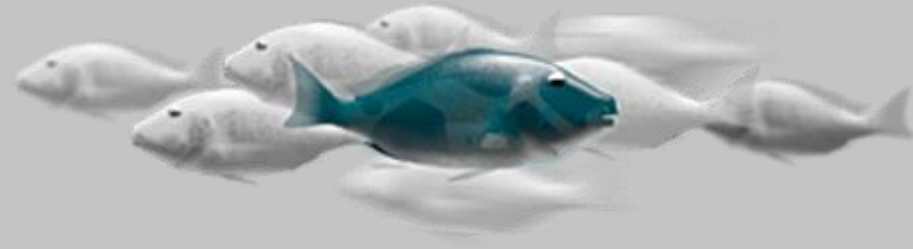


EDEM



Máster en Data Analytics

laC Terraform (DevSecOps)
Ignacio Asín Calamonte

ABOUT ME

- Working in **SIEMENS** as a Cloud DevSecOps in the Global Cybersecurity Cloud Protection unit
- Located in the SIEMENS **Madrid Cybersecurity Hub**
- Previously I was:
 - Cloud Architect & Blockchain Specialist
 - Big Data Engineer
 - DevOps Engineer
 - Senior Java Programmer
- **Computer Science**
- **Master in Big Data & Visual Analytics**
- **Cloud Certified** in Cloud Security Automation, Several Clouds & other Certs.
- Favorite topics: **Automation, Google Cloud, Blockchain, latest Tech trends, ...**
- Project Architect/Developer, Research, Formation courses, Meetups, ...



[@iasinDev](https://twitter.com/iasinDev)



[ignacioasincalamonte](https://www.linkedin.com/in/ignacioasincalamonte)



iasin.dev@gmail.com

AGENDA

1. FORMAT OF THE CLASS
2. LOCAL ENVIRONMENT
3. WHAT IS DEVOPS & DEVSECOPS
 1. Everything as Code
 2. Communication & Collaboration
 3. Security Management
 4. Continuous Integration (CI) & Continuous Deployment (CD)
 5. Platform as Code
 6. Infrastructure as Code
 7. Testing
 8. Destroy All

09,00h – 14,00h

15,30h – 19,30h

BREAKS

10,30h – 10,50h

12,30h – 12,40h

BREAKS

17,30h – 17,45h

Questions??

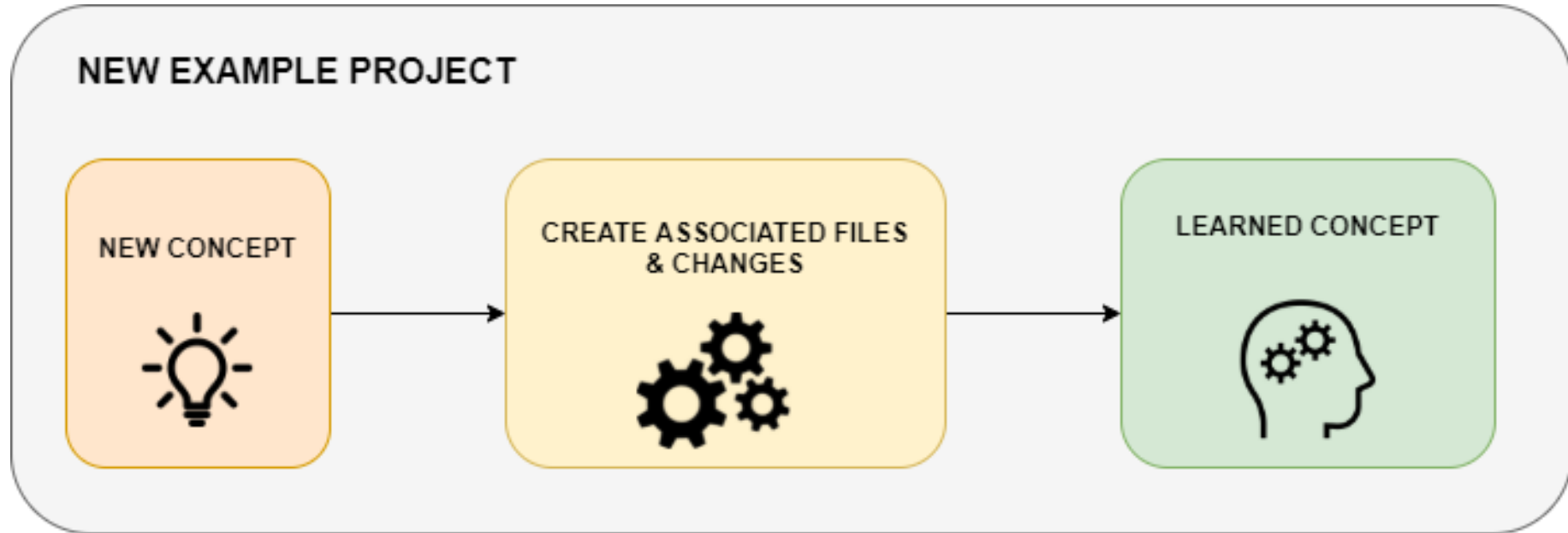
1. FORMAT OF THE CLASS

FORMAT OF THE CLASS

“Learning by doing”

FORMAT OF THE CLASS

“Learning by doing”



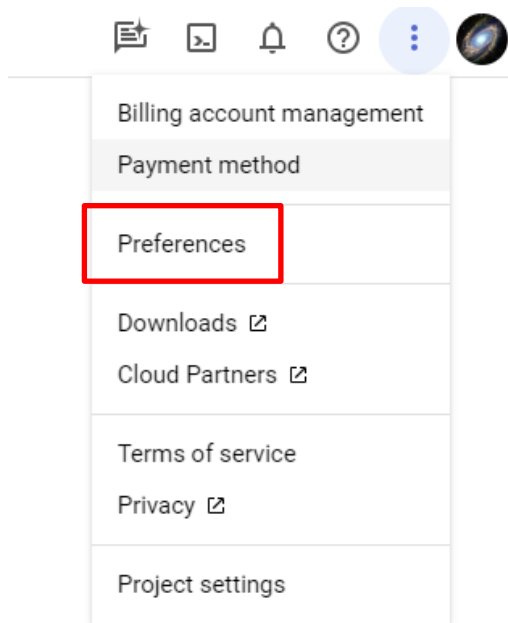
2. LOCAL ENVIRONMENT

LOCAL ENVIRONMENT

- [Visual Studio Code](#) + Git Graph Extension
- [GitHub Account](#)
- [Google Cloud Platform \(GCP\) account](#)
- [Google Chrome](#) / similar browser
- [GitHub Desktop \(Recommended\)](#) or [Git for Windows \(PRO users\)](#)
- [Notepad++](#) / any other extra text editor more than VS Code

LOCAL ENVIRONMENT

- [Google Cloud Platform \(GCP\) account](#) – set language in english



3. WHAT IS DEVOPS & DEVSECOPS?

WHAT IS DEVOPS & DEVSECOPS?



What **IS NOT** DevOps?



New
Superhero



Profession
(not only)



Culture
(not only)

WHAT IS DEVOPS & DEVSECOPS?



What **IS** DevOps?



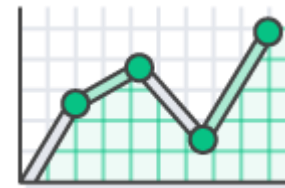
Velocity



Faster
releases



Reliability



Scale



Improved
collaboration

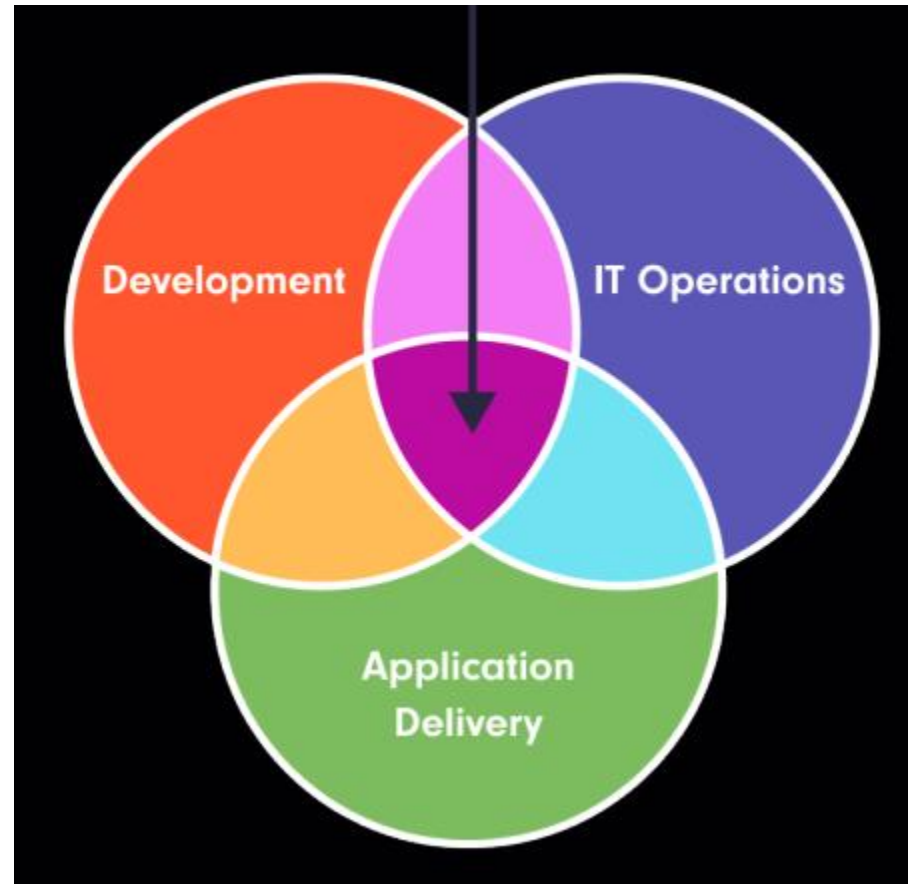


Scripting + Communicative + Process reengineering +
Experience with certain tools / languages + ...

WHAT IS DEVOPS & DEVSECOPS?



What **IS** DevOps?



WHAT IS DEVOPS & DEVSECOPS?



What **IS** DevOps?



DIFFICULT TO FIND !!

WHAT IS DEVOPS & DEVSECOPS?



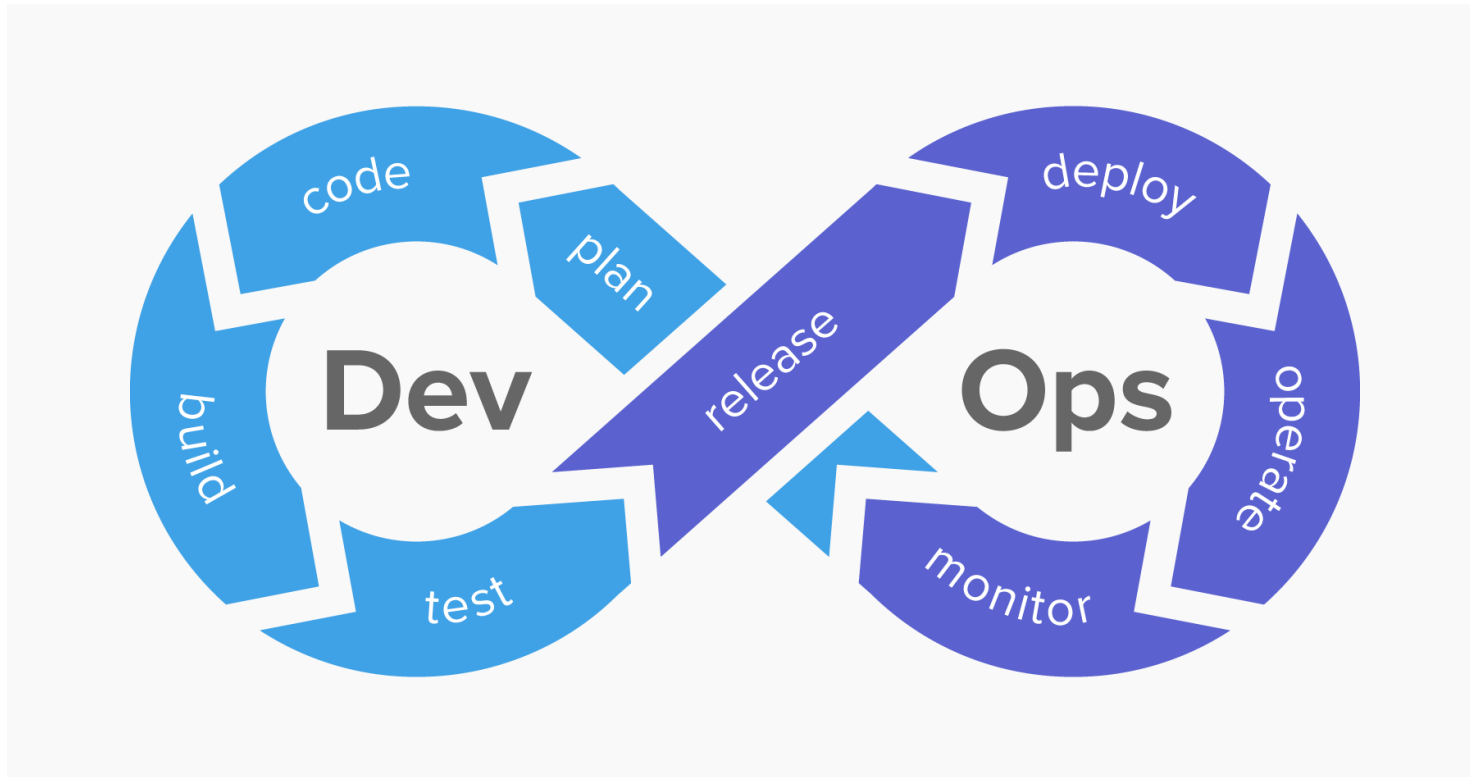
What **IS** DevOps?



WHAT IS DEVOPS & DEVSECOPS?



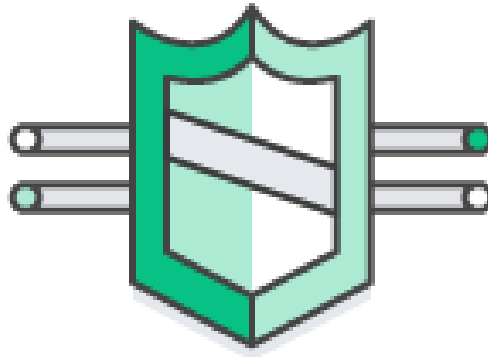
What **IS** DevOps?



WHAT IS DEVOPS & DEVSECOPS?



What **IS** Dev**Sec**Ops?

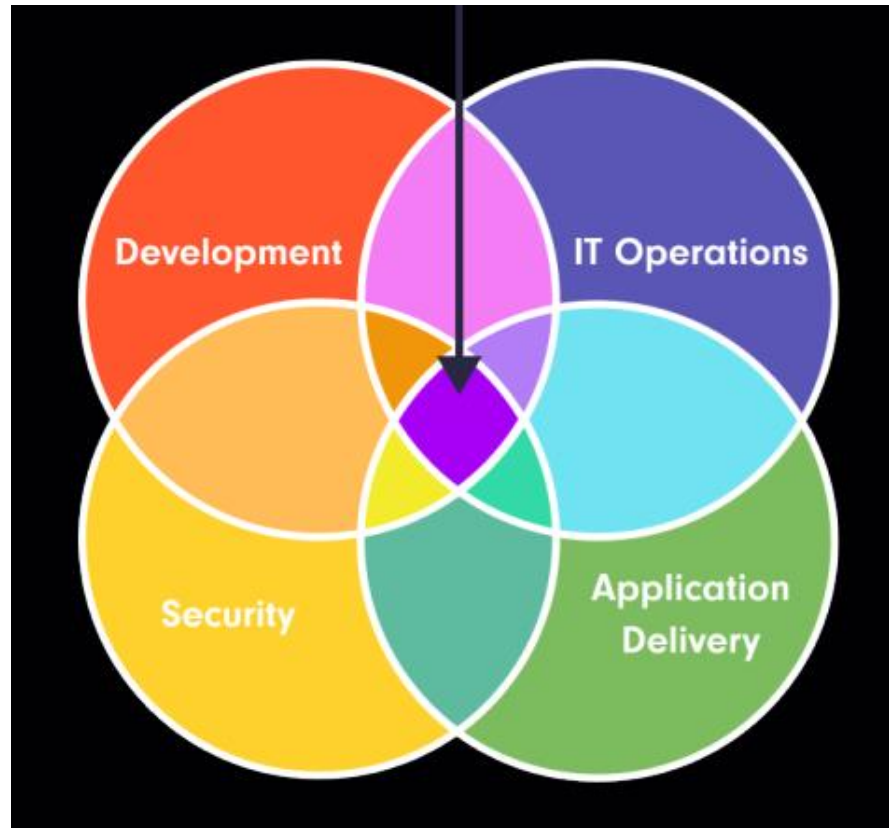


Security

WHAT IS DEVOPS & DEVSECOPS?



What **IS** Dev**Sec**Ops?



WHAT IS DEVOPS & DEVSECOPS?



What **IS** Dev**Sec**Ops?



DIFFICULT TO FIND !!

WHAT IS DEVOPS & DEVSECOPS?



What **IS** Dev**Sec**Ops?

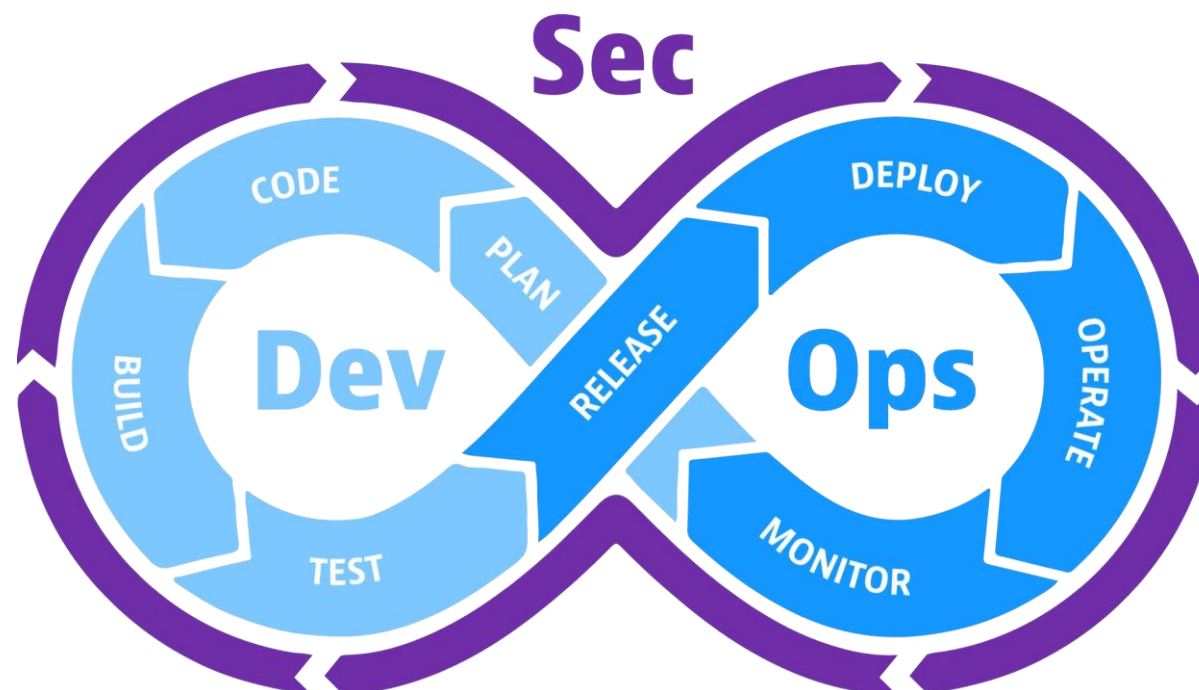


DIFFICULT TO FIND !!

WHAT IS DEVOPS & DEVSECOPS?



What **IS** Dev**Sec**Ops?



WHAT IS DEVOPS & DEVSECOPS?



Everything as Code



Infrastructure as Code (IaC)

(Application as Code)

Configuration as Code

Security as Code

Policy as Code

... as Code

WHAT IS DEVOPS & DEVSECOPS?

Everything as Code



[Solution here](#)



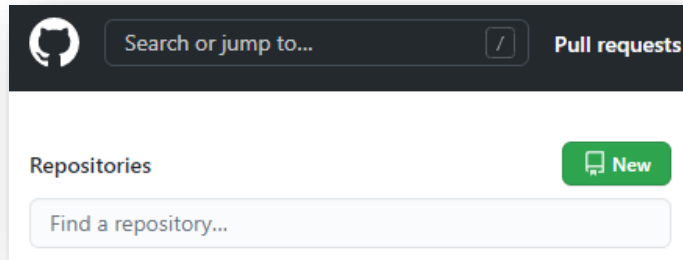
1. Create a new Project in GitHub (Private project)

How to ... in next slide ...



WHAT IS DEVOPS & DEVSECOPS?

Everything as Code



Create a new repository

A repository contains all project files, including the revision history. Already have a project repository elsewhere? [Import a repository.](#)

Owner * Repository name *
iasinDev / my-super-project ✓

Great repository names are short and memorable. Need inspiration? How about [symmetrical-train](#)?

Description (optional)

An awesome project that I'm going to make this summer.

- ☐ Public
Anyone on the internet can see this repository. You choose who can commit.
- ☒ Private
You choose who can see and commit to this repository.

Initialize this repository with:

Skip this step if you're importing an existing repository.

