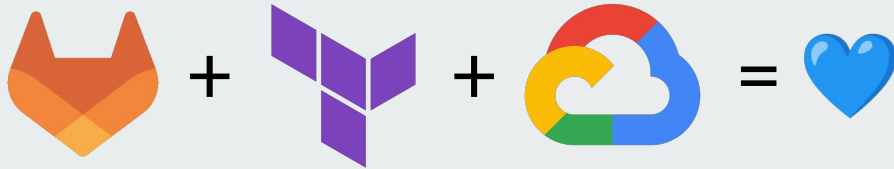

Self-Service infrastructure pour GCP avec Terraform et Gitlab



Salut 🖐️

Moi c'est Julien



Freelance @CodeKaio

Associé @Ekité

Teacher @univ-lille





**Vêtements, Chaussures,
Accessoires**



Mode à Petits Prix





Move to cloud - top départ en juin 2021

0

c'est de là où on part

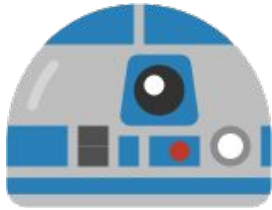
70

applications spécifiques à migrer

100

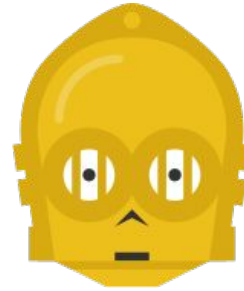
développeurs à accompagner

Des objectifs #DevOps



R2 - Développeur

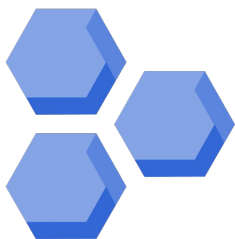
“Je veux être autonome sur la création des mes environnements”
“ça doit aller plus vite que le processus de tickets existant”



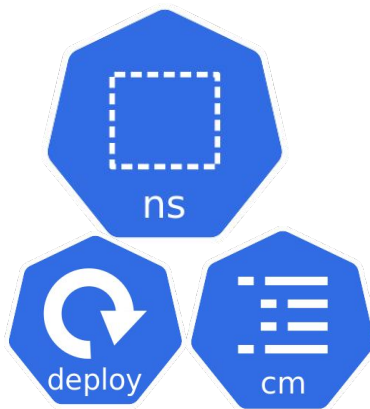
C3 - Opérateur

“Je veux m’assurer du respect des bonnes pratiques, nommage, sécurité, backup”

