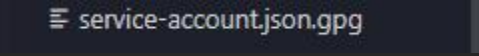


05.Github Actions Secret, Repo secret

- Server klasör ağacı



service-account.json.gpg

- GCP' den Service Account oluşturma.
- Git üzerinde encrypt etme.
- Repo secret'ına PASSPHRASE secret ekleme
- Docker hub girişi için username ve password secret ekleme

05.Github Actions Secret, Repo secret

- console.cloud.google.com/
- iam-admin/serviceaccount
- Create Service Account
- Select a Role / Kubernetes Engine Admin

The screenshot shows the Google Cloud IAM console for project "multi-k8s". The page title is "Service accounts" with a search bar containing "domain". The left sidebar shows the navigation menu with "Service accounts" selected. The main content area displays "Service accounts for project 'multi-k8s'" and provides information about service accounts and organization policies. Below this is a table of service accounts.

Email	Status	Name	Description	Key ID	Key creation date	OAuth 2 Client ID	Actions
217276651507-compute@developer.gserviceaccount.com	Enabled	Compute Engine default service account		No keys		118387595549830752232	⋮
deployment@multi-k8s-445712.iam.gserviceaccount.com	Enabled	deployment		0434674fdc0dd0410bba4bee64b69e9678a89aee	Dec 27, 2024	107590117945499756551	⋮

05.Github Actions Secret, Repo secret

- Manage keys/Create new key/JSON

Google Cloud multi-k8s domain

Service accounts + CREATE SERVICE ACCOUNT DELETE MANAGE ACCESS REFRESH

Service accounts for project "multi-k8s"

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. [Learn more about service accounts.](#)

Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload, or the creation of service accounts entirely. [Learn more about service account organization policies.](#)

Filter Enter property name or value

<input type="checkbox"/>	Email	Status	Name ↑	Description	Key ID	Key creation date	OAuth 2 Client ID ?	Actions
<input type="checkbox"/>	217276651507-compute@developer.gserviceaccount.com	Enabled	Compute Engine default service account		No keys		118387595549830752232	⋮
<input type="checkbox"/>	deployment@multi-k8s-445712.iam.gserviceaccount.com	Enabled	deployment		0434674fdc0dd0410bba4bee64b69e9678a89aee	Dec 27, 2024	107590117945499756551	⋮

- Manage details
- Manage permissions
- Manage keys
- View metrics
- View logs
- Disable
- Delete