☒ Add a README file
This is where you can write a long description for your project. [Learn more.](#)

☒ Add .gitignore
Choose which files not to track from a list of templates. [Learn more.](#)
.gitignore template: Terraform ▼

☒ Choose a license
A license tells others what they can and can't do with your code. [Learn more.](#)
License: MIT License ▼

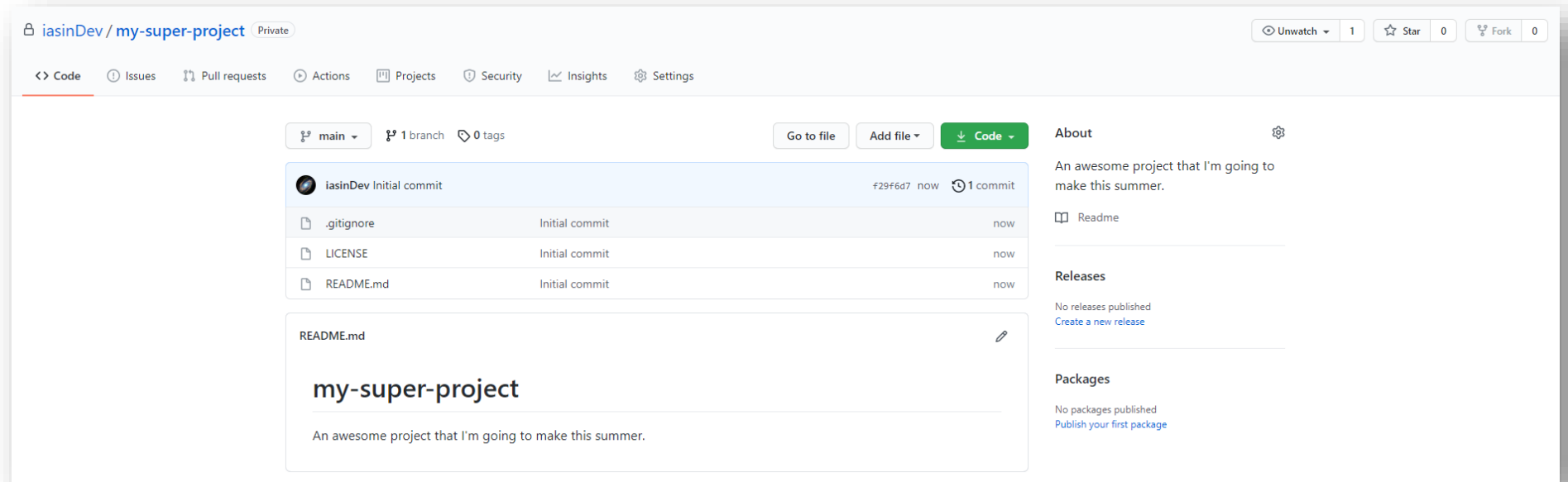
This will set `main` as the default branch. Change the default name in your [settings](#).

Create repository



WHAT IS DEVOPS & DEVSECOPS?

Everything as Code



WHAT IS DEVOPS & DEVSECOPS?

Everything as Code



Solution [here](#)

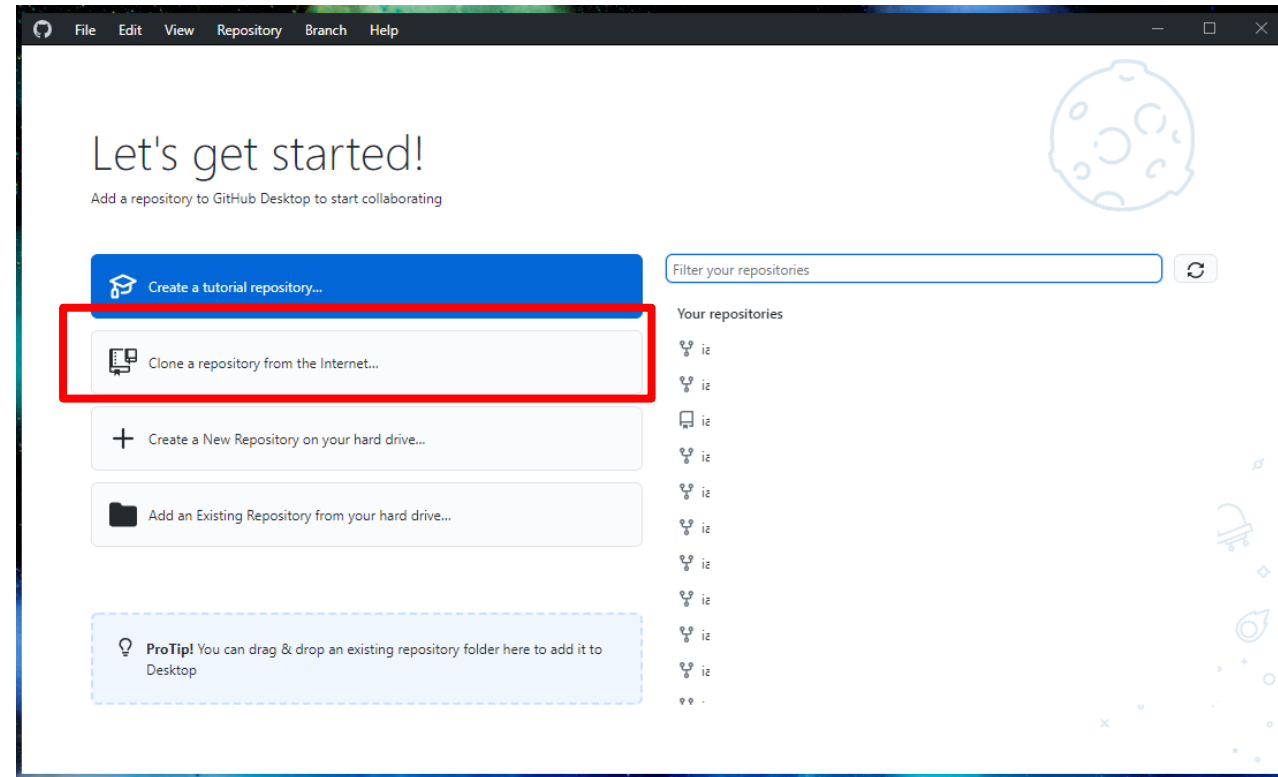


2. Clone the new Project in local

How to ... in next slide ...

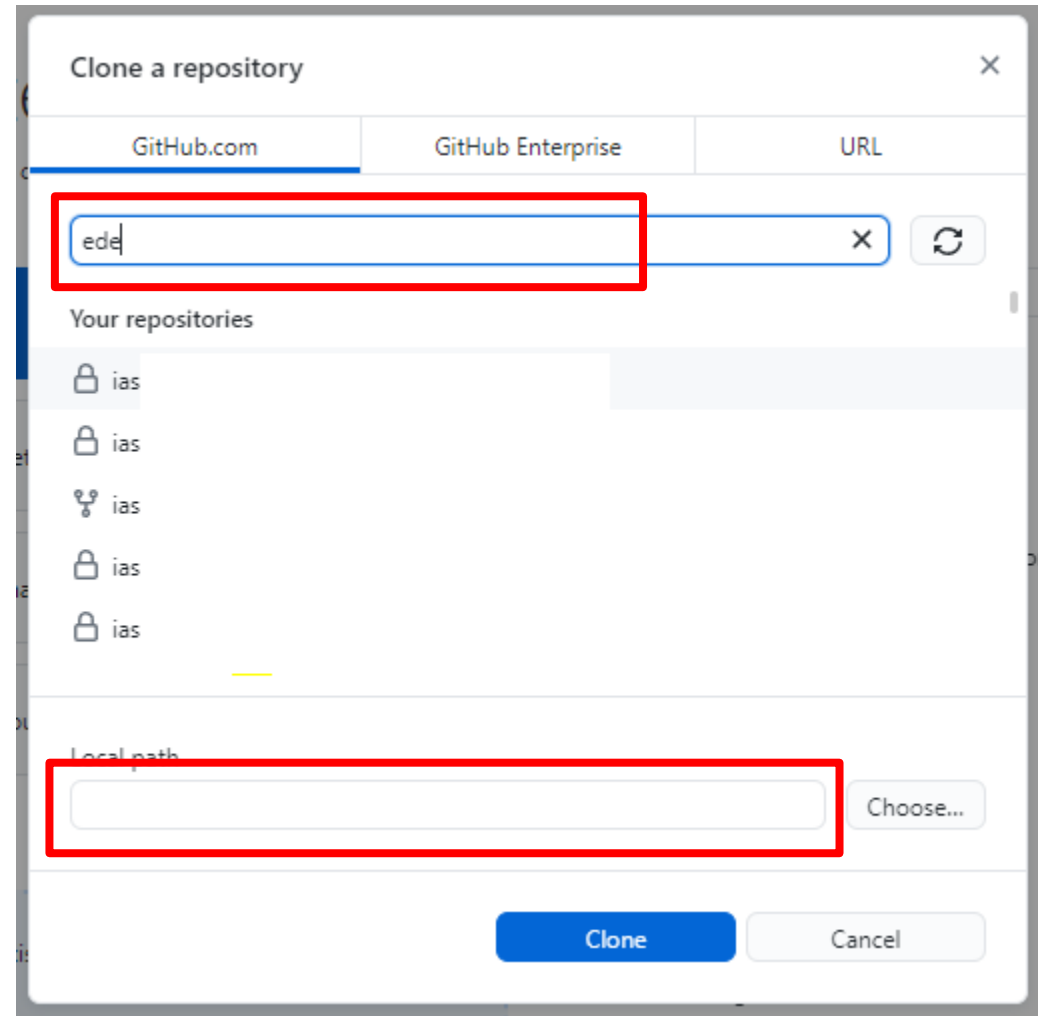
WHAT IS DEVOPS & DEVSECOPS?

Everything as Code



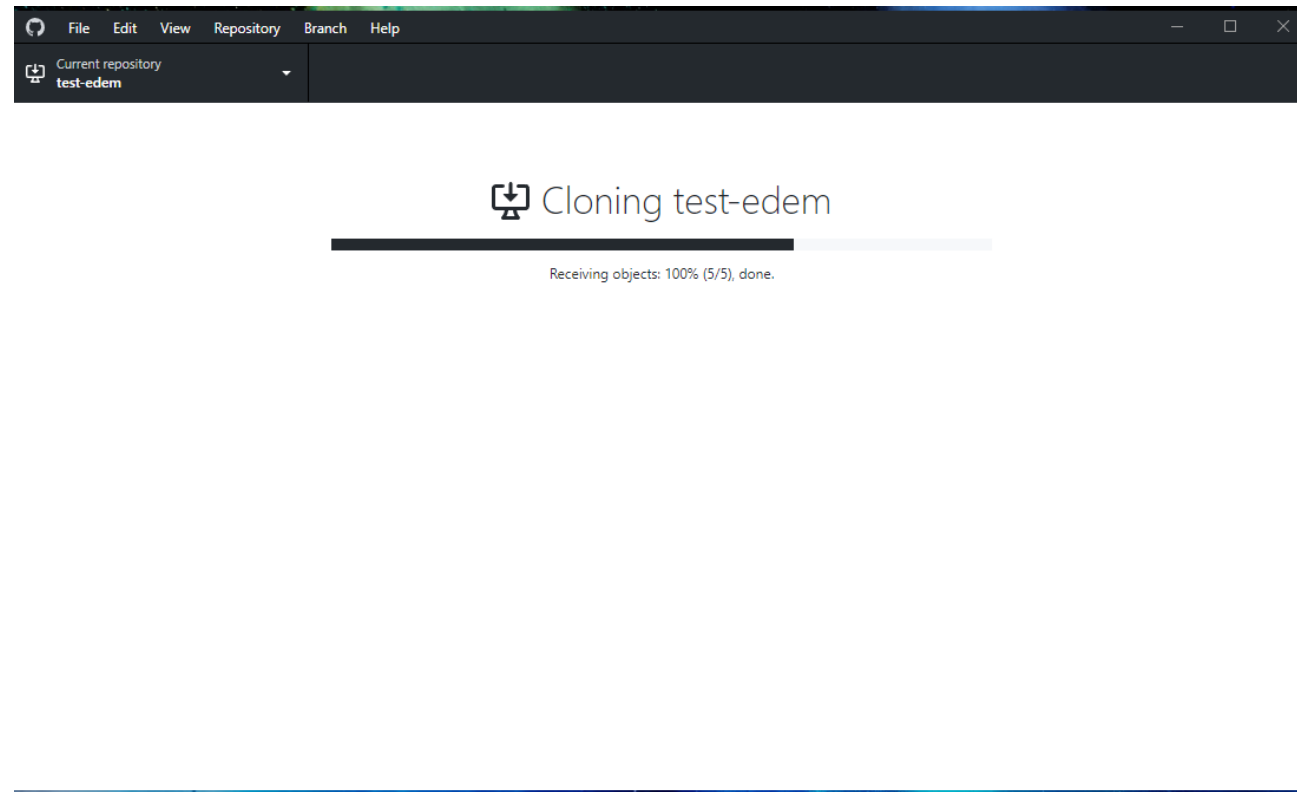
WHAT IS DEVOPS & DEVSECOPS?

Everything as Code



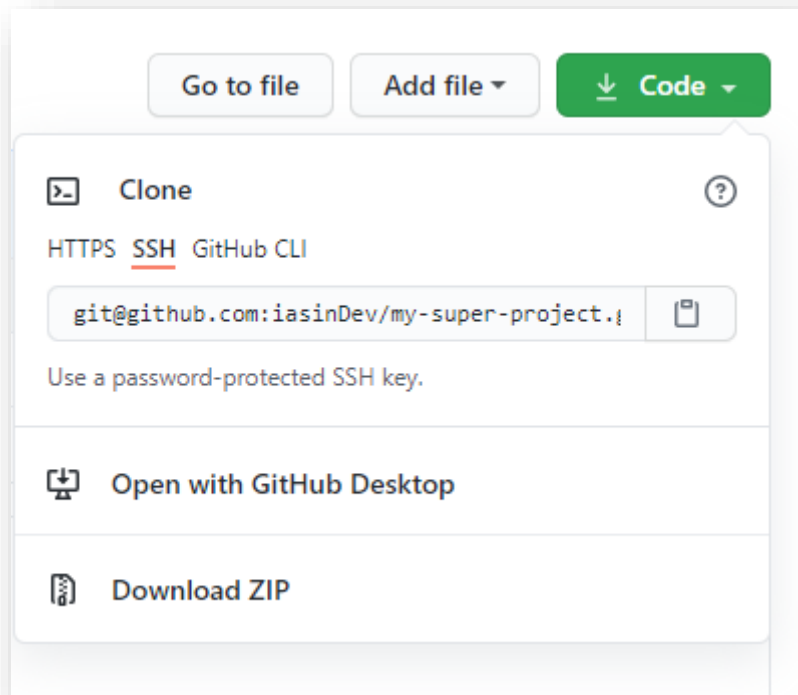
WHAT IS DEVOPS & DEVSECOPS?

Everything as Code



WHAT IS DEVOPS & DEVSECOPS?

Everything as Code

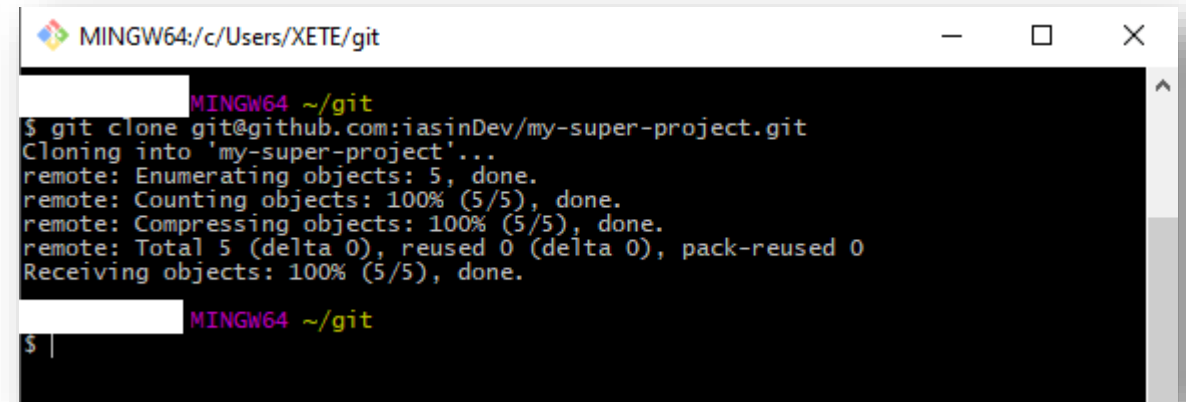


Pro Mode



Using ssh keys in console

See [here](#), [here](#) and [here](#) for more info



WHAT IS DEVOPS & DEVSECOPS?

Everything as Code



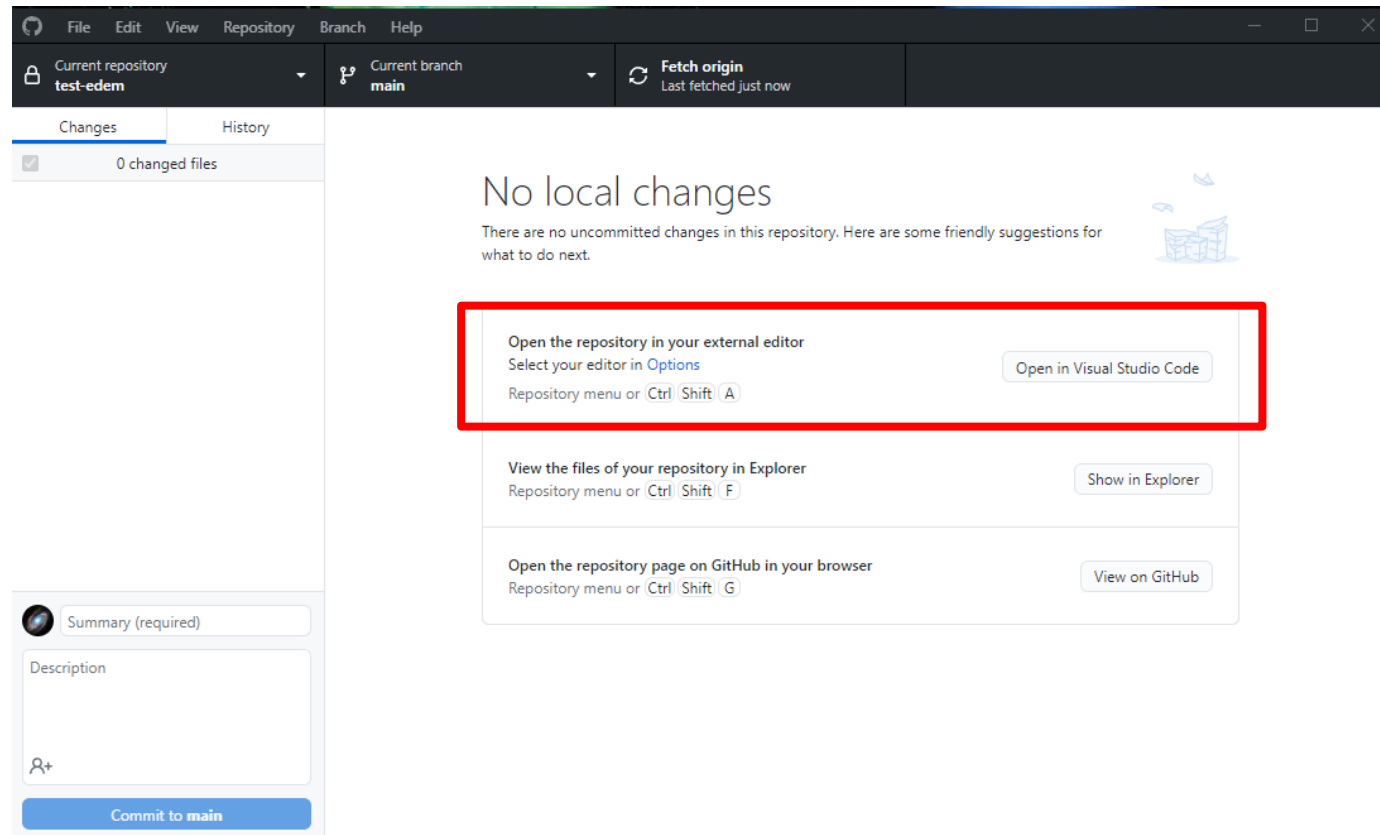
Solution [here](#)



3. Open the new Project with Visual Studio Code

WHAT IS DEVOPS & DEVSECOPS?

Everything as Code

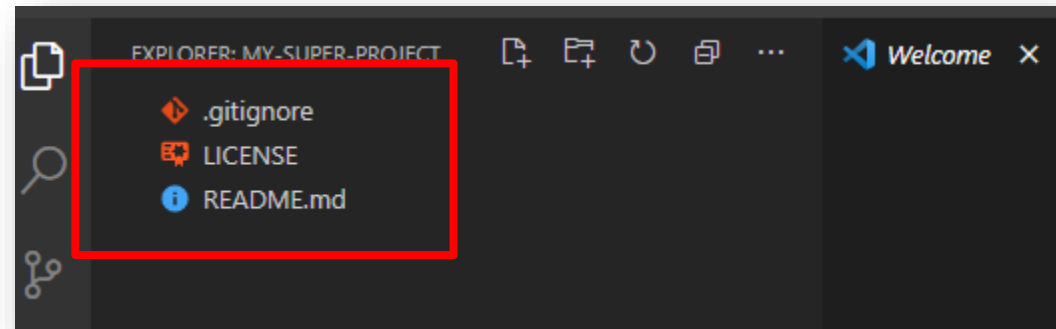


WHAT IS DEVOPS & DEVSECOPS?