Une application / environnement



un projet GCP



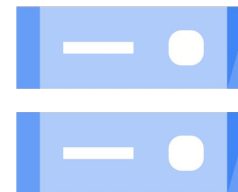
un namespace
kubernetes



une BDD

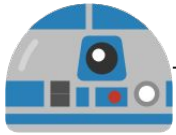


d'autres services



des buckets

En Infrastructure As Code

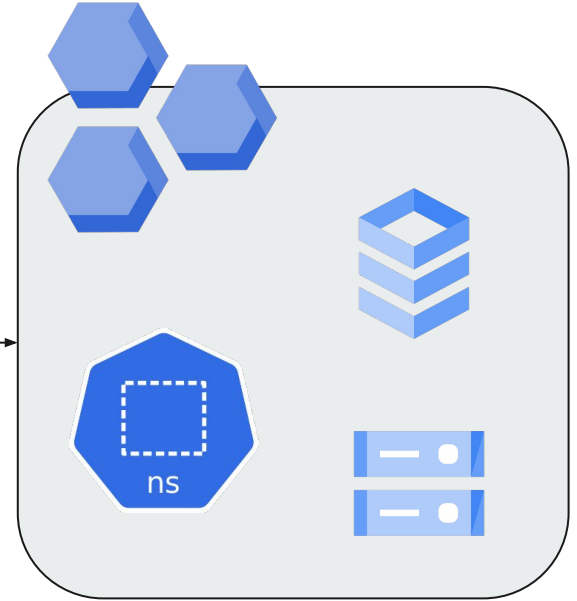