05.Github Actions Secret, Repo secret

- Manage keys/Create new key/JSON

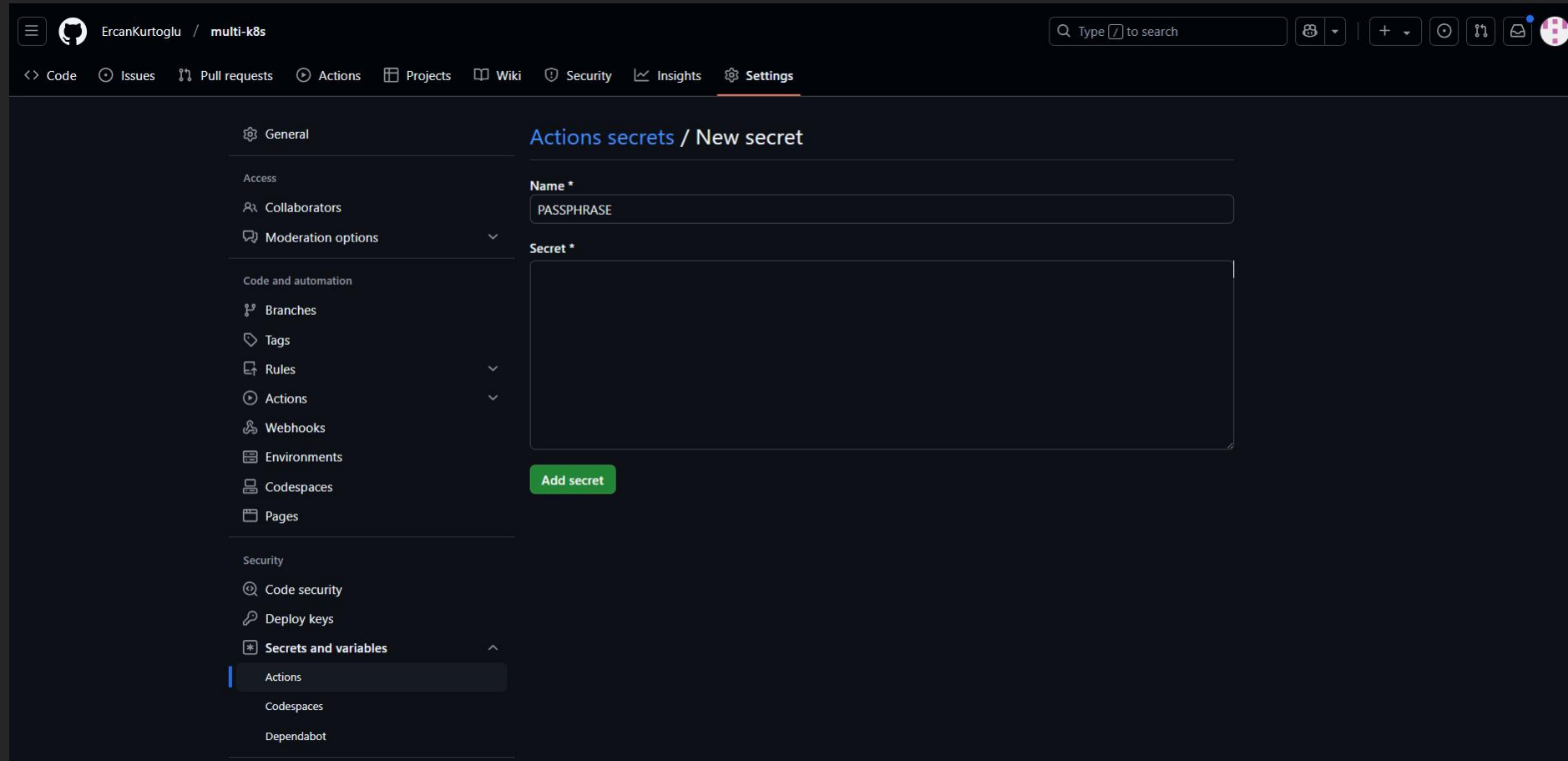
```
gpg --symetric --cipher-algo AES256 service-account.json
```

```
≡ service-account.json.gpg
```

- İndirilen json dosyası gpg komutuyla encrypt edilir.
- gpg kodu bir Passphase şifresi girilmesini ister. Girilecek bu şifre Github repo secrets bölümüne de eklenmelidir
- Encrypt edilmiş dosya uzantısı '.gpg' olur.

05.Github Actions Secret, Repo secret

- <https://github.com/ErcanKurtoglu/multi-k8s/settings/secrets/actions>



05.Github Actions Secret, Repo secret - all secrets

The screenshot shows the GitHub repository settings page for 'Actions secrets and variables'. The left sidebar contains navigation links for General, Access, Collaborators, Moderation options, Code and automation (Branches, Tags, Rules, Actions, Webhooks, Environments, Codespaces, Pages), Security (Code security, Deploy keys, Secrets and variables, Actions, Codespaces, Dependabot), and Integrations (GitHub Apps, Email notifications). The 'Secrets and variables' link is highlighted. The main content area is titled 'Actions secrets and variables' and includes a description of secrets and variables, a warning about collaborator access, and tabs for 'Secrets' and 'Variables'. Below this is the 'Environment secrets' section, which is currently empty. At the bottom is the 'Repository secrets' section, which contains a table of existing secrets.

Actions secrets and variables

Secrets and variables allow you to manage reusable configuration data. Secrets are **encrypted** and are used for sensitive data. [Learn more about encrypted secrets](#). Variables are shown as plain text and are used for **non-sensitive** data. [Learn more about variables](#).

Anyone with collaborator access to this repository can use these secrets and variables for actions. They are not passed to workflows that are triggered by a pull request from a fork.

Environment secrets

This environment has no secrets.

[Manage environment secrets](#)

Repository secrets

[New repository secret](#)

Name	Last updated		
DOCKER_PASSWORD	last week	Edit	Delete
DOCKER_USERNAME	last week	Edit	Delete
PASSPHRASE	last week	Edit	Delete

05.Github Actions Secret, Repo secret

- Decryption json file

```
deploy:
  name: Deploy to GKE
  runs-on: ubuntu-latest
  needs: build

  steps:
    - name: Checkout code
      uses: actions/checkout@v4

    - name: Decrypt service account key
      run: gpg --quiet --batch --yes --decrypt --passphrase="${{ secrets.PASSPHRASE }}" --output service-account.json service-account.json.gpg

    - name: Authenticate to Google Cloud
      run: gcloud auth activate-service-account --key-file=service-account.json
```