Everything as Code



```
MINGW64 ~/git  
$ cd my-super-project/  
MINGW64 ~/git/my-super-project (main)  
$ code .
```

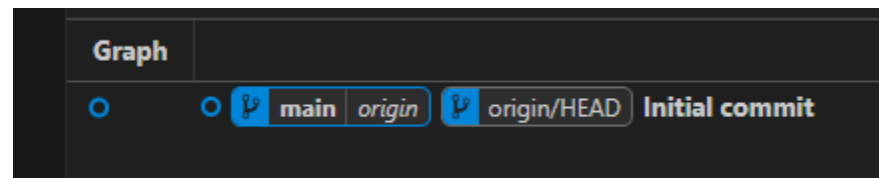


WHAT IS DEVOPS & DEVSECOPS?

Everything as Code



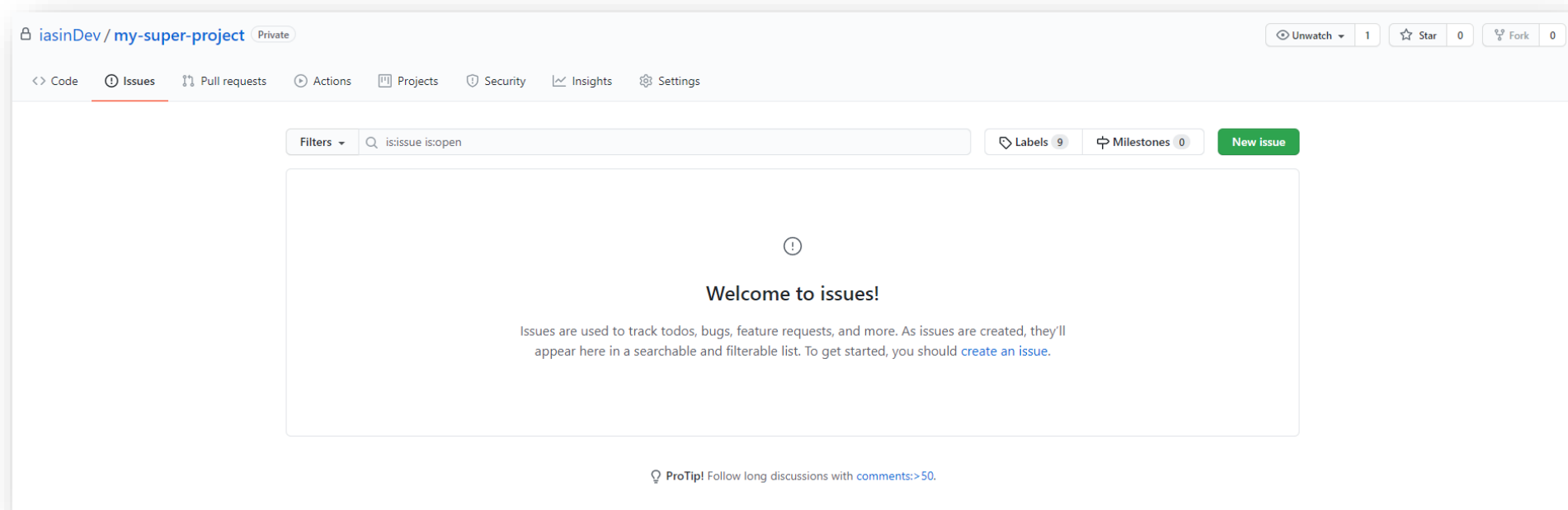
Check also with Git Graph!!



WHAT IS DEVOPS & DEVSECOPS?



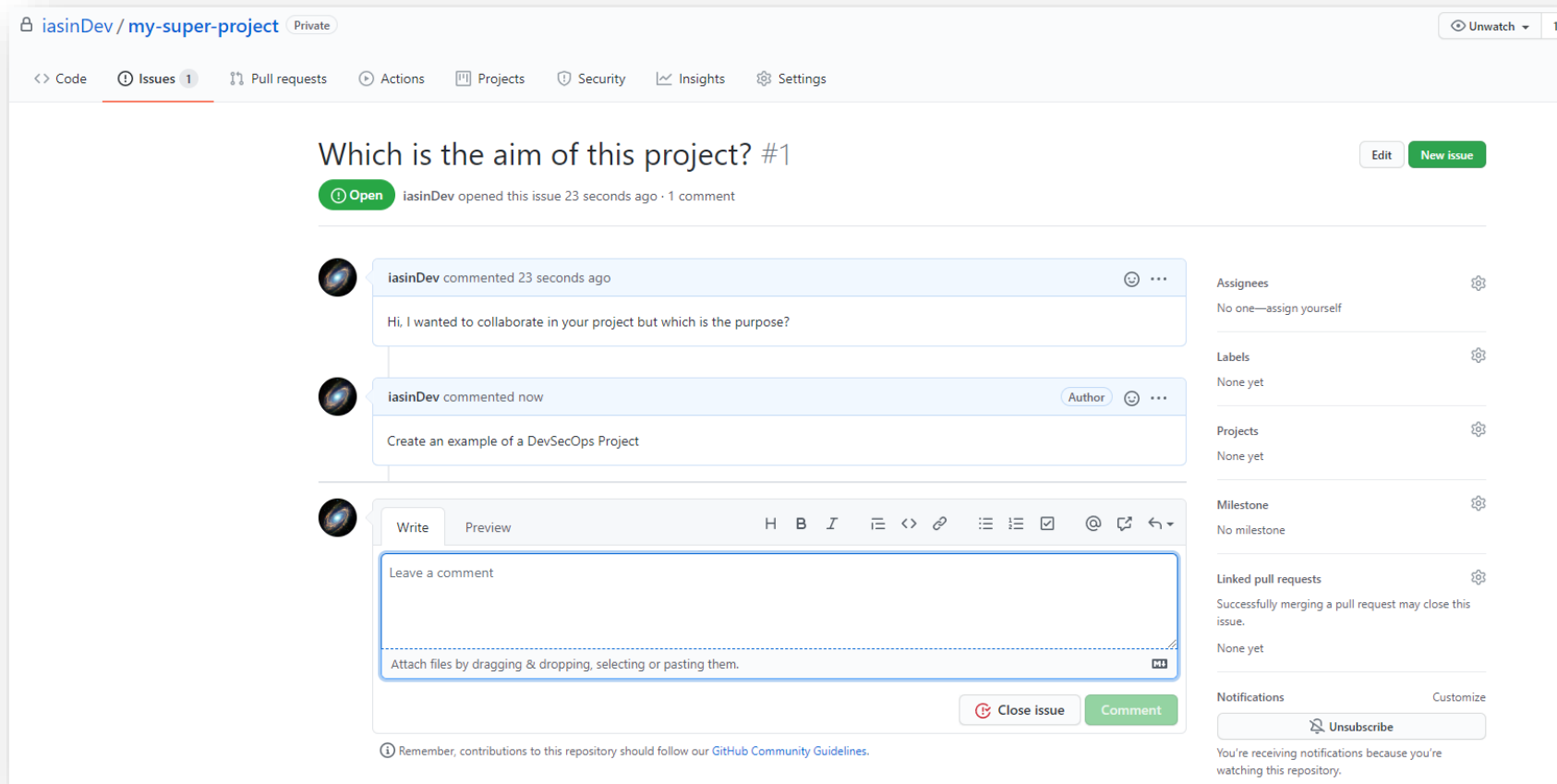
Communication & Collaboration



WHAT IS DEVOPS & DEVSECOPS?



Communication & Collaboration



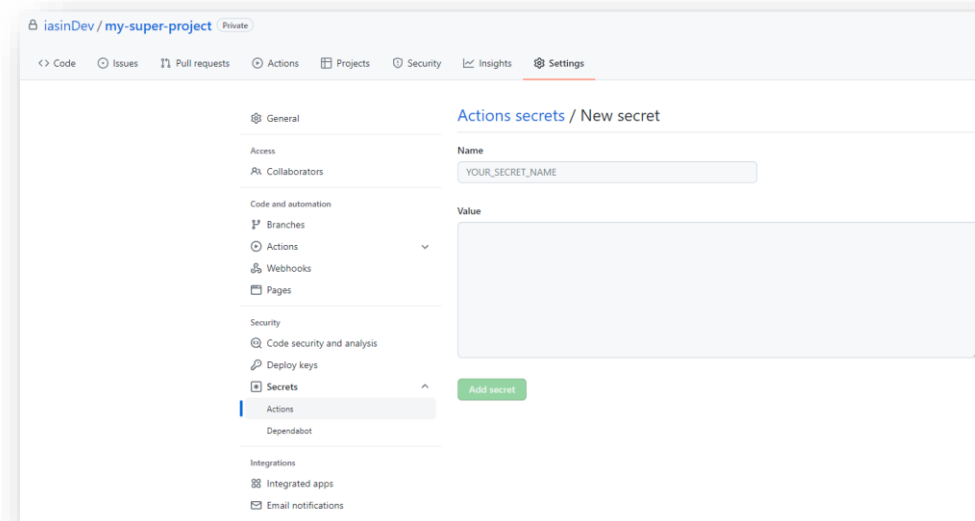
The screenshot shows a GitHub issue page for the repository 'iasinDev / my-super-project'. The issue title is 'Which is the aim of this project? #1'. The issue is marked as 'Open' and was opened by 'iasinDev' 23 seconds ago, with 1 comment. The issue page includes a navigation bar with links to Code, Issues (1), Pull requests, Actions, Projects, Security, Insights, and Settings. The main content area shows two comments from 'iasinDev'. The first comment, posted 23 seconds ago, says 'Hi, I wanted to collaborate in your project but which is the purpose?'. The second comment, posted 'now', says 'Create an example of a DevSecOps Project'. Below the comments is a text input field for leaving a comment, with a 'Write' tab and a 'Preview' tab. The input field has a rich text editor toolbar with options for bold, italic, link, and other formatting. To the right of the comments is a sidebar with various issue settings, including Assignees (No one—assign yourself), Labels (None yet), Projects (None yet), Milestone (No milestone), Linked pull requests (Successfully merging a pull request may close this issue. None yet), and Notifications (Unsubscribe). At the bottom of the page, there is a footer note: 'Remember, contributions to this repository should follow our GitHub Community Guidelines.'

WHAT IS DEVOPS & DEVSECOPS?



Security Management

We need to obtain GCP credentials to interact with the Cloud; this is called, a “service account”.



GitHub Secrets

WHAT IS DEVOPS & DEVSECOPS?



Security Management

Create a new Google Cloud Project called `edemdevsecops`

Create a Google Cloud service account

Call it “`edemdevsecops`” with the description “Account used for the course of DevSecOps of EDEM”

With the following roles (PoLP, Principle of Less Privilege):

- `Cloud Run Admin` - allows for the creation of new Cloud Run services
- `Service Account User` - required to deploy to Cloud Run as service account
- `Storage Admin` - allow push to Google Container Registry

WHAT IS DEVOPS & DEVSECOPS?



Security Management



New Project

You have 24 projects remaining in your quota. Request an increase or delete projects. [Learn more](#)

[MANAGE QUOTAS](#)

Project name *
edemdevsecops

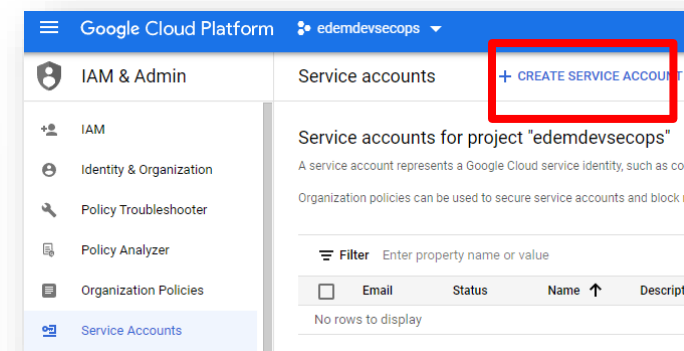
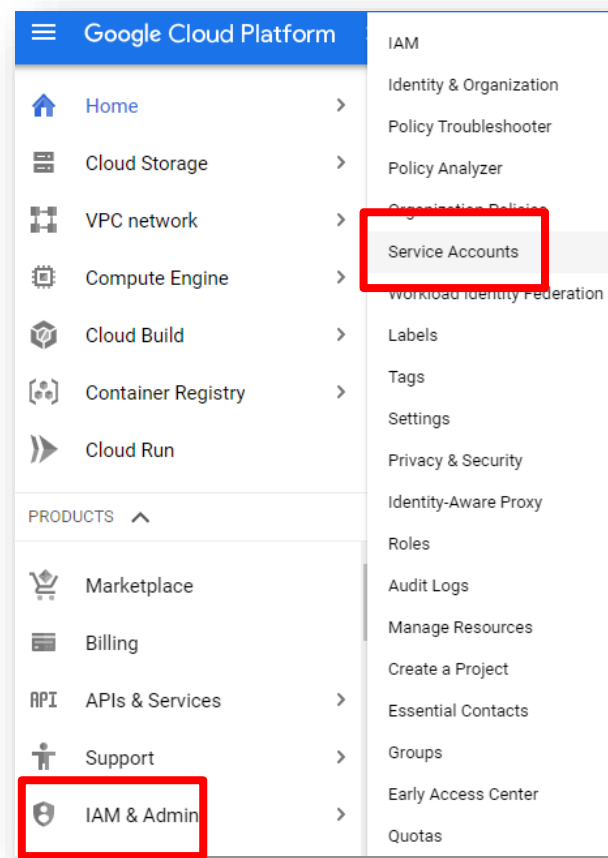
Project ID *
edemdevsecops

Project ID can have lowercase letters, digits, or hyphens. It must start with a lowercase letter and end with a letter or number.

Location *
 No organization [BROWSE](#)

Parent organization or folder

[CREATE](#) [CANCEL](#)



Create service account

- #### Service account details

Service account name *
edemdevsecops

Display name for this service account

Service account ID *
edemdevsecops @edemdevsecops.iam.gserviceaccount.com

Service account description
Account used for the edemdevsecops course [Clear](#)

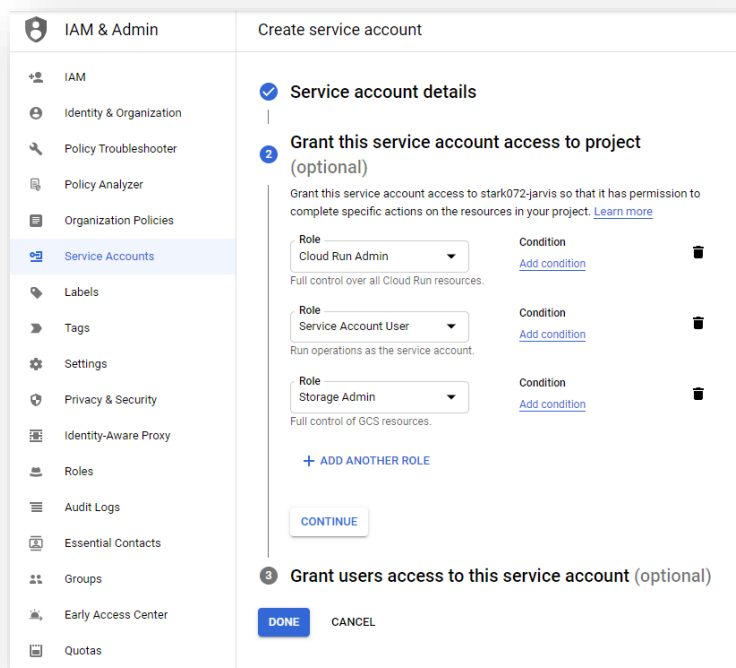
[CREATE AND CONTINUE](#)
- #### Grant this service account access to project (optional)
- #### Grant users access to this service account (optional)

[DONE](#) [CANCEL](#)

WHAT IS DEVOPS & DEVSECOPS?



Security Management



IAM & Admin | Create service account

Service account details

2 Grant this service account access to project (optional)

Grant this service account access to stark072-jarvis so that it has permission to complete specific actions on the resources in your project. [Learn more](#)

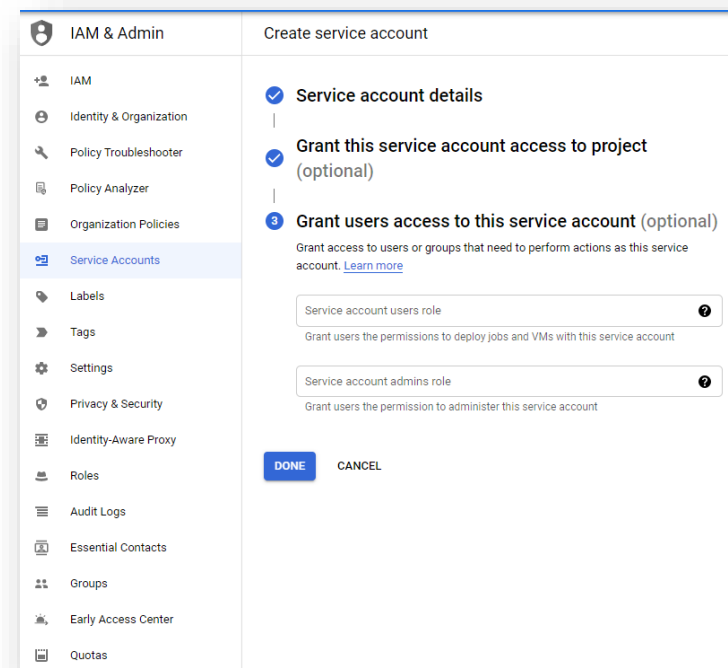
Role	Condition	
Cloud Run Admin	Add condition	
Full control over all Cloud Run resources.		
Service Account User	Add condition	
Run operations as the service account.		
Storage Admin	Add condition	
Full control of GCS resources.		

[+ ADD ANOTHER ROLE](#)

[CONTINUE](#)

3 Grant users access to this service account (optional)

[DONE](#) [CANCEL](#)



IAM & Admin | Create service account

Service account details

Grant this service account access to project (optional)

3 Grant users access to this service account (optional)

Grant access to users or groups that need to perform actions as this service account. [Learn more](#)

Role	Condition	
Service account users role	Add condition	
Grant users the permissions to deploy jobs and VMs with this service account		
Service account admins role	Add condition	
Grant users the permission to administer this service account		

[DONE](#) [CANCEL](#)





<input type="checkbox"/>	Email	Status	Name ↑	Description	Key ID	Key creation date	OAuth 2 Client ID ?	Actions
<input type="checkbox"/>	edemdevops@edemdevsecops.iam.gserviceaccount.com	✓	edemdevops	Account used for the edemdevops course	No keys		113302195566610601320	







WHAT IS DEVOPS & DEVSECOPS?



Security Management

Check it

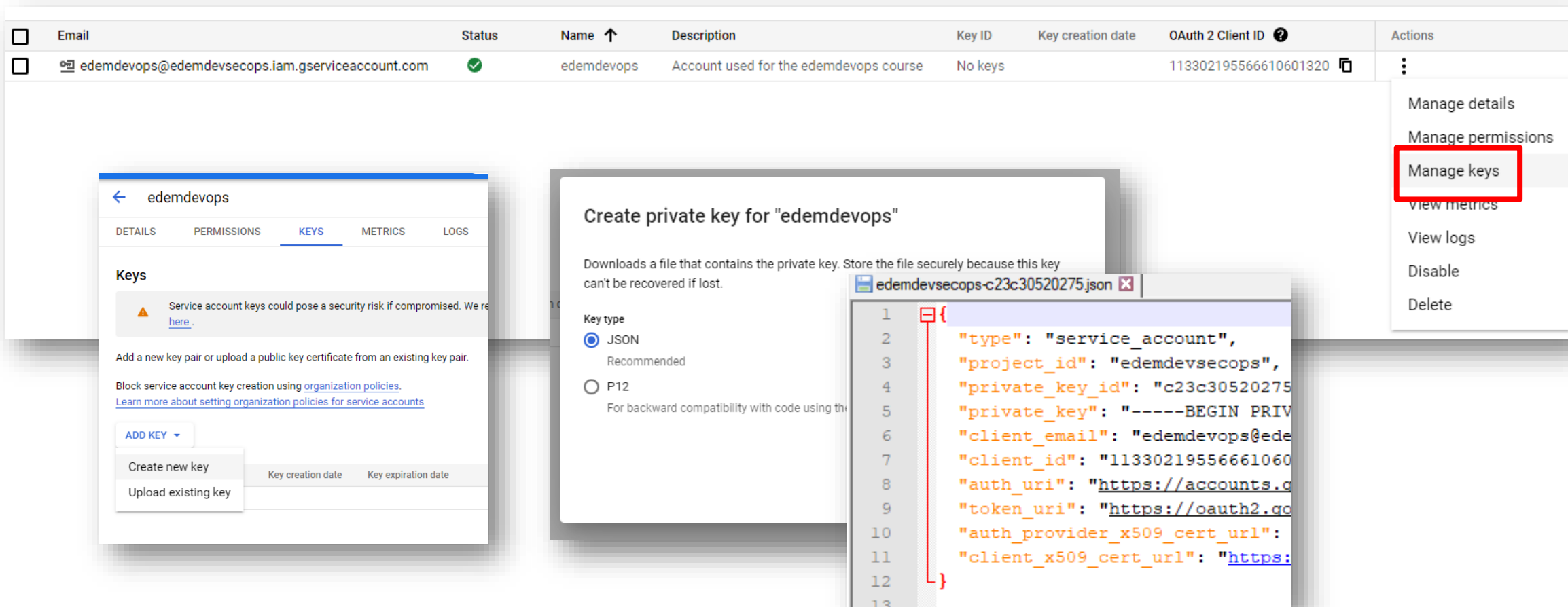
-  IAM & Admin
-  IAM
-  Identity & Organization
-  Policy Troubleshooter

 	edemdevsecops@edemdevsecops-374816.iam.gserviceaccount.com	edemdevsecops	Cloud Run Admin	 63/63 excess permissions	▼	
			Service Account User	 5/5 excess permissions	▼	
			Storage Admin	 42/42 excess permissions	▼	

WHAT IS DEVOPS & DEVSECOPS?