un repo gitlab +
pipeline

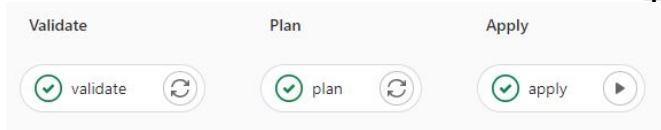


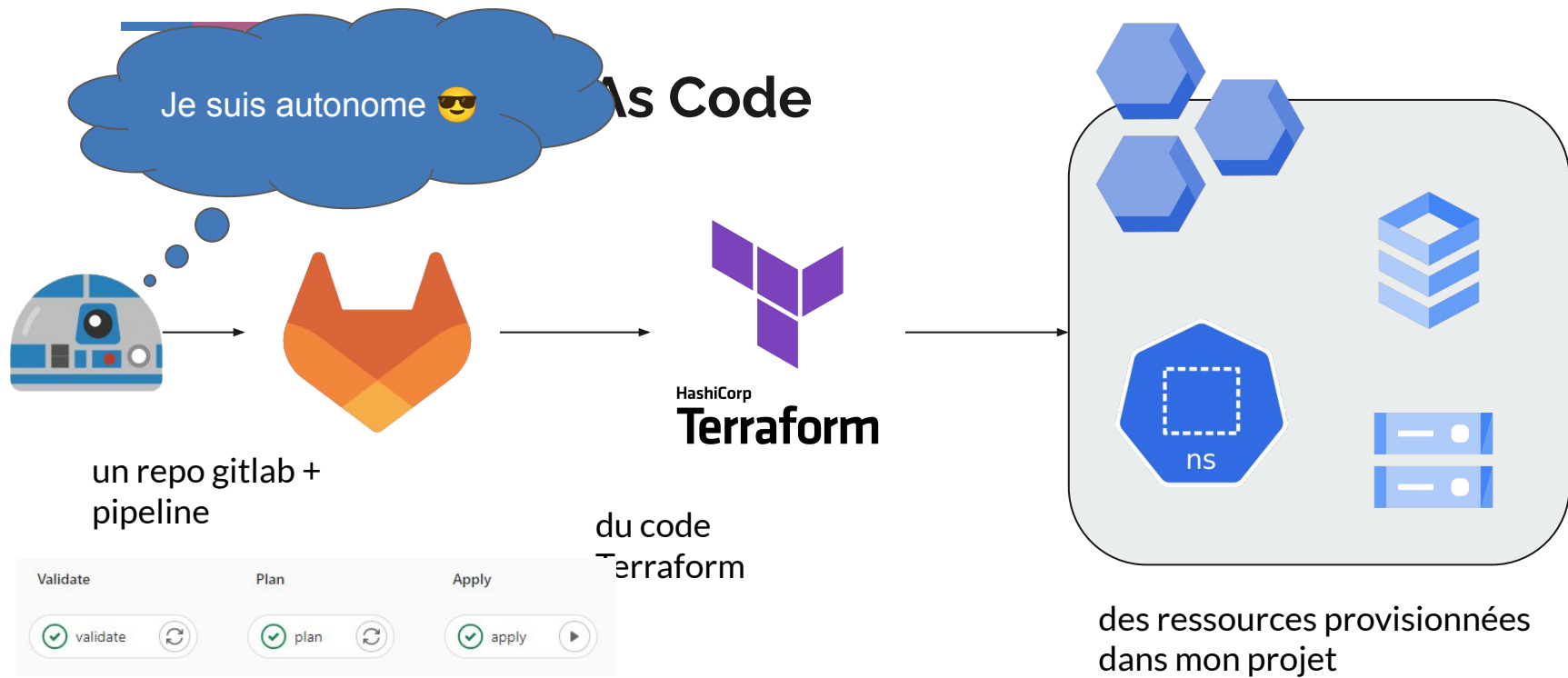
HashiCorp
Terraform

du code
Terraform



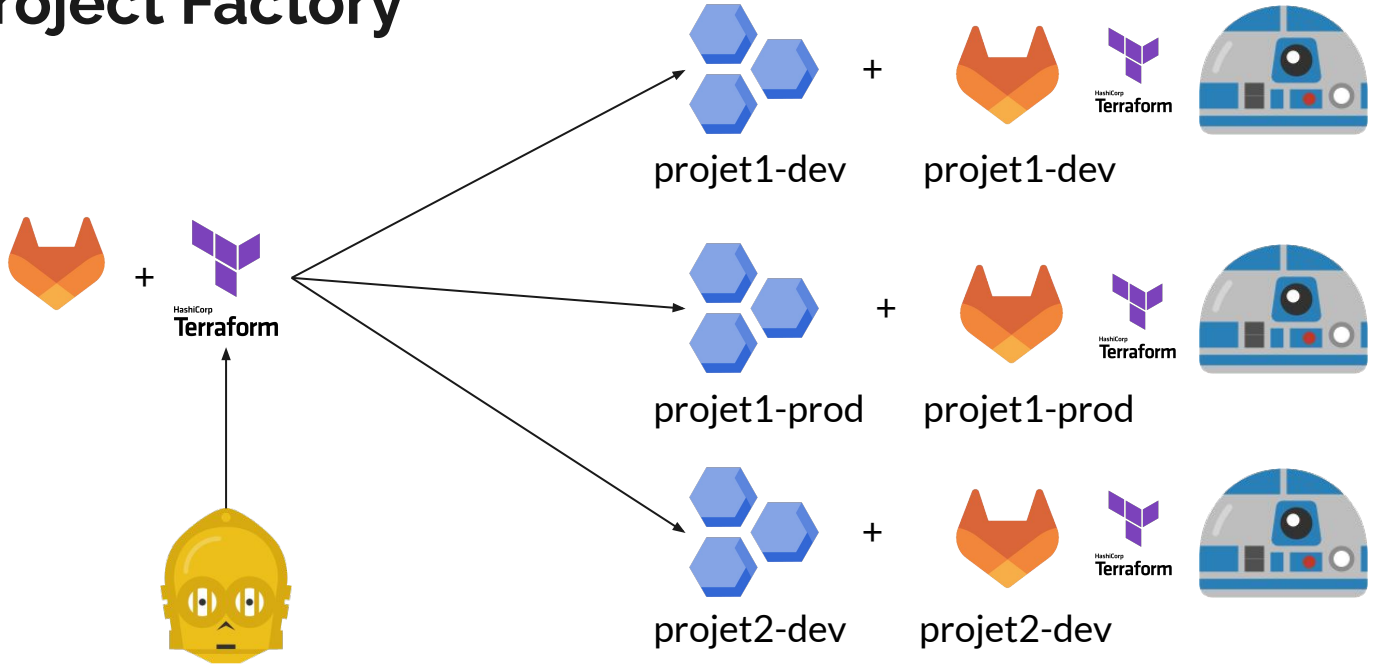
des ressources provisionnées
dans mon projet



