request
Marc Müller
attempted
Enabled
EDIT SERVICE HOOKS SUBSCRIPTION
Trigger
Select an event to trigger on and configure any filters.
Pull request updated
Remember that selected events are visible to users of the target service, even if they don't have permission to view the related artifact.
FILTERS
Repository
optional
DevFun
Target branch
optional
[Any]
Status changed
Requested by a member of group:
optional
[Any]
Previous
Next
Test
Finish
Cancel


4tecture-demo / k8sDemo / Settings / Service hooks
Search
Project Settings
k8sDemo
General
Overview
Teams
Permissions
Notifications
Project configuration
Team configuration
GitHub connections
Pipelines
Agent pools
Parallel jobs
Settings
Test management
Release retention
Service connections
XAML build services
Repos
Repositories
Service Hooks
Integrate with your favorite services by notifying them when events happen in your project.
History
Consumer
Event
Owner
7 Day Status
State
Web Hooks
Pull request
Marc Müller
attempted
Enabled
EDIT SERVICE HOOKS SUBSCRIPTION
Action
Select and configure the action to perform.
Perform this action
Post via HTTP
https://dev.azure.com/4tecture-demo/_apis/public/distributedtask/webhooks/prupdated?api-version=6.0-preview
SETTINGS
URL
required
https://dev.azure.com/4tecture-demo/_apis/public/distributedt
Accept untrusted SSL certificates
Basic authentication username
optional
Basic authentication password
optional
Previous
Next
Test
Finish
Cancel


4tecture-demo / k8sDemo / Settings / Service hooks
Search
Project Settings
k8sDemo
General
Overview
Teams
Permissions
Notifications
Service hooks
Dashboards
Boards
Project configuration
Team configuration
GitHub connections
Pipelines
Agent pools
Parallel jobs
Settings
Test management
Release retention
Service connections
XAML build services
Repos
Repositories
Service Hooks
Integrate with your favorite services by notifying them when events happen in your project.
History
Consumer
Event
Owner
7 Day Status
State
Web Hooks
Pull request
Marc Müller
attempted
Enabled
EDIT SERVICE HOOKS SUBSCRIPTION
https://dev.azure.com/4tecture-demo/_apis/public/distributedt
Accept untrusted SSL certificates
Basic authentication username
optional
Basic authentication password
optional
HTTP headers
optional
Resource details to send
optional
All
Messages to send
optional
All
Detailed messages to send
optional
All
RESOURCE VERSION
1.0
Previous
Next
Test
Finish
Cancel

Sample event payload



k8sDemo

Overview
Boards
Repos
Pipelines
Pipelines
Environments
Releases
Library
Task groups
Deployment groups
Test Plans
Artifacts

Project settings

DevFun PR Cleanup

Variables | Run

master | DevFun / .azure-pipelines/**devfun-prcleanup.yml** | Show assistant

```yaml
trigger: none

pool:
  vmImage: ubuntu-latest

resources:
  # https://dev.azure.com/4tecture-demo/_apis/public/distributedtask/webhooks/prupdated?api-version=6.0-preview
  webhooks:
    - webhook: PRUpdated                ### Webhook alias
      connection: PREventsConnection    ### Incoming webhook service connection
      filters:
        - path: eventType
          value: git.pullrequest.updated
        - path: publisherId
          value: tfs
        - path: resource.repository.name
          value: DevFun

variables:
Validate
- template: templates/common_variables.yml
Validate
- template: templates/common_variables-cd.yml

stages:
- stage: CleanupPr
  jobs:
  - deployment: CleanupPrEnvironment
    displayName: 'Cleanup PR environment'
    environment: devfuncleanuppr
    condition: or(eq('${{ parameters.PRUpdated.resource.status }}', 'completed'), eq('${{ parameters.PRUpdated.resource.status }}', 'abandoned'))
    strategy:
      runOnce:
        deploy:
          steps:
            - download: none
```

Incoming WebHook as resource with trigger

Additional conditions for dynamic payload evaluation

k8sDemo

Overview
Boards
Repos
Pipelines
Pipelines
Environments
Releases
Library
Task groups
Deployment groups
Test Plans
Artifacts

Project settings

DevFun PR Cleanup

Variables | Run

master | DevFun / .azure-pipelines/**devfun-prcleanup.yml** | Show assistant

```yaml
    runOnce:
      deploy:
        steps:
        - download: none
        - pwsh: |
            $prId = "${{ parameters.PRUpdated.resource.pullRequestId }}"
            $dbname = "devfun-pr$($prId)"
            Write-Host "##vso[task.setvariable variable=dbname;]$dbname"
            Write-Host "##vso[task.setvariable variable=k8sNamespace;]pr-$($prId)"
            Write-Host "##vso[task.setvariable variable=managedIdentityApi;]devfunapi-pr-$($prId)"
            Write-Host "##vso[task.setvariable variable=deploymentManagedIdentityApi;]devfunapi-deployment-pr-$($prId)"
          displayName: "Calculate PR related variables"
        Validate
        - template: templates/pr_DeleteK8sPrEnvironment.yml
          parameters:
            azureSubscription: '$(AzureSubscription)'
            clusterResourceGroup: '$(AzureResourceGroup)'
            clusterName: '$(KubernetesCluster)'
            clusterNamespace: '$(k8sNamespace)'
            continueOnError: true
        Validate
        - template: templates/sql_DeleteAzureSqlDatabase.yml
          parameters:
            AzureSubscription: '$(AzureSubscription)'
            ResourceGroup: '$(AzureResourceGroup)'
            AzureSqlName: '$(dbservername)'
            DbName: '$(dbname)'
            continueOnError: true
        Validate
        - template: templates/az_DeleteManagedIdentity.yml
          parameters:
            AzureSubscription: '$(AzureSubscription)'
            ManagedIdentity: '$(managedIdentityApi)'
            ManagedIdentityResourceGroup: '$(ManagedIdentityResourceGroup)'
            continueOnError: true
```

Calculate PR specific variables

Delete deployment

Delete database

Delete Identities

Azure Deployments

Conclusion

4tecture
empower your software solutions

Conclusion

- Everything is Code – IaC, CaC
- Put Secrets in KeyVault / Secure Files
- Use Managed Identities → no credentials!
- Deployment agents in target environment

Azure Deployments

Q & A

4tecture
empower your software solutions

Thank you for your attention!

If you have any questions do not hesitate to contact us:

4tecture GmbH
Industriestrasse 25
CH-8604 Volketswil
www.4tecture.ch

Marc Müller
Principal Consultant

www.powerofdevops.com

4tecture©
empower your software solutions

ProAuth

ReaFx


4tecture©
empower your software solutions