Security Management



The screenshot displays the Google Cloud IAM console interface for managing service account keys. The main table lists service accounts, with 'edemdevops' selected. The 'Actions' menu for this account is open, highlighting 'Manage keys'. Below this, the 'Keys' tab for 'edemdevops' is shown, indicating that no keys are currently present. A 'Create private key for "edemdevops"' dialog is open, showing the 'JSON' key type selected. A preview of the resulting JSON key file is also visible, showing fields like 'type', 'project_id', 'private_key_id', 'private_key', 'client_email', 'client_id', 'auth_uri', 'token_uri', 'auth_provider_x509_cert_url', and 'client_x509_cert_url'.

Email	Status	Name	Description	Key ID	Key creation date	OAuth 2 Client ID	Actions
edemdevops@edemdevsecops.iam.gserviceaccount.com		edemdevops	Account used for the edemdevops course	No keys		113302195566610601320	<ul style="list-style-type: none">Manage detailsManage permissionsManage keysView metricsView logsDisableDelete

edemdevops

DETAILS PERMISSIONS **KEYS** METRICS LOGS

Keys

Service account keys could pose a security risk if compromised. We recommend you [rotate keys](#).

Add a new key pair or upload a public key certificate from an existing key pair.

Block service account key creation using [organization policies](#).
[Learn more about setting organization policies for service accounts](#)

ADD KEY

- Create new key
- Upload existing key

	Key creation date	Key expiration date
--	-------------------	---------------------

Create private key for "edemdevops"

Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.

Key type

- ☒ JSON
Recommended
- ☐ P12
For backward compatibility with code using the P12 key type

edemdevsecops-c23c30520275.json

```
1 {  
2   "type": "service_account",  
3   "project_id": "edemdevsecops",  
4   "private_key_id": "c23c30520275",  
5   "private_key": "-----BEGIN PRIVATE KEY-----",  
6   "client_email": "edemdevops@edemdevsecops.iam.gserviceaccount.com",  
7   "client_id": "113302195566610601320",  
8   "auth_uri": "https://accounts.google.com/o/oauth2/auth",  
9   "token_uri": "https://oauth2.googleapis.com/token",  
10  "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs",  
11  "client_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs",  
12 }  
13
```

WHAT IS DEVOPS & DEVSECOPS?

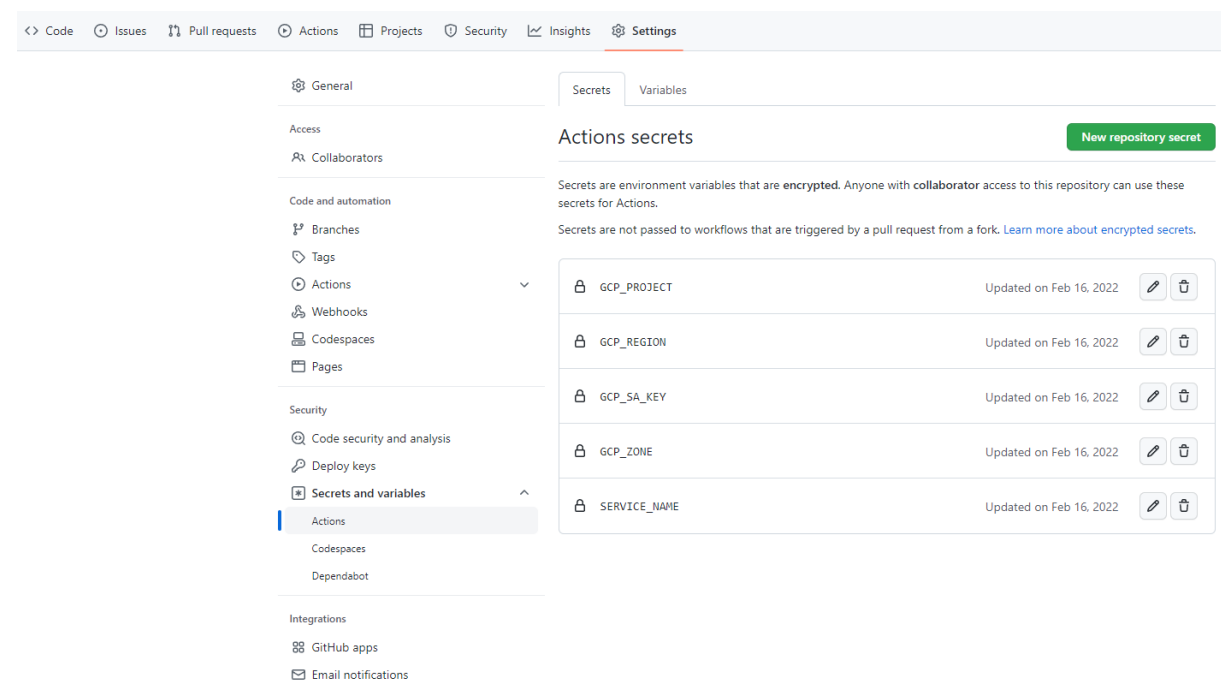
Security Management



Add the following secrets to your GitHub project secrets:

- ``GCP_PROJECT`` - field `project_id` of the json file
- ``GCP_REGION`` - `europe-west1`
- ``GCP_SA_KEY`` - copy&paste whole json file
- ``GCP_ZONE`` - `europe-west1-b`
- ``SERVICE_NAME`` - `edemdevsecops`

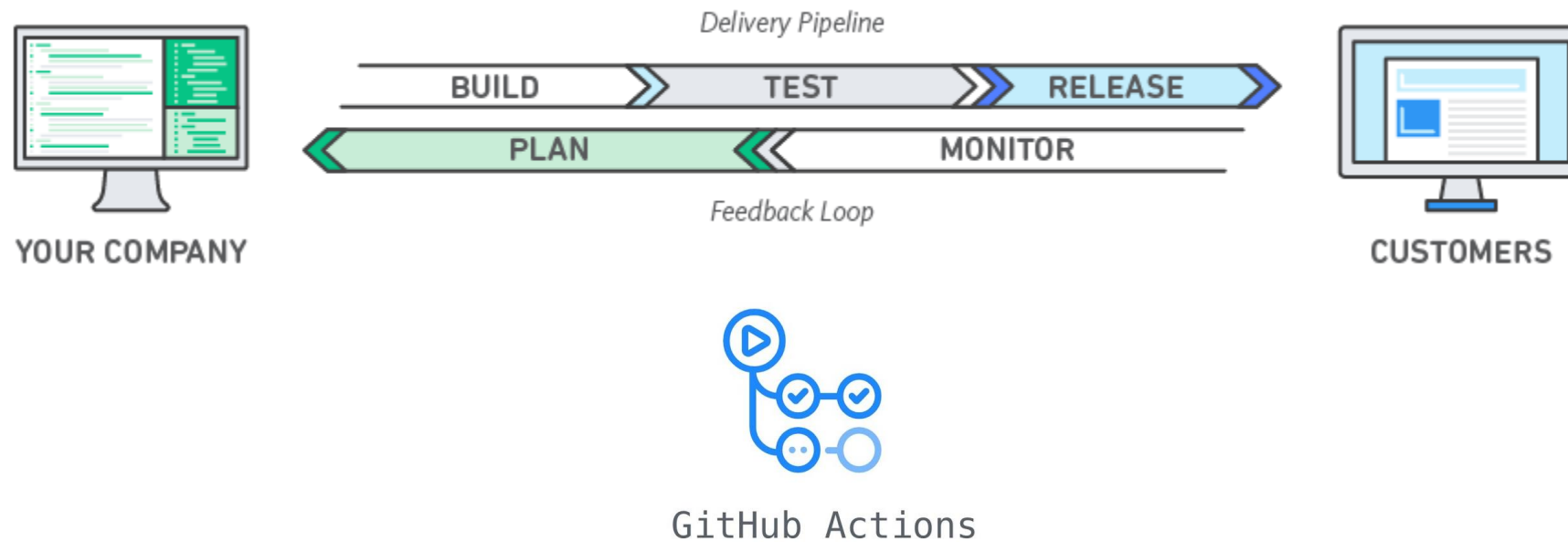
After copy-pasting the secrets delete the downloaded json file



WHAT IS DEVOPS & DEVSECOPS?



Continuous Integration (CI) & Continuous Delivery (CD)



WHAT IS DEVOPS & DEVSECOPS?



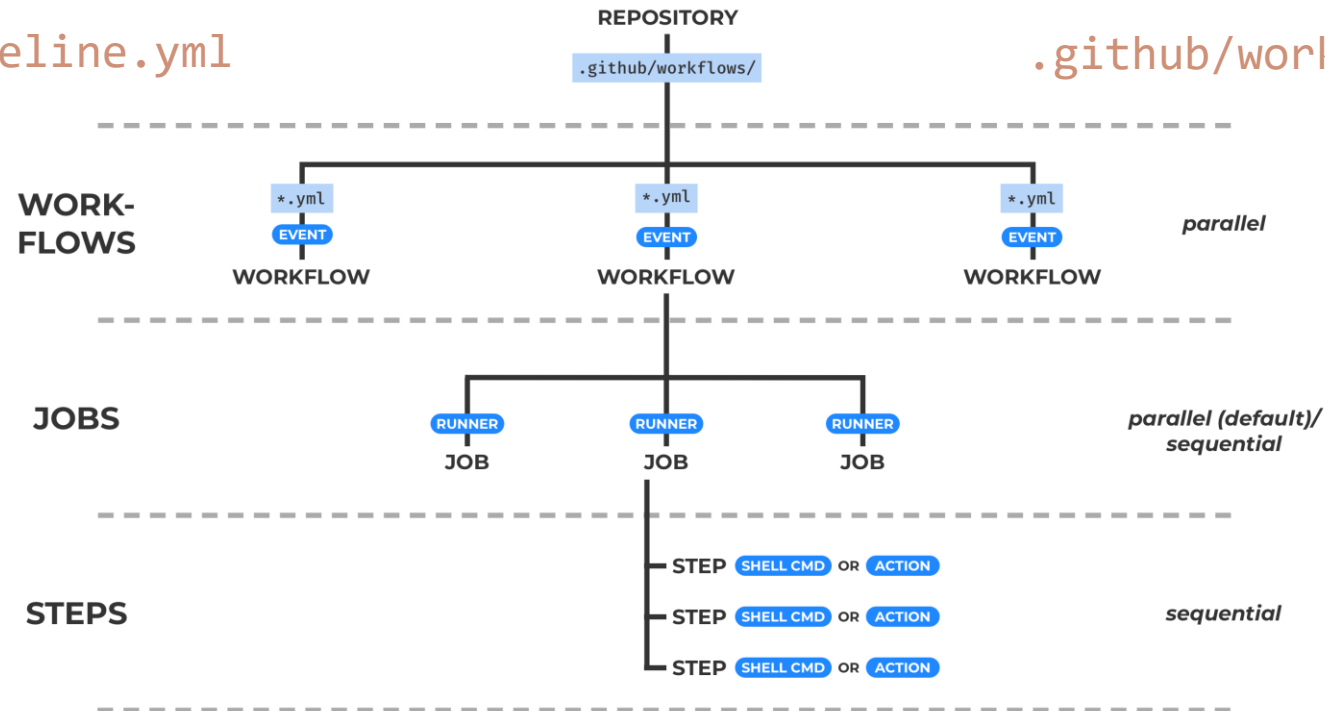
Continuous Integration (CI) & Continuous Delivery (CD)



GitHub Actions

`.github/workflows/pipeline.yml`

`.github/workflows/destroy.yml`



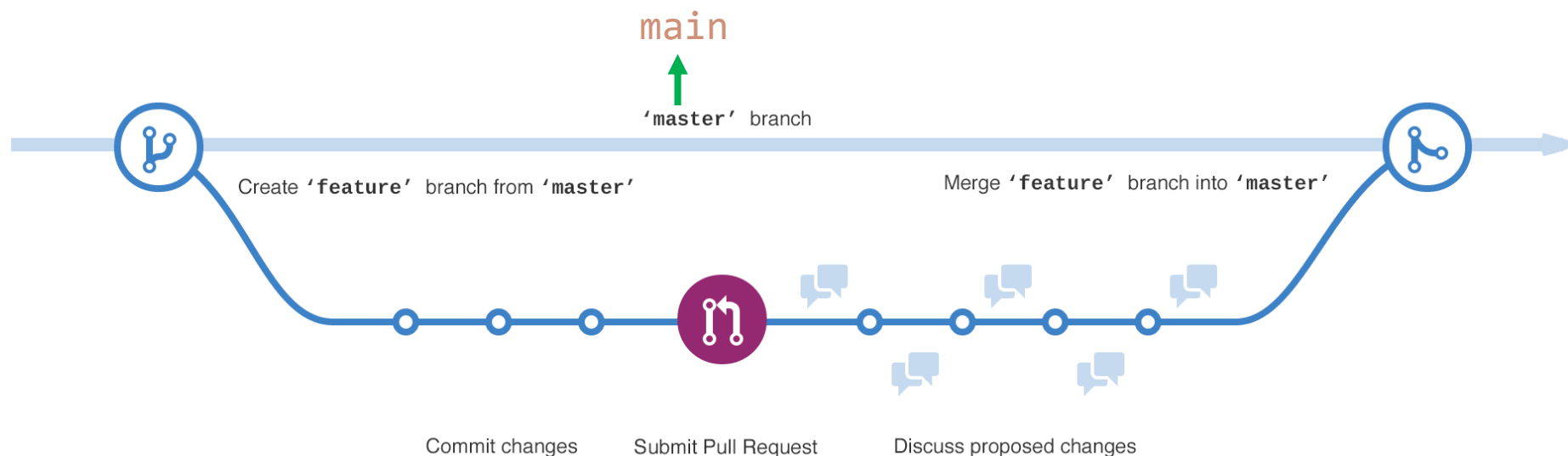
WHAT IS DEVOPS & DEVSECOPS?



Continuous Integration (CI) & Continuous Delivery (CD)



GitHub Flow



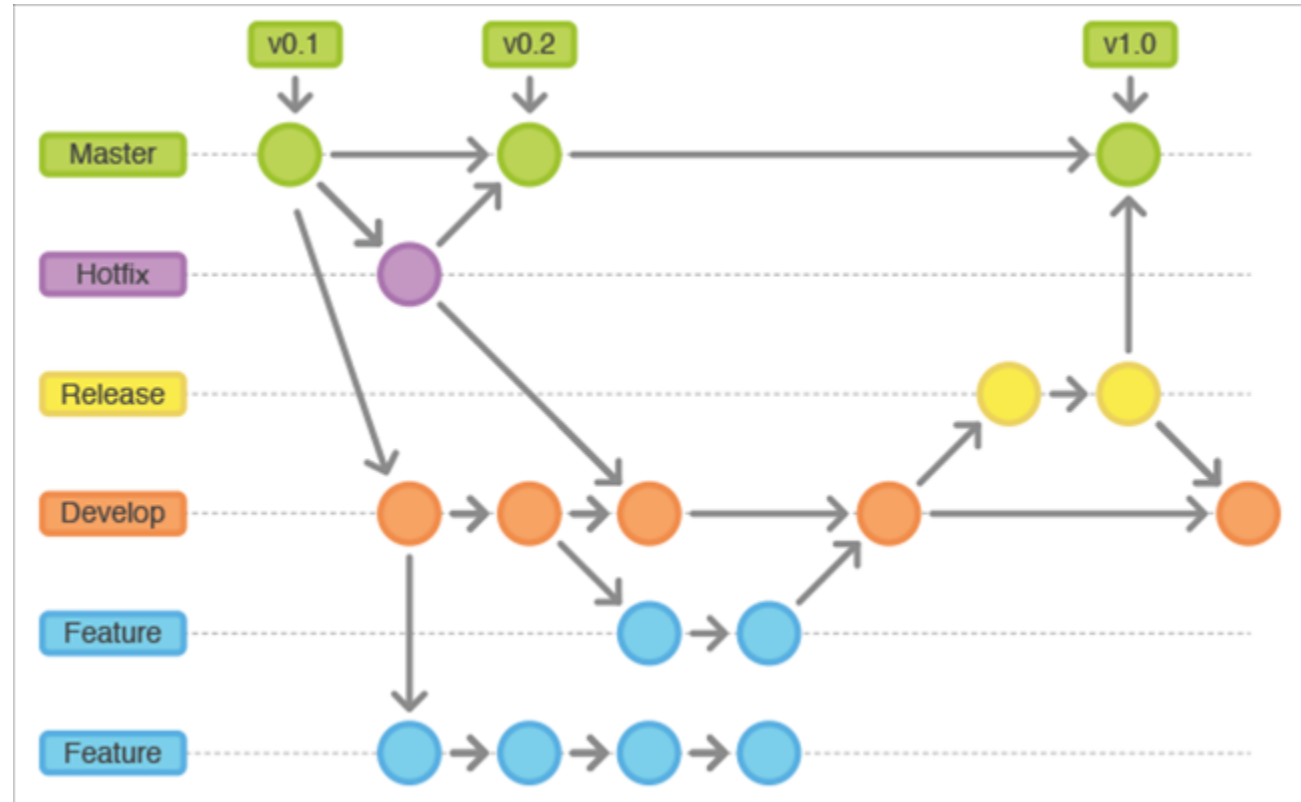
WHAT IS DEVOPS & DEVSECOPS?



Continuous Integration (CI) & Continuous Delivery (CD)



Git Flow



WHAT IS DEVOPS & DEVSECOPS?



Continuous Integration (CI) & Continuous Delivery (CD)



`.github/workflows/pipeline.yml`

```
# Copyright 2024 Ignacio Asin (iasinDev)
#
# Licensed under the Apache License, Version 2.0 (the "License");
# you may not use this file except in compliance with the License.
# You may obtain a copy of the License at
#
#     http://www.apache.org/licenses/LICENSE-2.0
#
# Unless required by applicable law or agreed to in writing, software
# distributed under the License is distributed on an "AS IS" BASIS,
# WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
# See the License for the specific language governing permissions and
# limitations under the License.
















on:
  push:
    branches:
      - main
  pull_request:
  workflow_dispatch:
```


WHAT IS DEVOPS & DEVSECOPS?



Continuous Integration (CI) & Continuous Delivery (CD)



 GCP_PROJECT	Updated 11 minutes ago		
 GCP_REGION	Updated 11 minutes ago		
 GCP_SA_KEY	Updated 11 minutes ago		
 GCP_ZONE	Updated 10 minutes ago		
 SERVICE_NAME	Updated 10 minutes ago		

WHAT IS DEVOPS & DEVSECOPS?



Continuous Integration (CI) & Continuous Delivery (CD)



`.github/workflows/pipeline.yml`

```
name: Build, Check and Deploy to Cloud Run on GCP
env:
  PROJECT_ID: ${ secrets.GCP_PROJECT }
  SERVICE: ${ secrets.SERVICE_NAME }
  REGION: ${ secrets.GCP_REGION }
  ZONE: ${ secrets.GCP_ZONE }

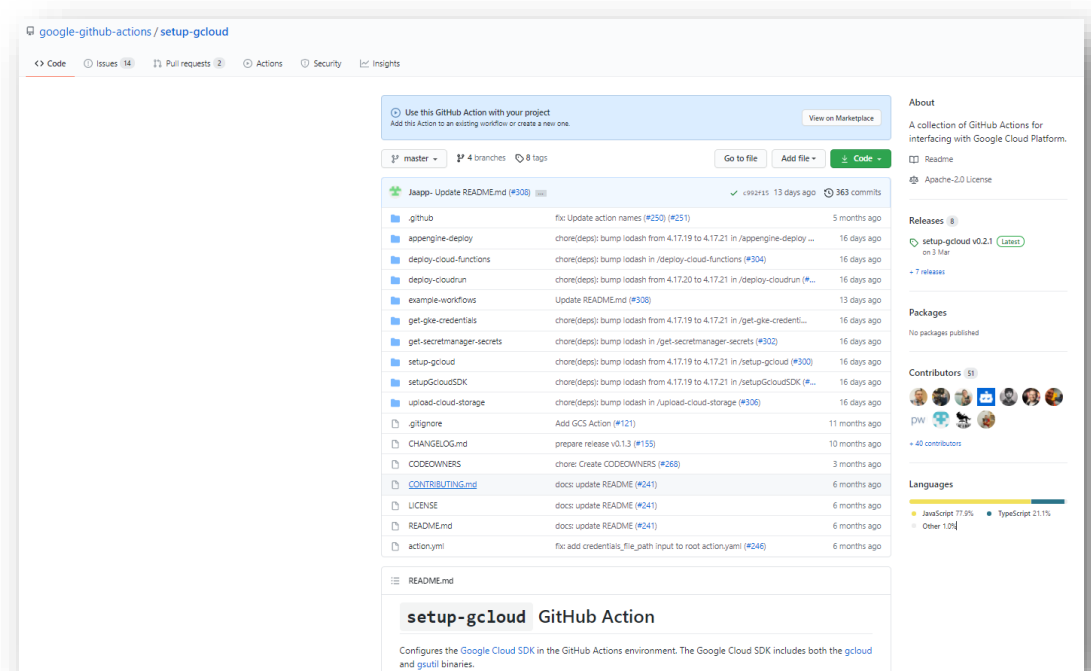
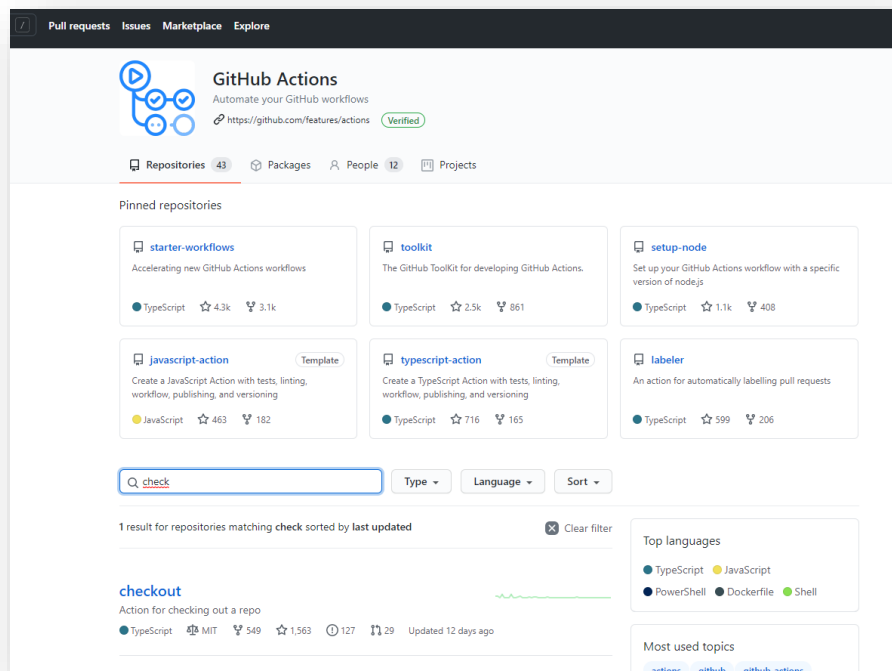
jobs:
```

WHAT IS DEVOPS & DEVSECOPS?