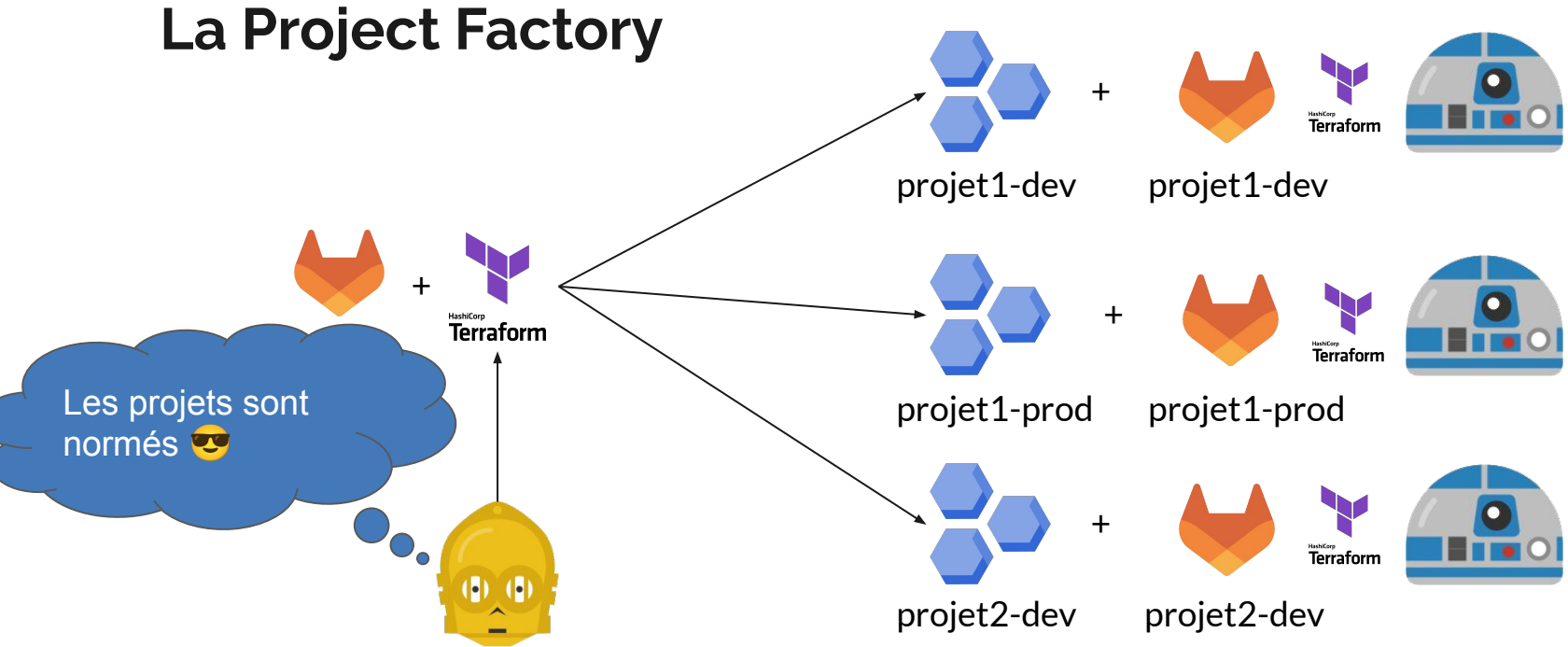


Comment construire ces projets Gitlab + GCP ?