Continuous Integration (CI) & Continuous Delivery (CD)



Examples here, here and here

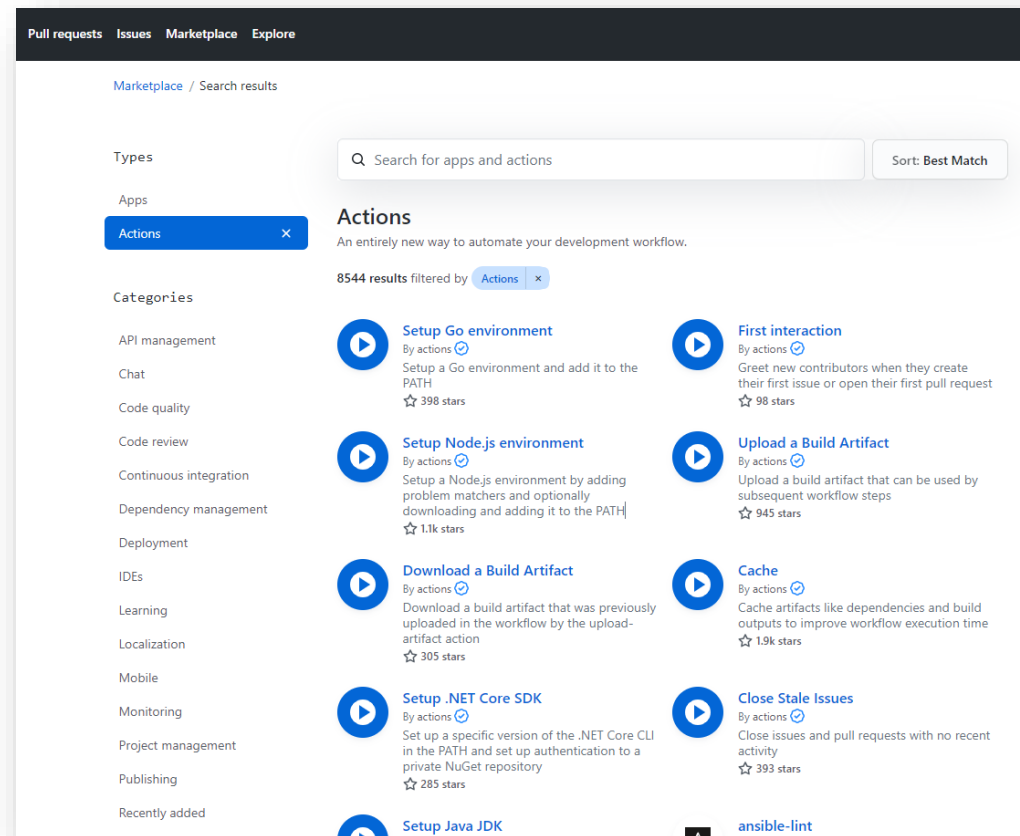


WHAT IS DEVOPS & DEVSECOPS?

Continuous Integration (CI) & Continuous Delivery (CD)



<https://github.com/marketplace?type=actions>



WHAT IS DEVOPS & DEVSECOPS?



Continuous Integration (CI) & Continuous Delivery (CD)



`.github/workflows/pipeline.yml`

```
build-and-push-container-image:

  runs-on: ubuntu-latest

  steps:

    - name: Enable GitHub Actions
      uses: actions/checkout@v3.3.0

    - id: auth
      uses: google-github-actions/auth@v1
      with:
        credentials_json: ${{ secrets.GCP_SA_KEY }}

    - name: Set up Cloud SDK
      uses: google-github-actions/setup-gcloud@v1
      with:
        project_id: ${{ env.PROJECT_ID }}
```

WHAT IS DEVOPS & DEVSECOPS?



Continuous Integration (CI) & Continuous Delivery (CD)



`.github/workflows/pipeline.yml`

- `name:` Check GCP account details
`run:` `gcloud config list`
- `name:` Authorize Docker push
`run:` `gcloud auth configure-docker`

WHAT IS DEVOPS & DEVSECOPS?

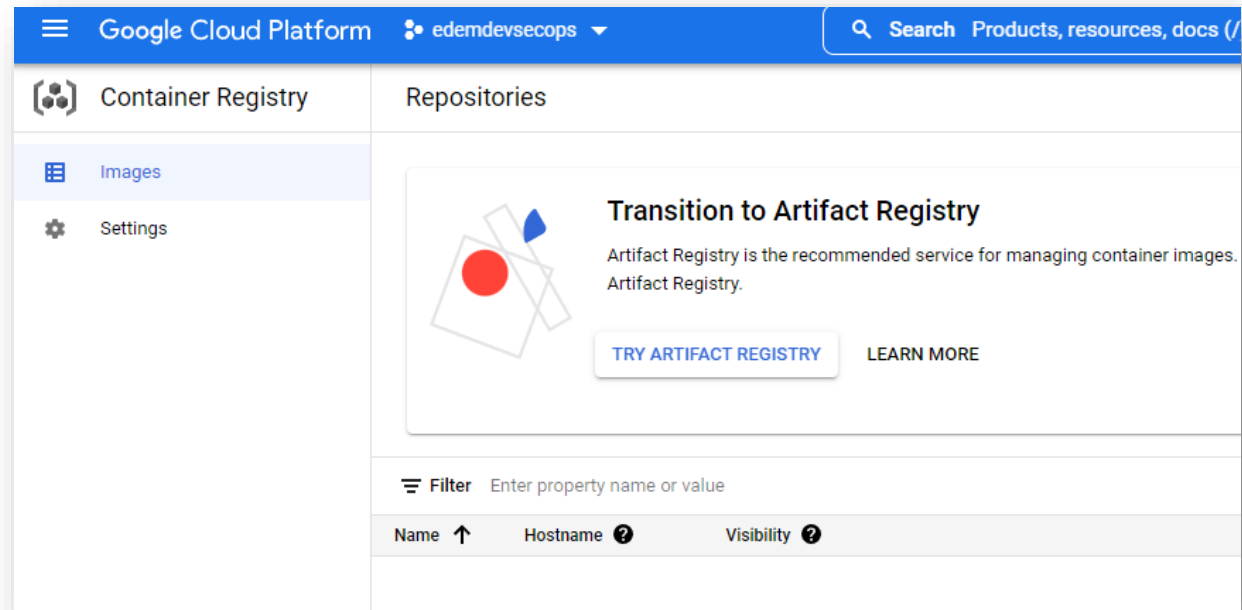
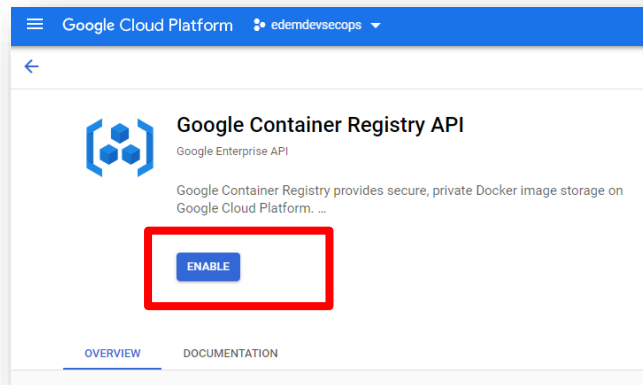


Continuous Integration (CI) & Continuous Delivery (CD)



Enable the Container Registry API

<https://console.cloud.google.com/marketplace/product/google/containerregistry.googleapis.com>



WHAT IS DEVOPS & DEVSECOPS?

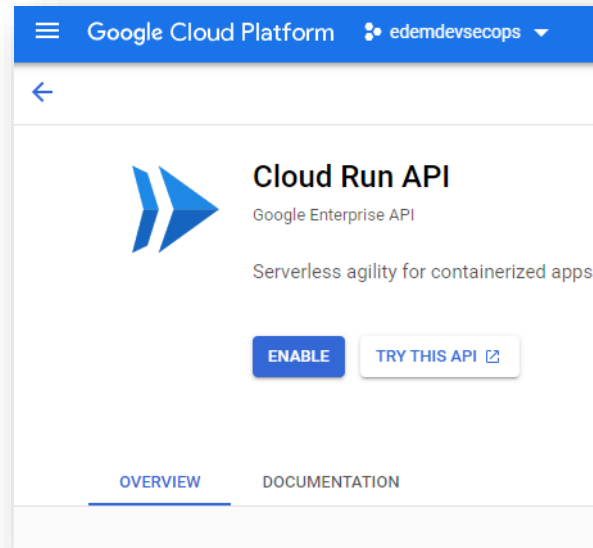


Continuous Integration (CI) & Continuous Delivery (CD)



Enable also the Cloud Run API

<https://console.cloud.google.com/apis/library/run.googleapis.com>



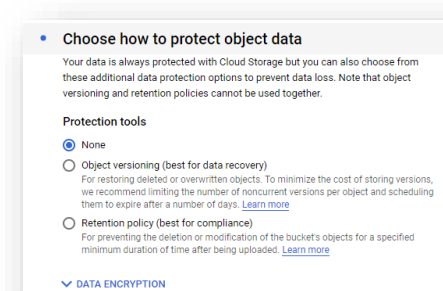
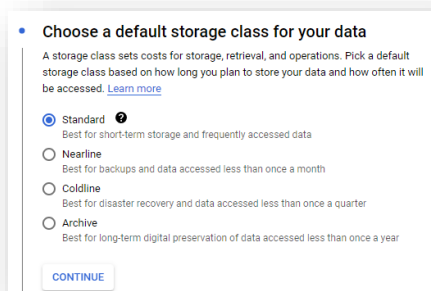
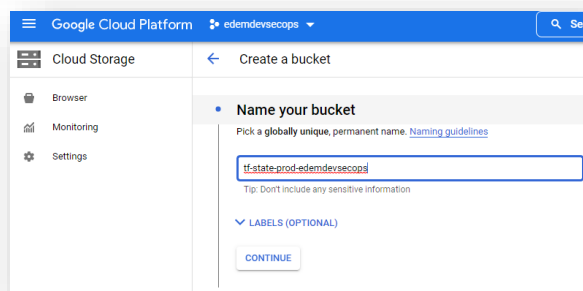
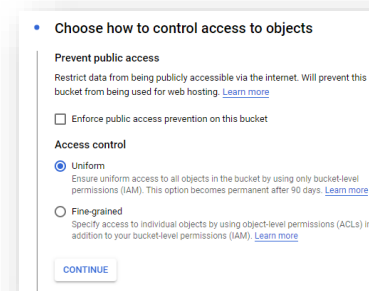
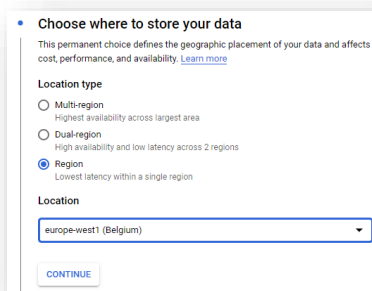
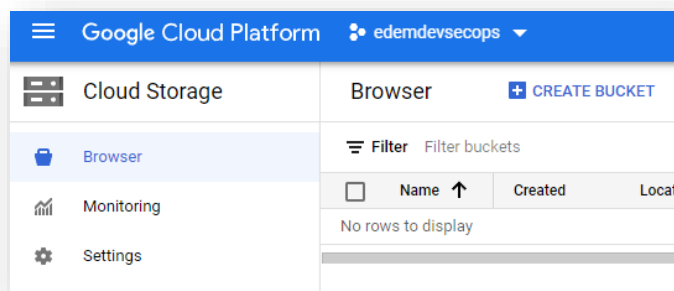
WHAT IS DEVOPS & DEVSECOPS?



Continuous Integration (CI) & Continuous Delivery (CD)



In Google Cloud create a bucket called "tf-state-prod-edemdevsecops" or a free name



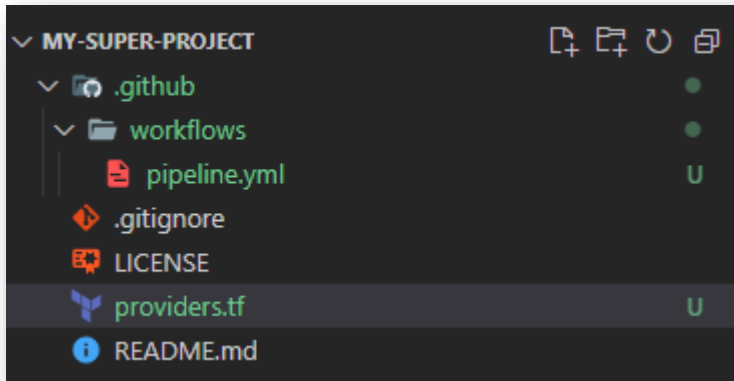
WHAT IS DEVOPS & DEVSECOPS?



Continuous Integration (CI) & Continuous Delivery (CD)



In Google Cloud create a bucket called "tf-state-prod-edemdevsecop" or a **free name**



```
provider "google" {  
  project = var.project_id  
  region  = var.region  
  zone    = var.zone  
}
```

```
terraform {  
  backend "gcs" {  
    bucket = "tf-state-prod-edemdevsecops"  
    prefix = "terraform/state"  
  }  
}
```

Same name

WHAT IS DEVOPS & DEVSECOPS?



Continuous Integration (CI) & Continuous Delivery (CD)



`.github/workflows/pipeline.yml`

```
- name: Build and Push Container
  run: |-
    docker build -t gcr.io/${{ env.PROJECT_ID }}/${{ env.SERVICE }}:${{ github.sha }} .
    docker push gcr.io/${{ env.PROJECT_ID }}/${{ env.SERVICE }}:${{ github.sha }}
    docker build -t gcr.io/${{ env.PROJECT_ID }}/${{ env.SERVICE }}:latest .
    docker push gcr.io/${{ env.PROJECT_ID }}/${{ env.SERVICE }}:latest
```

WHAT IS DEVOPS & DEVSECOPS?



Continuous Integration (CI) & Continuous Delivery (CD)



The screenshot shows the HashiCorp Terraform website. The top navigation bar includes the HashiCorp logo, 'Browse Products', and 'About HashiCorp'. Below this is the 'Terraform' logo and a navigation menu with 'Overview', 'Editions', 'Registry', 'Tutorials', 'Docs', 'Community', and 'GitHub'. There are buttons for 'Download CLI' and 'Terraform Cloud'. A 'BLOG POST' link is visible with the text 'Announcing Controlled Remote State Access'. The main heading is 'Write, Plan, Apply', followed by a paragraph describing Terraform as an open-source infrastructure as code software tool. A 'Get started' button is at the bottom left. On the right, a terminal window shows the output of 'terraform init', including 'Initializing the backend...' and 'Initializing provider plugins...'.

HashiCorp Browse Products About HashiCorp

Terraform Overview Editions Registry Tutorials Docs Community GitHub Download CLI Terraform Cloud

BLOG POST Announcing Controlled Remote State Access →

Write, Plan, Apply

Terraform is an open-source infrastructure as code software tool that provides a consistent CLI workflow to manage hundreds of cloud services. Terraform codifies cloud APIs into declarative configuration files.

Get started

```
→ iac-in-action git:(main) × terraform init

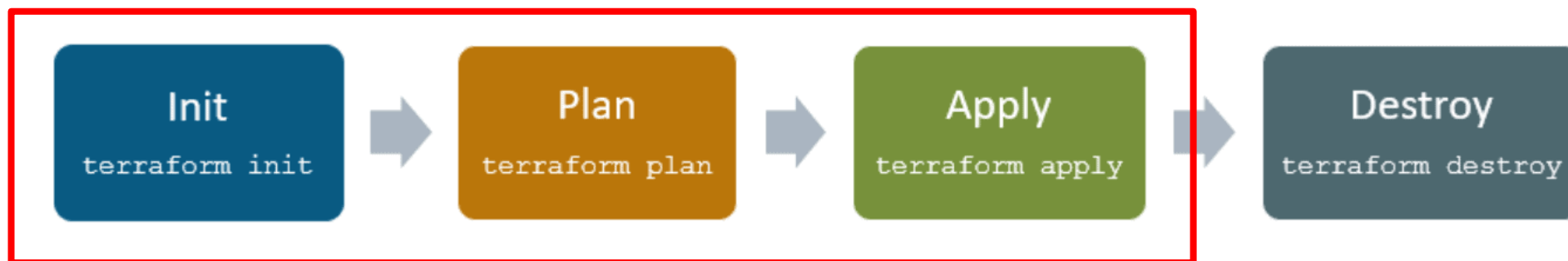
Initializing the backend...

Initializing provider plugins...
- Finding hashicorp/tls versions matching "~> 2.1"...
- Finding hashicorp/http versions matching "1.2.0"...
- Finding hashicorp/aws versions matching "~> 2.70"...
- Finding hashicorp/local versions matching "~> 1.4.0"...
- Installing hashicorp/tls v2.2.0...
- Installed hashicorp/tls v2.2.0 (signed by HashiCorp)
- Installing hashicorp/http v1.2.0...
```

WHAT IS DEVOPS & DEVSECOPS?



Continuous Integration (CI) & Continuous Delivery (CD)



WHAT IS DEVOPS & DEVSECOPS?



Continuous Integration (CI) & Continuous Delivery (CD)



tfsec

A static analysis security scanner for your Terraform code

tfsec is a developer-first security scanner for Terraform templates. It uses static analysis and deep integration with the official HCL parser to ensure security issues can be detected before your infrastructure changes take effect.

Designed to run locally and in your CI pipelines, developer-friendly output and fully documented checks mean detection and remediation can take place as quickly and efficiently as possible

WHAT IS DEVOPS & DEVSECOPS?



Continuous Integration (CI) & Continuous Delivery (CD)



`.github/workflows/pipeline.yml`

```
check-terraform-security:

  needs: build-and-push-container-image

  runs-on: ubuntu-latest

  steps:

    - name: Clone repo
      uses: actions/checkout@v3.3.0

    - name: Run tfsec
      uses: aquasecurity/tfsec-action@v1.0.0
```

WHAT IS DEVOPS & DEVSECOPS?



Continuous Integration (CI) & Continuous Delivery (CD)



```
Run tfsec
15
-e "GITHUB_TOKEN" -e "GITHUB_WORKFLOW" -e "GITHUB_WORKFLOW_SHA" -e "GITHUB_WORKSPACE" -e "GITHUB_ACTION" -e "GITHUB_EVENT_PATH" -e "GITHUB_ACTION_REPOSITORY" -e "GITHUB_ACTION_REF" -e
"GITHUB_REF_PROTECTED" -e "GITHUB_REF_TYPE" -e "GITHUB_WORKFLOW_REF" -e "GITHUB_WORKFLOW_SHA" -e "GITHUB_WORKSPACE" -e "GITHUB_ACTION" -e "GITHUB_EVENT_PATH" -e "GITHUB_ACTION_REPOSITORY" -e
"GITHUB_PATH" -e "GITHUB_ENV" -e "GITHUB_STEP_SUMMARY" -e "GITHUB_STATE" -e "GITHUB_OUTPUT" -e "RUNNER_OS" -e "RUNNER_ARCH" -e "RUNNER_NAME" -e "RUNNER_TOOL_CACHE" -e "RUNNER_TEMP" -e "RUNNER_WORKSPACE" -e
"ACTIONS_RUNTIME_URL" -e "ACTIONS_RUNTIME_TOKEN" -e "ACTIONS_CACHE_URL" -e "GITHUB_ACTIONS" -e "CI=true" -e "CI=true" -e "/var/run/docker.sock" -e "/var/run/docker.sock" -e "/home/runner/work/_temp/_github_home" -e
"/home/runner/work/_temp/_github_workflow" -e "/github/workflow" -e "/home/runner/work/_temp/_runner_file_commands" -e "/github/file_commands" -e "/home/runner/work/my-super-project/my-super-project" -e
"/github/workspace"
ea425b:4d5e22bfb2864eb980a62e13187bb4bb
13 + TFSEC_VERSION=latest
14 + '[' latest != latest ']'
15 ++ grep -o -E 'https://.*tfsec-linux-amd64'
16 ++ wget -q https://api.github.com/repos/aquasecurity/tfsec/releases/latest -O -
17 ++ head -n1
18 + wget -O - -q https://github.com/aquasecurity/tfsec/releases/download/v1.28.1/tfsec-linux-amd64
19 + install tfsec /usr/local/bin/
20 + '[' -n /github/workspace ']'
21 + cd /github/workspace
22 + '[' -n '' ']'
23 + '[' -n '' ']'
24 + FORMAT=default
25 + tfsec --format=default .
26
timings
27
28 disk i/o      45.1µs
29 parsing      493.6µs
30 adaptation    78.2µs
31 checks       7.443405ms
32 total        8.860305ms
33
34 counts
35
36 modules downloaded 0
37 modules processed 1
38 blocks processed 10
39 files read 3
40
41 results
42
43 passed 2
44 ignored 0
45 critical 0
46 high 0
47 medium 0
48 low 0
49
50
51 No problems detected!
52
```


WHAT IS DEVOPS & DEVSECOPS?



Continuous Integration (CI) & Continuous Delivery (CD)



`.github/workflows/pipeline.yml`

```
deploy-in-cloud-run:

  needs: [build-and-push-container-image, check-terraform-security]

  runs-on: ubuntu-latest

  steps:

    - name: Enable GitHub Actions
      uses: actions/checkout@v3.3.0

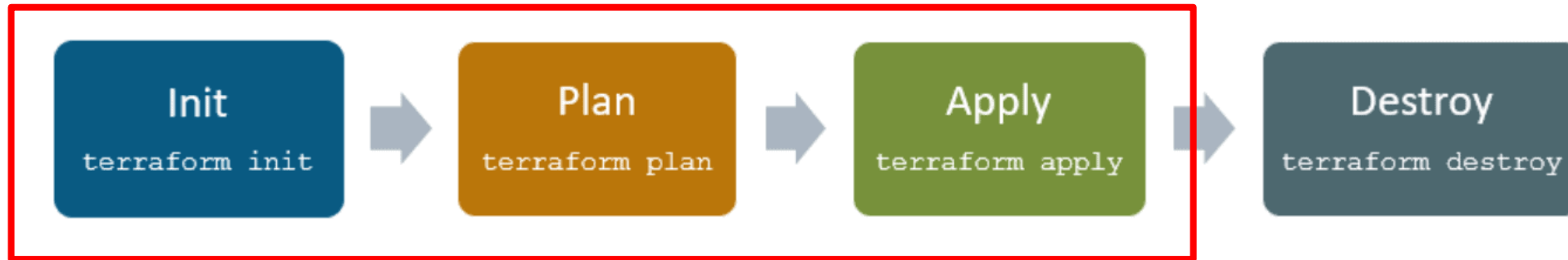
    - id: auth
      uses: google-github-actions/auth@v1
      with:
        credentials_json: ${ secrets.GCP_SA_KEY }

    - name: Set up Cloud SDK
      uses: google-github-actions/setup-gcloud@v1
      with:
        project_id: ${ env.PROJECT_ID }
```

WHAT IS DEVOPS & DEVSECOPS?



Continuous Integration (CI) & Continuous Delivery (CD)



WHAT IS DEVOPS & DEVSECOPS?



Continuous Integration (CI) & Continuous Delivery (CD)



`.github/workflows/pipeline.yml`

```
- name: Getting tag of the built image
  run: |-
    image_tag=$(gcloud container images list-tags gcr.io/${{ env.PROJECT_ID }}/${{ env.SERVICE }} --limit=1 --sort-by=~TIMESTAMP --format='get(tags)')
    IFS=';' read -ra image_tag_ARRAY <<< "$image_tag"
    image_tag=${image_tag_ARRAY[0]}
    echo "image_tag: $image_tag"
    echo "image_tag=$image_tag" >> $GITHUB_ENV

# Install the latest version of Terraform CLI and configure the Terraform CLI configuration file with a Terraform Cloud user API token
- name: Setup Terraform
  uses: hashicorp/setup-terraform@v2.0.3
```

WHAT IS DEVOPS & DEVSECOPS?

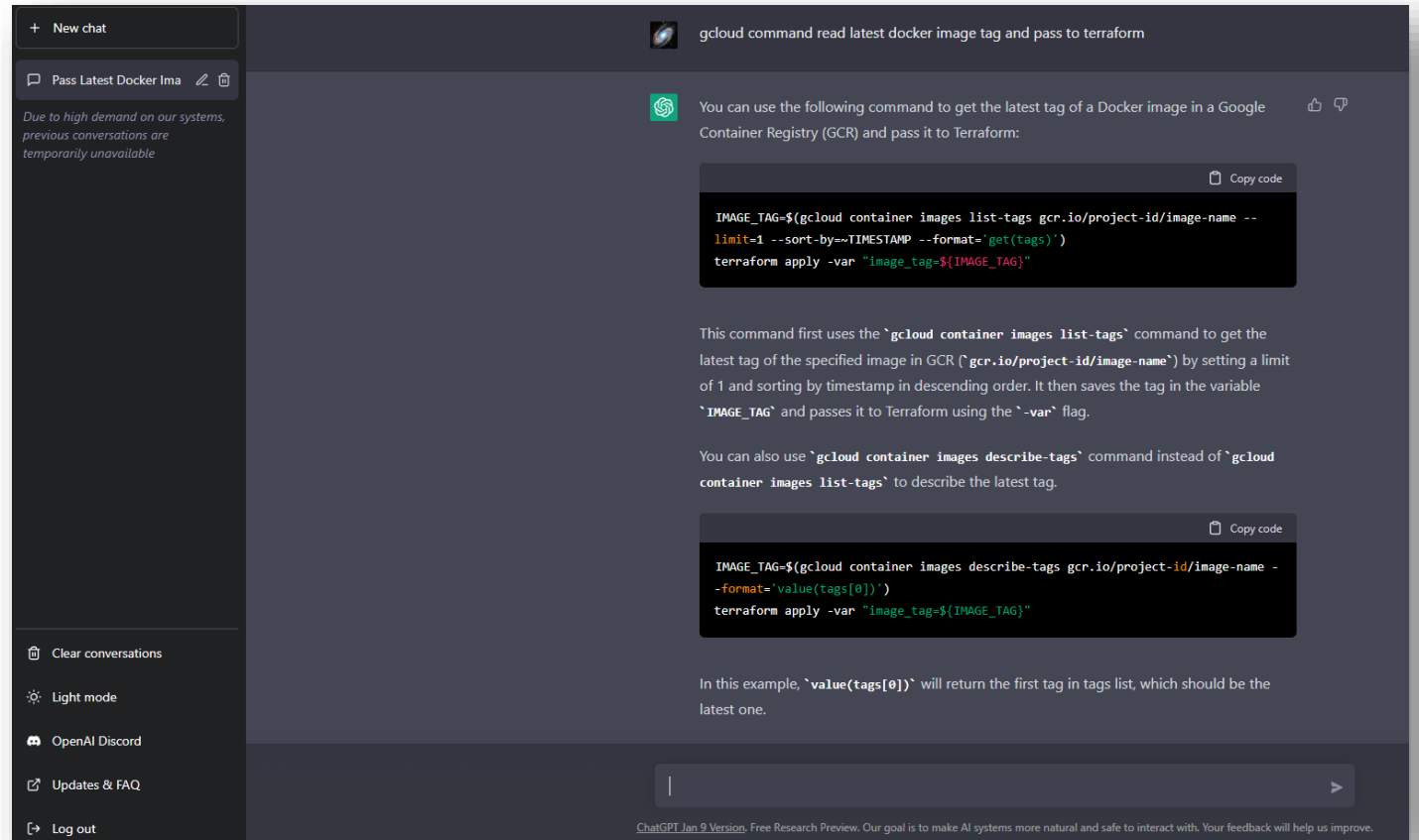


Continuous Integration (CI) & Continuous Delivery (CD)



`.github/workflows/pipeline.yml`

ChatGPT-3



WHAT IS DEVOPS & DEVSECOPS?



Continuous Integration (CI) & Continuous Delivery (CD)



`.github/workflows/pipeline.yml`

```
# Initialize a new or existing Terraform working directory by creating initial files, loading any remote state, downloading modules, etc.
- name: Terraform Init
  run: |
    echo "image_tag: ${ env.image_tag }"
    terraform init
  env:
    GOOGLE_CREDENTIALS: ${ secrets.GCP_SA_KEY }
    TF_VAR_project_id: ${ env.PROJECT_ID }
    TF_VAR_region: ${ env.REGION }
    TF_VAR_zone: ${ secrets.GCP_ZONE }
```

WHAT IS DEVOPS & DEVSECOPS?



Continuous Integration (CI) & Continuous Delivery (CD)



`.github/workflows/pipeline.yml`

```
# Generates an execution plan for Terraform
- name: Terraform Plan
  run: terraform plan -lock=false
  env:
    GOOGLE_CREDENTIALS: ${ secrets.GCP_SA_KEY }
    TF_VAR_project_id: ${ env.PROJECT_ID }
    TF_VAR_region: ${ env.REGION }
    TF_VAR_zone: ${ env.ZONE }
    TF_VAR_service: ${ env.SERVICE }
    TF_VAR_image_tag: ${ env.image_tag }
```

WHAT IS DEVOPS & DEVSECOPS?



Continuous Integration (CI) & Continuous Delivery (CD)



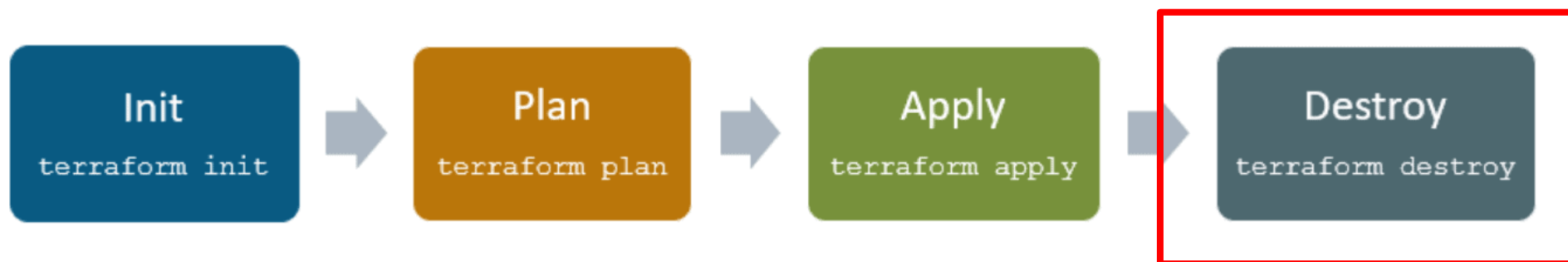
`.github/workflows/pipeline.yml`

```
# Apply the execution plan
- name: Terraform Apply
  if: github.ref == 'refs/heads/main'
  run: terraform apply -lock=false -auto-approve
  env:
    GOOGLE_CREDENTIALS: ${ secrets.GCP_SA_KEY }
    TF_VAR_project_id: ${ env.PROJECT_ID }
    TF_VAR_region: ${ env.REGION }
    TF_VAR_zone: ${ env.ZONE }
    TF_VAR_service: ${ env.SERVICE }
    TF_VAR_image_tag: ${ env.image_tag }
```

WHAT IS DEVOPS & DEVSECOPS?



Continuous Integration (CI) & Continuous Delivery (CD)



WHAT IS DEVOPS & DEVSECOPS?



Continuous Integration (CI) & Continuous Delivery (CD)



`.github/workflows/destroy.yml`

```
# Copyright 2021 Ignacio Asin (iasinDev)
#
# Licensed under the Apache License, Version 2.0 (the "License");
# you may not use this file except in compliance with the License.
# You may obtain a copy of the License at
#
#     http://www.apache.org/licenses/LICENSE-2.0
#
# Unless required by applicable law or agreed to in writing, software
# distributed under the License is distributed on an "AS IS" BASIS,
# WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
# See the License for the specific language governing permissions and
# limitations under the License.

on:
  workflow_dispatch:
```

WHAT IS DEVOPS & DEVSECOPS?



Continuous Integration (CI) & Continuous Delivery (CD)



`.github/workflows/destroy.yml`

```
name: Destroy GCP resources
env:
  PROJECT_ID: ${ secrets.GCP_PROJECT }
  SERVICE: ${ secrets.SERVICE_NAME }
  REGION: ${ secrets.GCP_REGION }
  ZONE: ${ secrets.GCP_ZONE }

jobs:
```

WHAT IS DEVOPS & DEVSECOPS?



Continuous Integration (CI) & Continuous Delivery (CD)



`.github/workflows/destroy.yml`

```
destroy-terraform-resources:
```

```
  runs-on: ubuntu-latest
```

```
  steps:
```

- name: Enable GitHub Actions
 uses: actions/checkout@v3.3.0
- id: auth
 uses: google-github-actions/auth@v1
 with:
 credentials_json: \${{ secrets.GCP_SA_KEY }}
- name: Set up Cloud SDK
 uses: google-github-actions/setup-gcloud@v1
 with:
 project_id: \${{ env.PROJECT_ID }}

WHAT IS DEVOPS & DEVSECOPS?



Continuous Integration (CI) & Continuous Delivery (CD)



`.github/workflows/destroy.yml`

```
- name: Getting tag of the built image
  run: |-
    image_tag=$(gcloud container images list-tags gcr.io/${{ env.PROJECT_ID }}/${{ env.SERVICE }} --limit=1 --sort-by=~TIMESTAMP --format='get(tags)')
    IFS=';' read -ra image_tag_ARRAY <<< "$image_tag"
    image_tag=${image_tag_ARRAY[0]}
    echo "image_tag: $image_tag"
    echo "image_tag=$image_tag" >> $GITHUB_ENV

# Install the latest version of Terraform CLI and configure the Terraform CLI configuration file with a Terraform Cloud user API token
- name: Setup Terraform
  uses: hashicorp/setup-terraform@v2.0.3
```

WHAT IS DEVOPS & DEVSECOPS?



Continuous Integration (CI) & Continuous Delivery (CD)



`.github/workflows/destroy.yml`

```
# Initialize a new or existing Terraform working directory by creating initial files, loading any remote state, downloading modules, etc.
- name: Terraform Init
  run: terraform init
  env:
    GOOGLE_CREDENTIALS: ${ secrets.GCP_SA_KEY }
    TF_VAR_project_id: ${ env.PROJECT_ID }
    TF_VAR_region: ${ env.REGION }
    TF_VAR_zone: ${ secrets.GCP_ZONE }
```

WHAT IS DEVOPS & DEVSECOPS?



Continuous Integration (CI) & Continuous Delivery (CD)



`.github/workflows/destroy.yml`

```
# Destroy the resources
- name: Terraform Destroy
  run: terraform destroy -lock=false -auto-approve
  env:
    GOOGLE_CREDENTIALS: ${ secrets.GCP_SA_KEY }
    TF_VAR_project_id: ${ env.PROJECT_ID }
    TF_VAR_region: ${ env.REGION }
    TF_VAR_zone: ${ env.ZONE }
    TF_VAR_service: ${ env.SERVICE }
    TF_VAR_image_tag: ${ env.image_tag }
```

WHAT IS DEVOPS & DEVSECOPS?

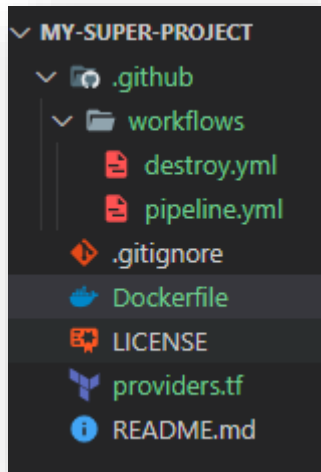


“Application as Code” ... “Platform as Code”



Containerization

Dockerfile



Dockerfile Multistage

```
# Use the official Golang image to create a build artifact.  
# This is based on Debian and sets the GOPATH to /go.  
# https://hub.docker.com/_/golang  
FROM golang:1.13 as builder
```

```
# Create and change to the app directory.  
WORKDIR /app
```

```
# Copy local code to the container image.  
COPY ./main.go ./main.go
```

```
# Build the binary.  
RUN CGO_ENABLED=0 GOOS=linux go build -v -o server
```

```
# Use the official Alpine image for a lean production container.  
# https://hub.docker.com/_/alpine  
# https://docs.docker.com/develop/develop-images/multistage-build/#use-multi-stage-builds  
FROM alpine:3  
RUN apk add --no-cache ca-certificates
```

```
# Copy the binary to the production image from the builder stage.  
COPY --from=builder /app/server /server  
COPY ./snake.html ./snake.html
```

```
# Run the web service on container startup.  
CMD ["/server"]
```

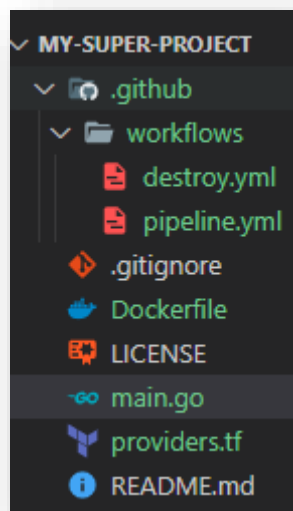
WHAT IS DEVOPS & DEVSECOPS?



“Application as Code” ... “Platform as Code”



main.go



```
package main

import (
    "fmt"
    "log"
    "net/http"
    "io/ioutil"
)

func handler(w http.ResponseWriter, r *http.Request) {
    file, err := ioutil.ReadFile("./snake.html")
    if err != nil {
        fmt.Print(err)
    }
    log.Print("Serving the body")
    log.Print(string(file))
    body := string(file)
    fmt.Fprintf(w, body)
}

func main() {
    log.Print("Hello world webapp started.")

    http.HandleFunc("/", handler)

    port := "8080"

    log.Fatal(http.ListenAndServe(fmt.Sprintf(":%s", port), nil))
}
```


WHAT IS DEVOPS & DEVSECOPS?

“Application as Code” ... “Platform as Code”



snake.html

Copy from
the
solution

```
<!DOCTYPE html>
<html>
<head>
  <title></title>
  <style>
    html, body {
      height: 100%;
      margin: 0;
    }

    body {
      background: black;
      display: flex;
      align-items: center;
      justify-content: center;
    }
    canvas {
  }
  ...
```

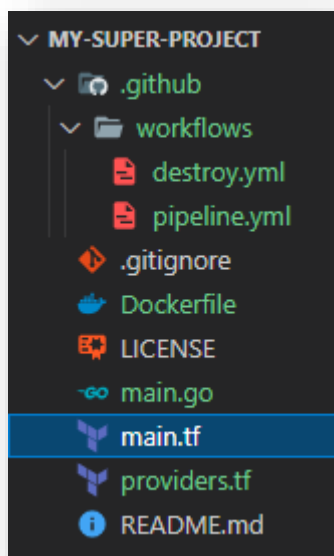
WHAT IS DEVOPS & DEVSECOPS?



Infrastructure as Code



main.tf



```
resource "google_cloud_run_service" "edemdevsecops" {
  name      = "edemdevsecops"
  location = var.region

  template {
    spec {
      containers {
        image = "gcr.io/${var.project_id}/${var.service}:${var.image_tag}"
      }
    }
  }

  traffic {
    percent          = 100
    latest_revision = true
  }
}
```

WHAT IS DEVOPS & DEVSECOPS?



Infrastructure as Code



main.tf

```
data "google_iam_policy" "noauth" {
  binding {
    role = "roles/run.invoker"
    members = [
      "allUsers",
    ]
  }
}

resource "google_cloud_run_service_iam_policy" "noauth" {

  depends_on = [
    google_cloud_run_service.edemdevsecops,
  ]

  location      = var.region
  project       = var.project_id
  service       = var.service

  policy_data = data.google_iam_policy.noauth.policy_data
}
```

WHAT IS DEVOPS & DEVSECOPS?



Infrastructure as Code



providers.tf

```
provider "google" {  
  project = var.project_id  
  region  = var.region  
  zone    = var.zone  
}  
  
terraform {  
  backend "gcs" {  
    bucket = "tf-state-prod-edemdevsecops-2023"  
    prefix = "terraform/state"  
  }  
}
```

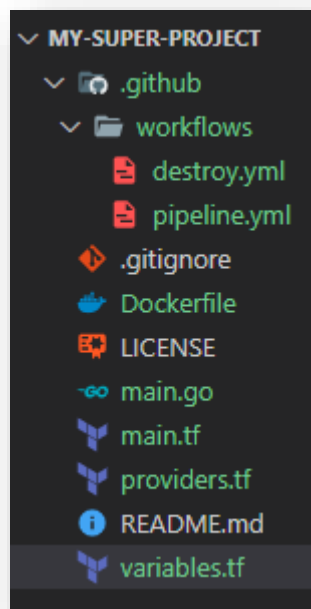
WHAT IS DEVOPS & DEVSECOPS?