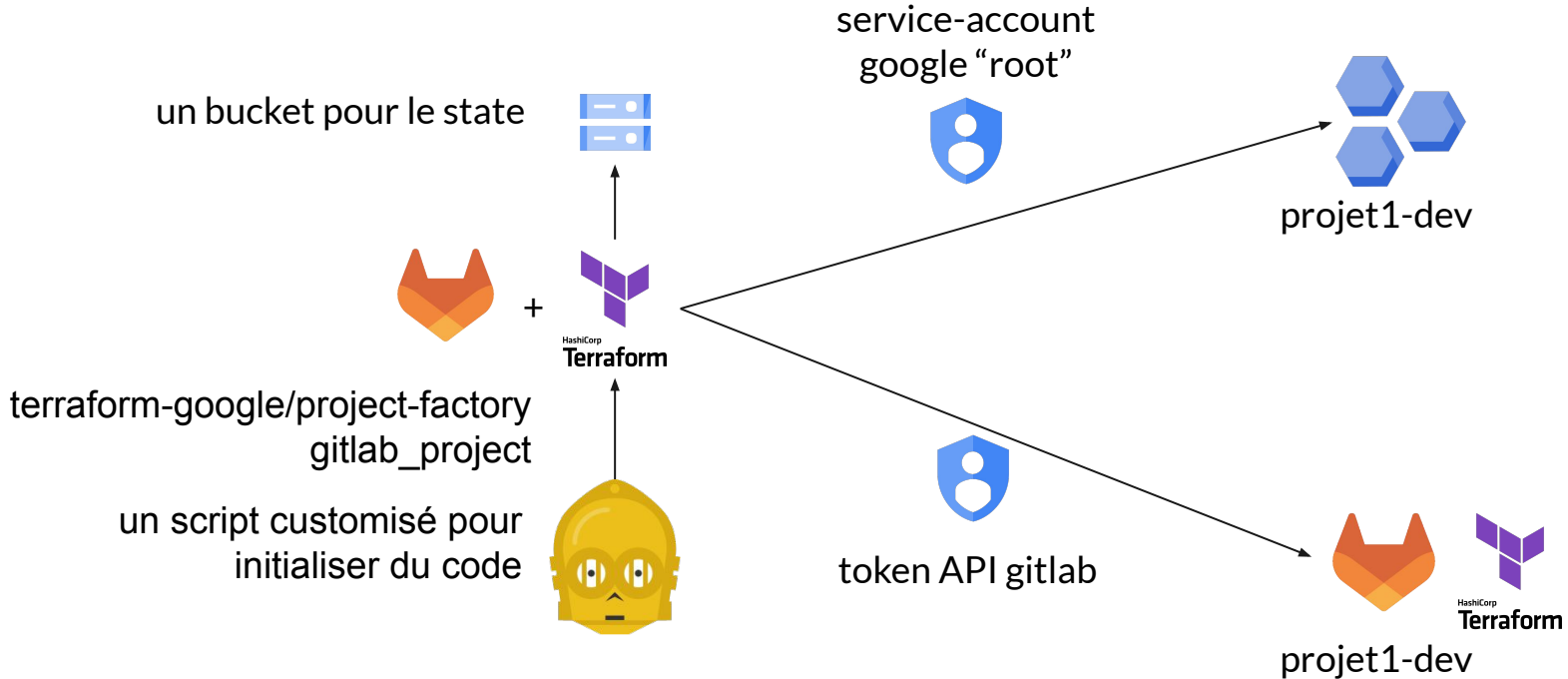
La Project Factory



La Project Factory



La Project Factory





Le service-account “root” de la project-factory (pas Terraformé, une sombre histoire d’🥚 et de 🐔)

project-factory@codekaio-seed-project.iam.gserviceaccount.com

project-factory

Billing Account User

Billing Account Viewer

Compute Network Admin

Compute Shared VPC Admin

Folder IAM Admin

Organization Viewer

Project Creator

Project IAM Admin

Security Admin

Service Account Admin

Service Account Key Admin



Un service account

Project Creator
Project IAM Admin
Folder Admin

Le bucket pour le state Terraform de la project-factory (pas Terraformé, une sombre histoire d'🥚 et de 🐔)

project-factory-terraform-state


Location	Storage class	Public access	Protection
eu (multiple regions in European Union)	Standard	Subject to object ACLs	None

[OBJECTS](#) [CONFIGURATION](#) [PERMISSIONS](#) [PROTECTION](#) [LIFECYCLE](#)

Buckets > project-factory-terraform-state 🗄















[UPLOAD FILES](#) [UPLOAD FOLDER](#) [CREATE FOLDER](#) [MANAGE HOLDS](#) [DOWNLOAD](#) [DELETE](#)

Filter by name prefix only ▾  **Filter** Filter objects and folders

<input type="checkbox"/>	Name	Size	Type	Created 	Storage class
<input type="checkbox"/>	📁 terraform/	—	Folder	—	—

Le code de la project factory

<https://gitlab.com/codekaio/devfest-2022/gcp-project-factory>

Name	Last commit	Last update
import-gitlab-project	 : add project-template loading code	1 day ago
project	 : correct GOOGLE_PROJECT variable	1 day ago
 .gitlab-ci.yml	 : correct before_script	1 day ago
 backend.tf	 : add backend.tf	1 week ago
 main.tf	 : create gitlab project	4 days ago
 outputs.tf	 : add outputs	4 days ago
 projets.auto.tfvars	 : add auto variables	1 week ago
 variables.tf	 : add main module code	1 week ago



gcp-project-factory

codekaio/devfest-2022/gcp-project-factory



main



Edit



import-gitlab-project



project

gcp-project.tf

gitlab-project.tf

outputs.tf

providers.tf

variables.tf

.gitlab-ci.yml

backend.tf

main.tf

outputs.tf

projets.auto.tfvars

variables.tf

gcp-project.tf

```
1 module "gcp-project" {
2   source = "terraform-google-modules/project-factory/google"
3   version = "~> 13.0"
4
5   name = var.project_name
6
7   org_id          = "xxxx-xxx"
8   billing_account = "xxxx-xxx-xxx-xxxx"
9
10  activate_apis = [
11    "compute.googleapis.com",
12    "storage-component.googleapis.com",
13    "pubsub.googleapis.com",
14  ]
15 }
16
```