Infrastructure as Code



variables.tf



```
variable "project_id" {  
    type = string  
}  
  
variable "region" {  
    type = string  
}  
  
variable "zone" {  
    type = string  
}  
  
variable "service" {  
    type = string  
}  
  
variable "image_tag" {  
    type = string  
}
```

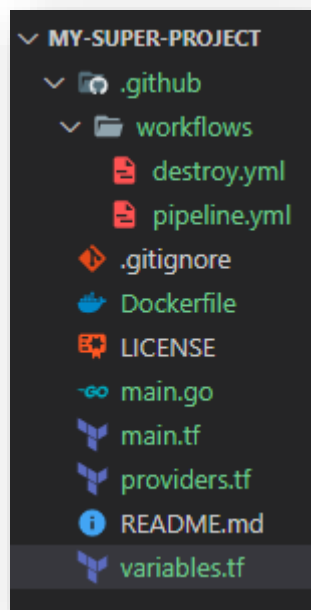
WHAT IS DEVOPS & DEVSECOPS?



Infrastructure as Code



.tf files



```
main.tf
main.tf
1 resource "google_cloud_run_service" "edemdevsecops" {
2   name      = "edemdevsecops"
3   location = var.region
4
5   template {
6     spec {
7       containers {
8         image = "gcr.io/${var.project_id}/${var.service}:${var.image_tag}"
9       }
10    }
11  }
12
13  traffic {
14    percent      = 100
15    latest_revision = true
16  }
17 }
18
19 data "google_iam_policy" "pauth" {
```

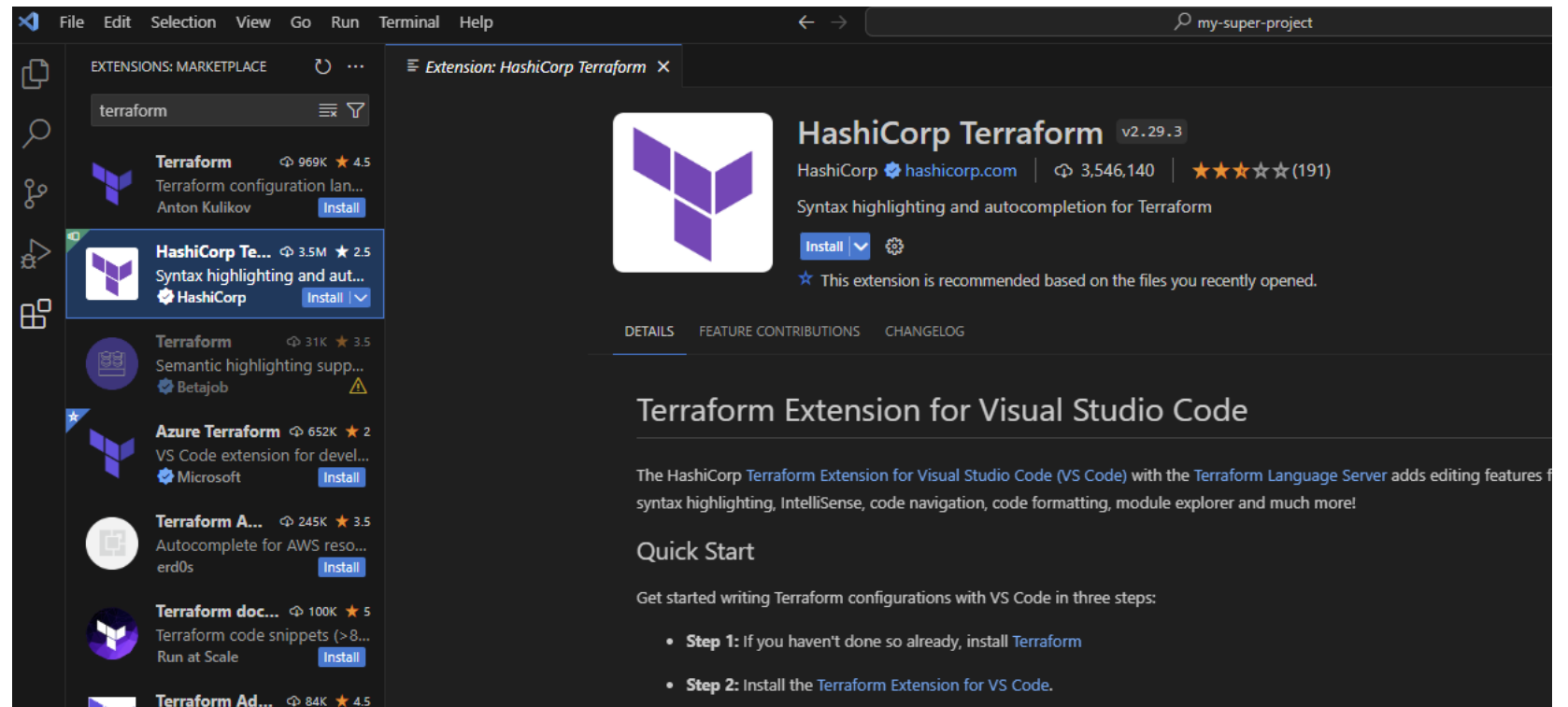
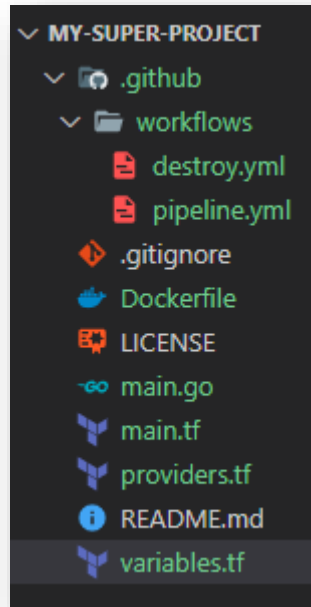
No syntax highlighting !!

WHAT IS DEVOPS & DEVSECOPS?

Infrastructure as Code



.tf files

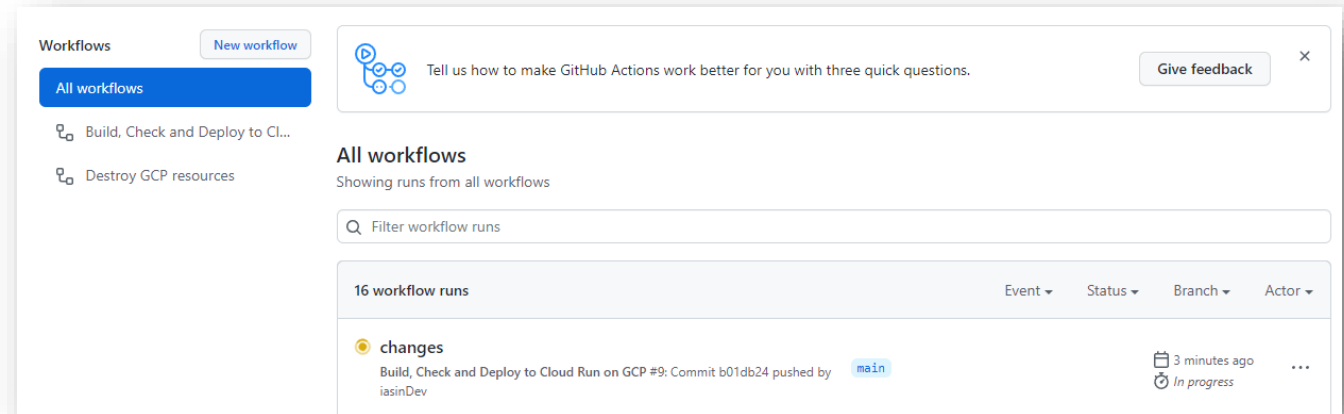
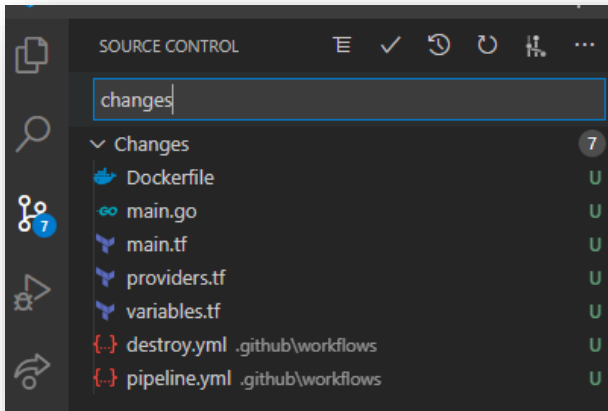


WHAT IS DEVOPS & DEVSECOPS?



Testing

commit & push your changes to GitHub



WHAT IS DEVOPS & DEVSECOPS?



Testing

PLUS

Semantic Versioning & Semantic Commit Messages

Major Minor Patch

v2.21.2

breaking changes features bugfixes and hotfixes

feat(website): add some cool stuff

↓ ↓ ↓

type scope subject

WHAT IS DEVOPS & DEVSECOPS?



Testing

See the pipeline execution

The screenshot shows the GitHub Actions interface for a repository named 'iasinDev / my-super-project'. The 'Actions' tab is selected, displaying a workflow named 'changes Build, Check and Deploy to Cloud Run on GCP #9'. The workflow status is 'Success', triggered by a push to the 'main' branch. The total duration is 3m 59s. The workflow consists of three jobs: 'build-and-push-container-image' (1m 6s), 'check-terraform-security' (9s), and 'deploy-in-cloud-run' (2m 4s). The 'Summary' tab is active, showing a list of jobs and their status. The 'pipeline.yml' file is also visible, showing the workflow definition.

Search or jump to... Pull requests Issues Marketplace Explore

iasinDev / my-super-project Private

<> Code Issues Pull requests **Actions** Projects Security Insights Settings

✓ changes Build, Check and Deploy to Cloud Run on GCP #9

Summary

Jobs

- ✓ build-and-push-container-image
- ✓ check-terraform-security
- ✓ deploy-in-cloud-run

Triggered via push 4 minutes ago

iasinDev pushed · b01db24 main

Status: Success

Total duration: 3m 59s

Artifacts: -

pipeline.yml

on: push

✓ build-and-push-containe... 1m 6s

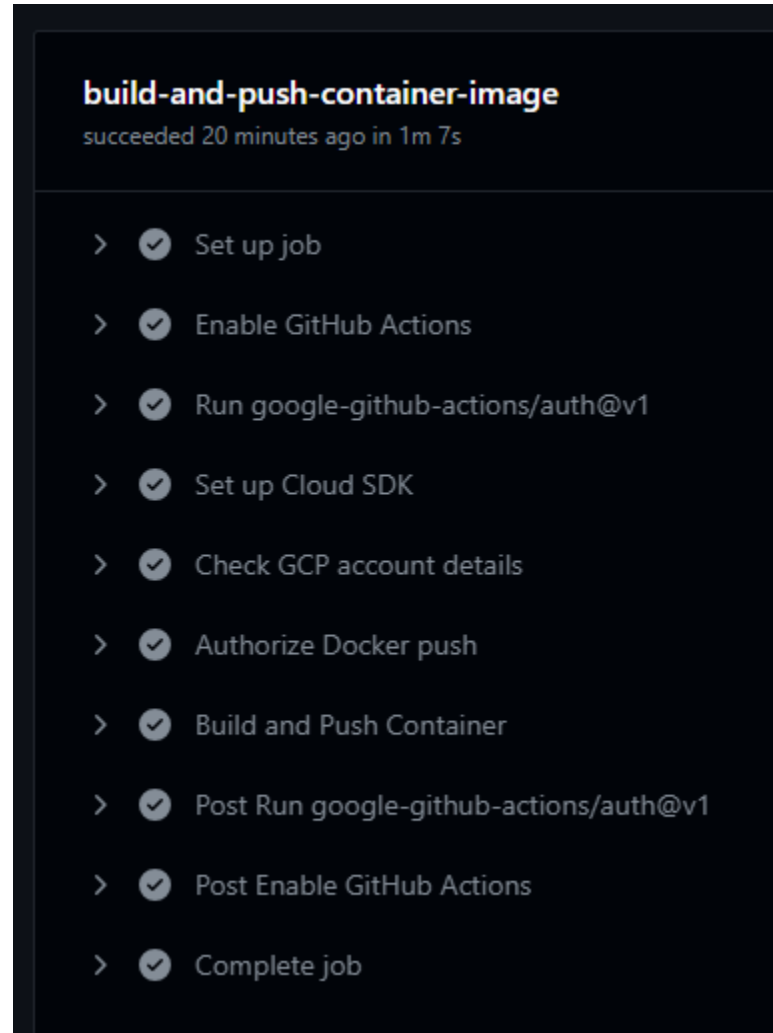
✓ check-terraform-security 9s

✓ deploy-in-cloud-run 2m 4s

WHAT IS DEVOPS & DEVSECOPS?

Testing

See the pipeline execution



WHAT IS DEVOPS & DEVSECOPS?



Testing

See the pipeline execution

Google Cloud Platform edemdevsecops							
Search cloud run							
Cloud Run Services + CREATE SERVICE MANAGE CUSTOM DOMAINS COPY DELETE							
Filter Filter services							
<input type="checkbox"/>	<input type="radio"/>	Name ↑	Req/sec ?	Region	Authentication ?	Ingress ?	Last deployed
<input type="checkbox"/>	<input checked="" type="radio"/>	edemdevsecops	0	europe-west1	Allow unauthenticated	All	1 minute ago
Deployed by edemdevops@edemdevsecops.iam.gserviceaccount.com							

WHAT IS DEVOPS & DEVSECOPS?



Testing

See the pipeline execution

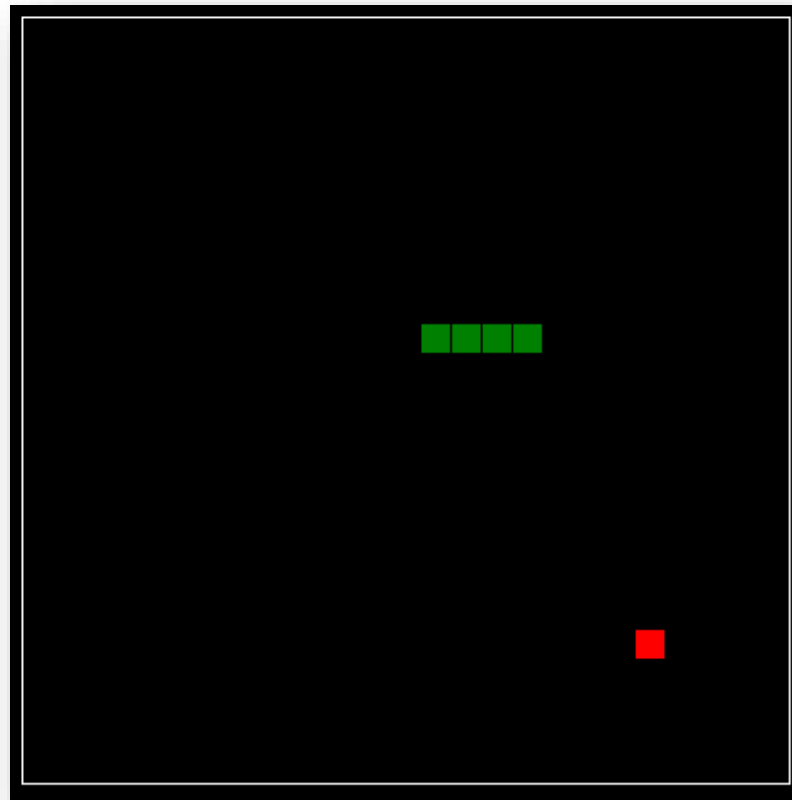
A screenshot of the Google Cloud Platform console. The top navigation bar is blue with the Google Cloud Platform logo, the project name 'edemdevsecops', and a search bar. Below the navigation bar, the 'Cloud Run' section is active, showing 'Service details' for the service 'edemdevsecops'. The region is 'europe-west1'. A red rectangle highlights the URL: <https://edemdevsecops-dyl5yf6hya-ew.a.run.app>. Below the URL, there are tabs for 'METRICS', 'LOGS', 'REVISIONS', 'TRIGGERS', 'DETAILS', 'YAML', and 'PERMISSIONS'. The 'METRICS' tab is selected, showing a message: 'No errors found during this interval.' At the bottom, there are sections for 'Request count' and 'Request latencies', each with a 'Create alerting policy' link and a search icon.

WHAT IS DEVOPS & DEVSECOPS?



Testing

See the pipeline execution



WHAT IS DEVOPS & DEVSECOPS?

Testing



WHAT IS DEVOPS & DEVSECOPS?



Security Management

Repositories


i Container Registry is deprecated. After May 15, 2024, Artifact Registry will host images for the gcr.io domain in projects without previous Container Registry usage. [Learn more](#)

Last updated 2024-01-31 UTC.

Container Registry is deprecated. After May 15, 2024, Artifact Registry will host images for the gcr.io domain in projects without previous Container Registry usage. If you use Container Registry, [learn about the deprecation](#). To get started with managing containers on Google Cloud, use [Artifact Registry](#).

Starting January 8, 2024, if your organization has not previously used Container Registry, new gcr.io repositories will be hosted on Artifact Registry by default. For more information on this change, see [gcr.io hosted on Artifact Registry](#).

Container Registry > Container Registry documentation > Resources

Was this helpful?  

Container Registry deprecation

[Send feedback](#)

Effective May 15, 2023, Container Registry is deprecated and is superseded by Artifact Registry.

We are taking a phased approach to discontinuing Container Registry. After May 15, 2024, Google Cloud projects without previous usage of Container Registry will only support hosting and managing images for the `gcr.io` domain in [Artifact](#)

WHAT IS DEVOPS & DEVSECOPS?



Continuous Integration (CI) & Continuous Delivery (CD)



Enable Artifact Registry API

<https://console.cloud.google.com/marketplace/product/google/artifactregistry.googleapis.com>



Artifact Registry API

[Google Enterprise API](#)

MANAGE

TRY THIS API [↗](#)

✓ API Enabled

WHAT IS DEVOPS & DEVSECOPS?








Security Management

Add to the created key the following rights:

- `Artifact Registry Administrator
- `Artifact Registry Create-On-Push Writer

Assign roles

Roles are composed of sets of permissions and determine what the principal can do with this resource. [Learn more](#)

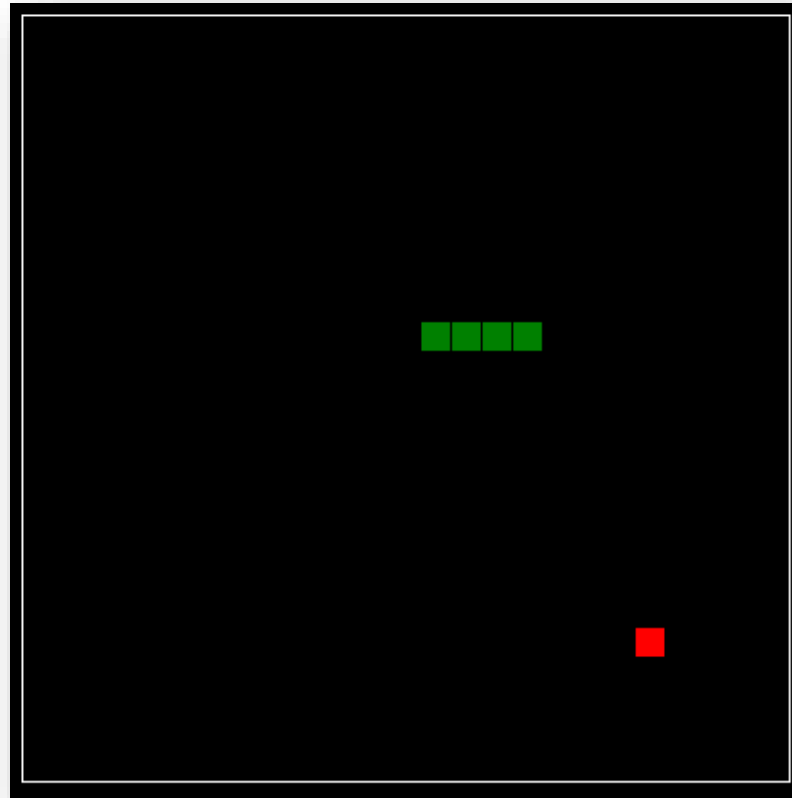
<div>Role</div> <div>Cloud Run Admin</div> <div>Full control over all Cloud Run resources.</div>	<div>IAM condition (optional) ?</div> <div>+ ADD IAM CONDITION</div>	
<div>Role</div> <div>Service Account User</div> <div>Run operations as the service account.</div>	<div>IAM condition (optional) ?</div> <div>+ ADD IAM CONDITION</div>	
<div>Role</div> <div>Storage Admin</div> <div>Grants full control of buckets and objects.</div>	<div>IAM condition (optional) ?</div> <div>+ ADD IAM CONDITION</div>	
<div>Role</div> <div>Artifact Registry Administrator</div> <div>Administrator access to create and manage repositories.</div>	<div>IAM condition (optional) ?</div> <div>+ ADD IAM CONDITION</div>	
<div>Role</div> <div>Artifact Registry Create-on-Push ...</div> <div>Access to read and write repository items, as well as create new repositories on push</div>	<div>IAM condition (optional) ?</div> <div>+ ADD IAM CONDITION</div>	

WHAT IS DEVOPS & DEVSECOPS?



Testing

See the pipeline execution

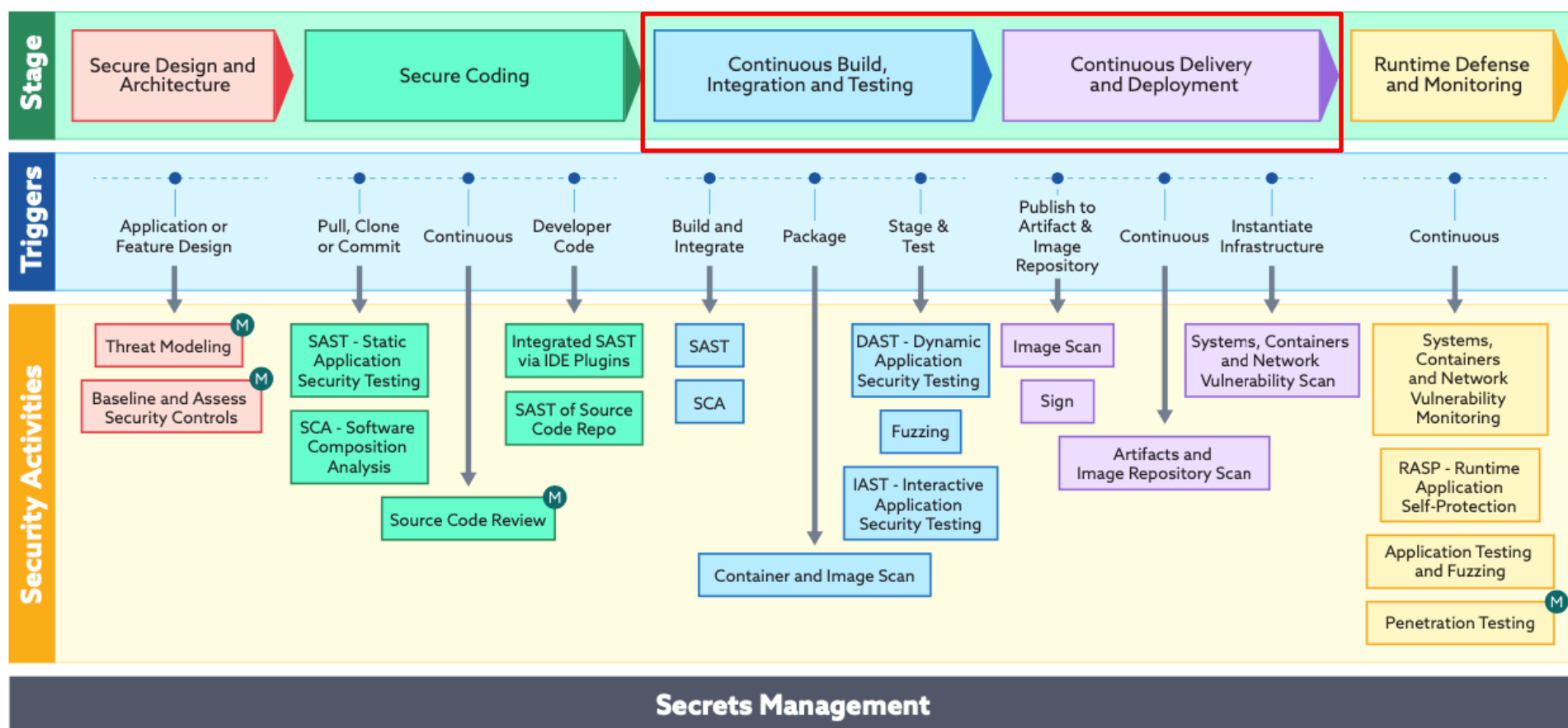


WHAT IS DEVOPS & DEVSECOPS?



Conclusions

Secure Development Lifecycle - Policies, Standards, Controls and Best Practices



WHAT IS DEVOPS & DEVSECOPS?



Conclusions

A screenshot of the Google Cloud Container Registry 'Settings' page. The left sidebar shows a navigation menu with 'Container Registry', 'Images', and 'Settings' (highlighted). The main content area has a header 'Settings' and a warning message: 'Container Registry is deprecated. After May 15, 2024, Artifact Registry will host images'. Below this is a section titled 'Vulnerability scanning' with a paragraph explaining the service and a 'Learn more' link. At the bottom, it shows 'Scanning: On' with a green checkmark and a 'DISABLE' button.

Google Cloud edemdevsecops Search (/) for resources, docs, products, a

Container Registry

Images

Settings

Settings

i Container Registry is deprecated. After May 15, 2024, Artifact Registry will host images

Vulnerability scanning

Vulnerability scanning automatically scans images when they are pushed to the registry for known security vulnerabilities and exposures. As new vulnerabilities are discovered, it checks if they affect images that are in Container Registry or Artifact Registry. Scanning is provided by the [Container Scanning API](#) and coverage is currently limited to Alpine, CentOS, Debian, RedHat, and Ubuntu based images. [Learn more](#)

✓ Scanning: On

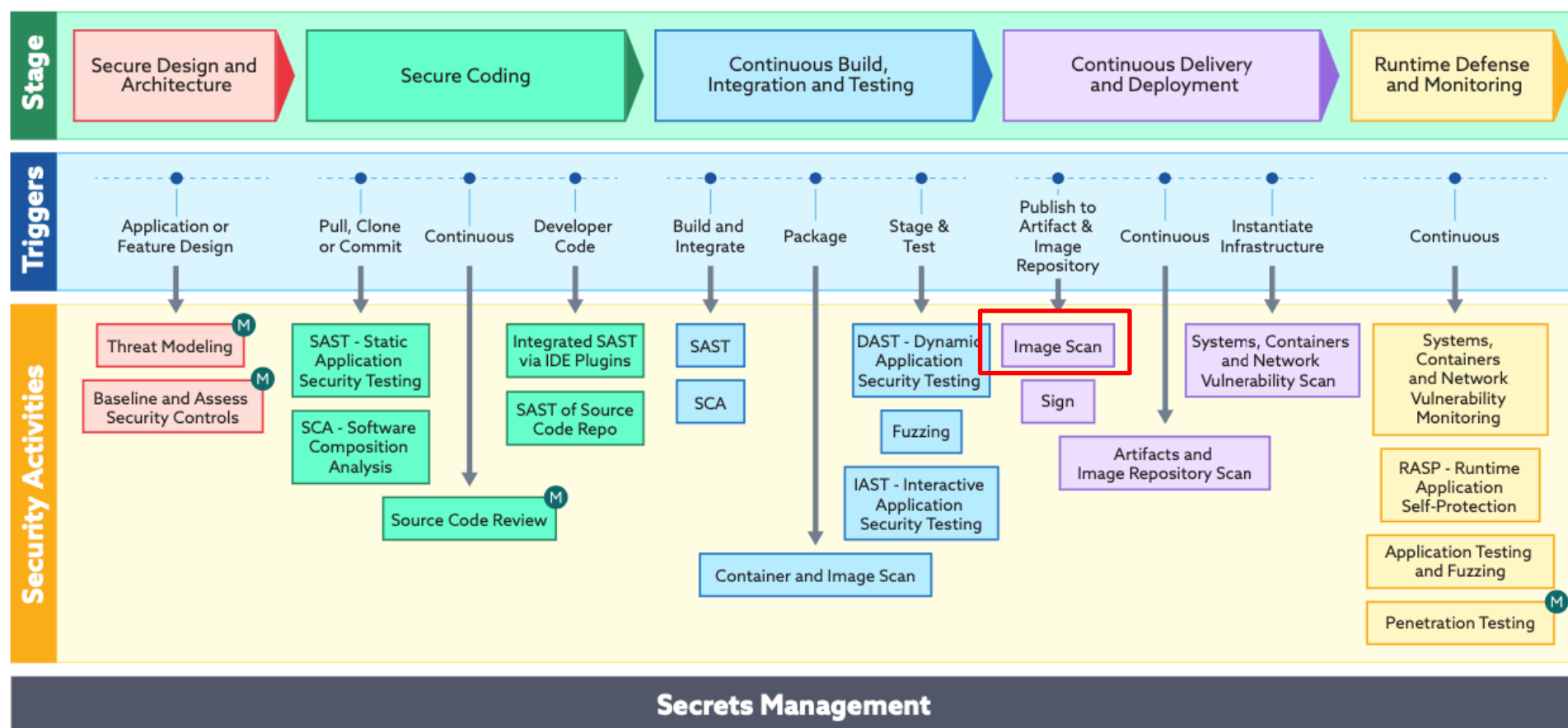
DISABLE

WHAT IS DEVOPS & DEVSECOPS?



Conclusions

Secure Development Lifecycle - Policies, Standards, Controls and Best Practices

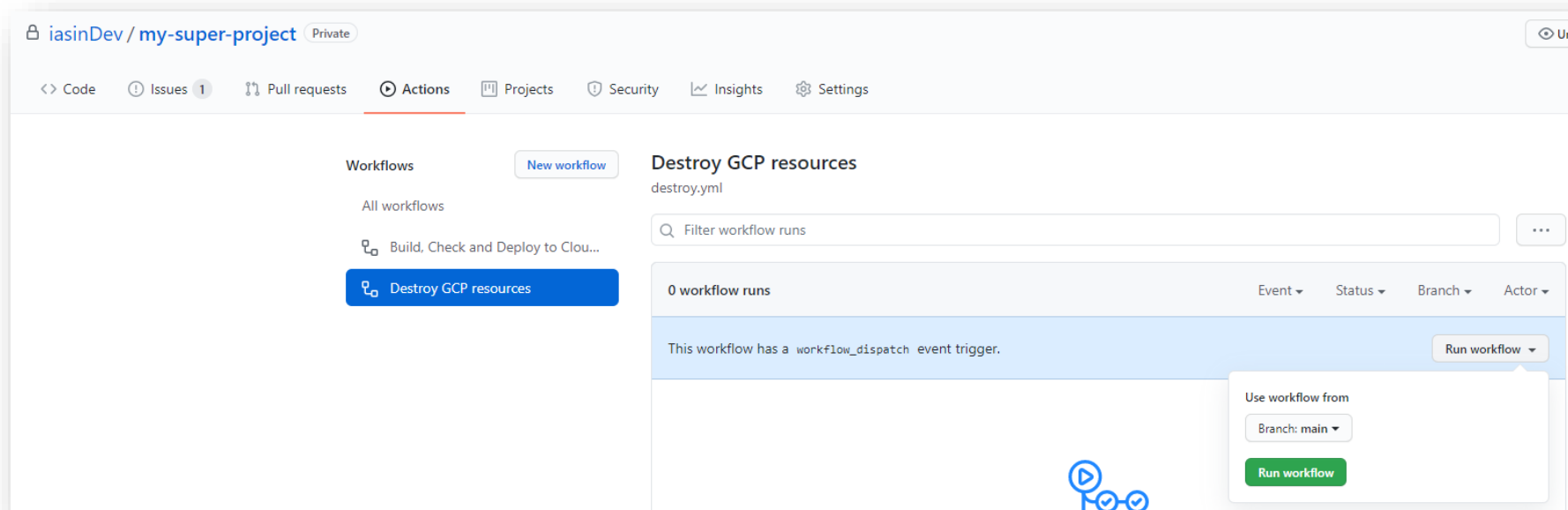


WHAT IS DEVOPS & DEVSECOPS?



Destroy All

Manually launch the destroy pipeline



WHAT IS DEVOPS & DEVSECOPS?



Destroy All

Manually launch the destroy pipeline

The screenshot shows the GitHub Actions interface for a repository named 'iasinDev / my-super-project'. The 'Actions' tab is selected, displaying a workflow run titled 'Destroy GCP resources Destroy GCP resources #1'. The run is marked as successful with a green checkmark. A summary table provides details about the run, including its manual trigger, status, duration, and billable time. Below the summary, the 'Jobs' section lists a single job named 'destroy-terraform-resources', which is also successful. The workflow file 'destroy.yml' is shown as being triggered by a 'workflow_dispatch' event. A detailed view of the 'destroy-terraform-resources' job shows its successful completion with a duration of 16 seconds.

iasinDev / my-super-project Private

<> Code ⓘ Issues 1 🔗 Pull requests ⌚ Actions 📁 Projects ⓘ Security 📈 Insights ⚙️ Settings

✓ Destroy GCP resources Destroy GCP resources #1

Summary

Manually triggered 38 seconds ago	Status	Total duration	Billable time	Artifacts
iasinDev d6cbc60	Success	35s	16s	—

Jobs

- ✓ destroy-terraform-resources

destroy.yml
on: workflow_dispatch

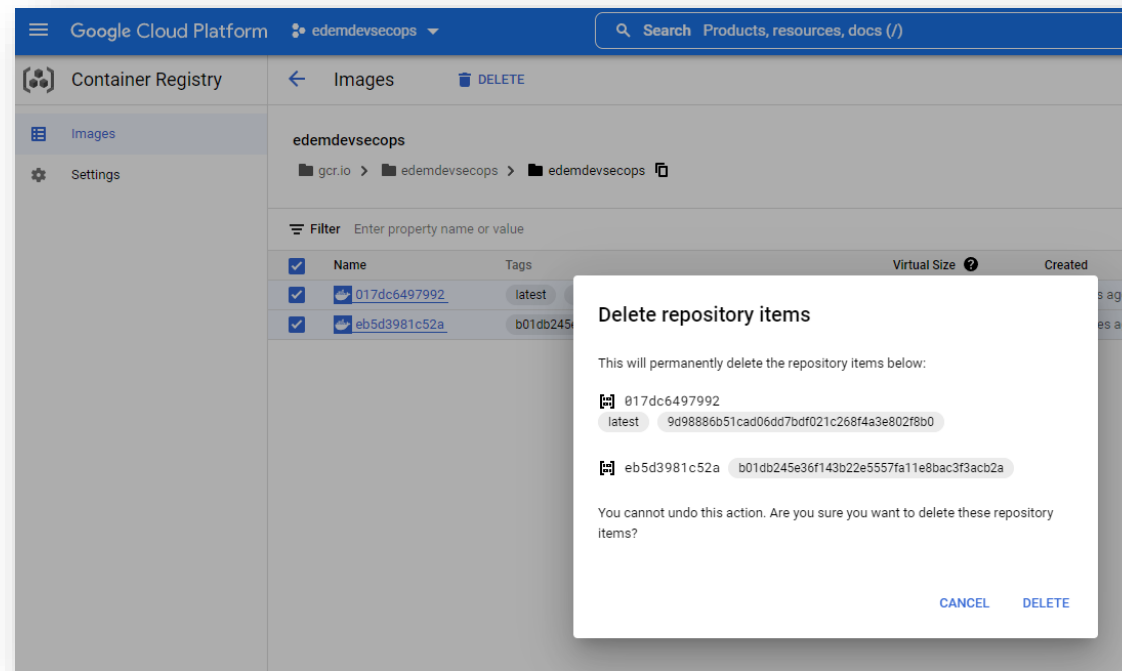
✓ destroy-terraform-resources 16s

WHAT IS DEVOPS & DEVSECOPS?



Destroy All

Delete all Container Registry images

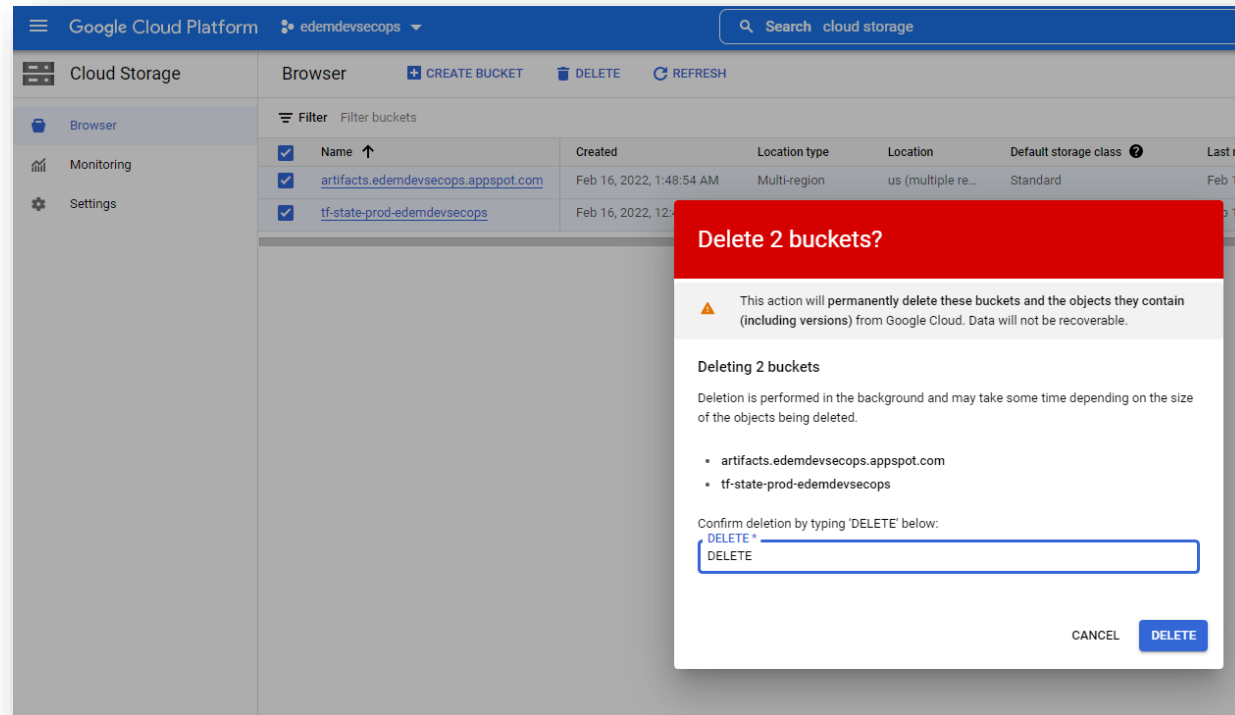


WHAT IS DEVOPS & DEVSECOPS?



Destroy All

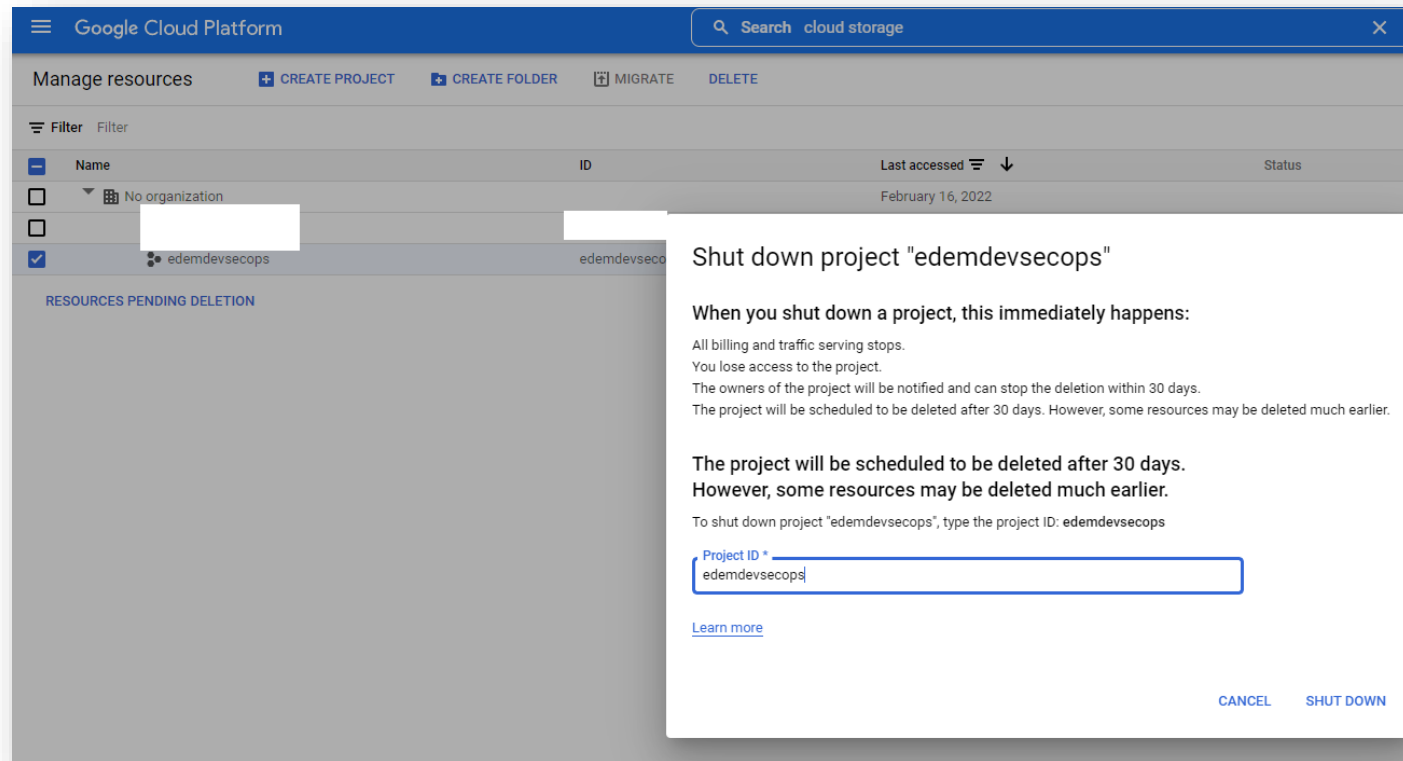
Delete the buckets created



WHAT IS DEVOPS & DEVSECOPS?

Destroy All

Delete the GCP project in [resource manager](#)



WHAT IS DEVOPS & DEVSECOPS?



Destroy All

Delete the GitHub Project

Are you absolutely sure?

×

Unexpected bad things will happen if you don't read this!

This action **cannot** be undone. This will permanently delete the **iasinDev/my-super-project** repository, wiki, issues, comments, packages, secrets, workflow runs, and remove all collaborator associations.

This will not change your billing plan. If you want to downgrade, you can do so in your Billing Settings.

Please type **iasinDev/my-super-project** to confirm.

iasinDev/my-super-project

I understand the consequences, delete this repository

AGENDA

QUESTIONS??

THANKS!!