gcp-project-factory

codekaio/devfest-2022/gcp-project-factory



main



import-gitlab-project



project

gcp-project.tf

gitlab-project.tf

outputs.tf

providers.tf

variables.tf

.gitlab-ci.yml

backend.tf

main.tf

outputs.tf

projets.auto.tfvars

variables.tf

gitlab-project.tf

```
1 data "gitlab_group" "group" {
2   full_path = "codekaio/devfest-2022"
3 }
4
5 resource "gitlab_project" "this" {
6   name                = var.project_name
7   visibility_level    = "private"
8   namespace_id       = data.gitlab_group.group.id
9   shared_runners_enabled = true
10 }
11
```







La conf du pipeline de la project-factory

Variables

Variables store information, like passwords and secret keys, that you can use in job scripts. [Learn more.](#)

Variables can be:

- **Protected:** Only exposed to protected branches or protected tags.
- **Masked:** Hidden in job logs. Must match masking requirements. [Learn more.](#)

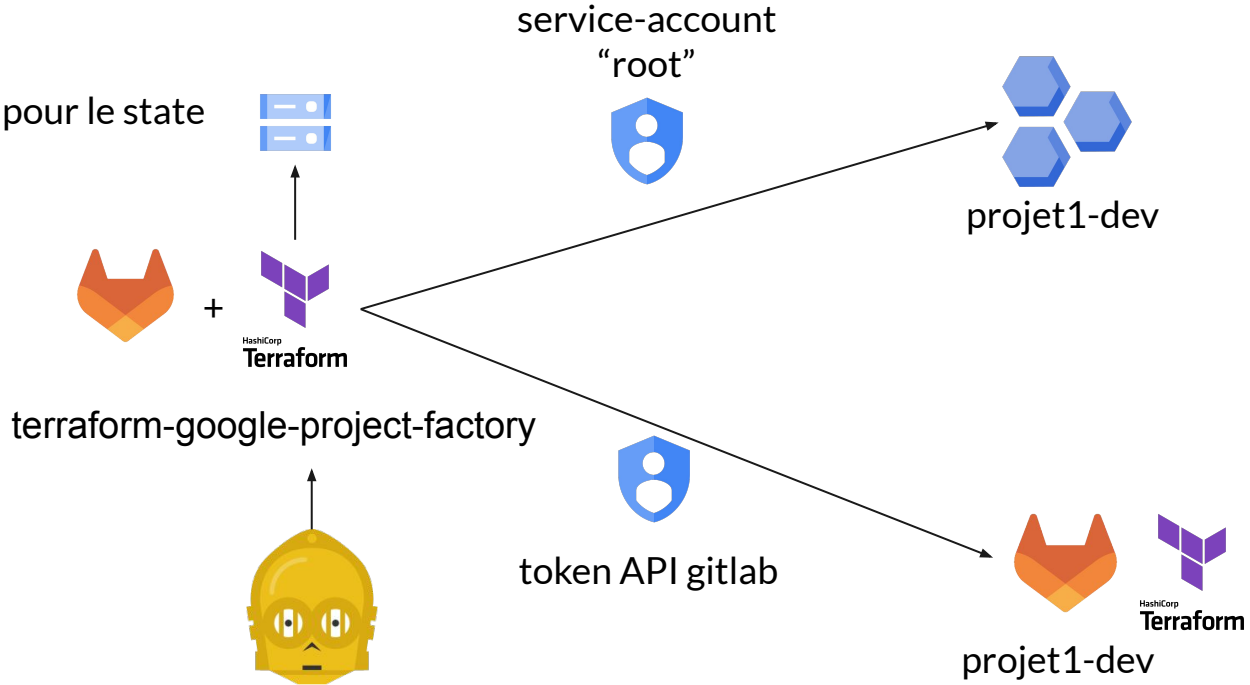
Type	↑ Key	Value	Protected	Masked	Environments	
Variable	GITLAB_TOKEN 	***** 	✓	✗	All (default)	
File	GOOGLE_APPLICATION_CREDENTIALS 	***** 	✓	✗	All (default)	

Add variable

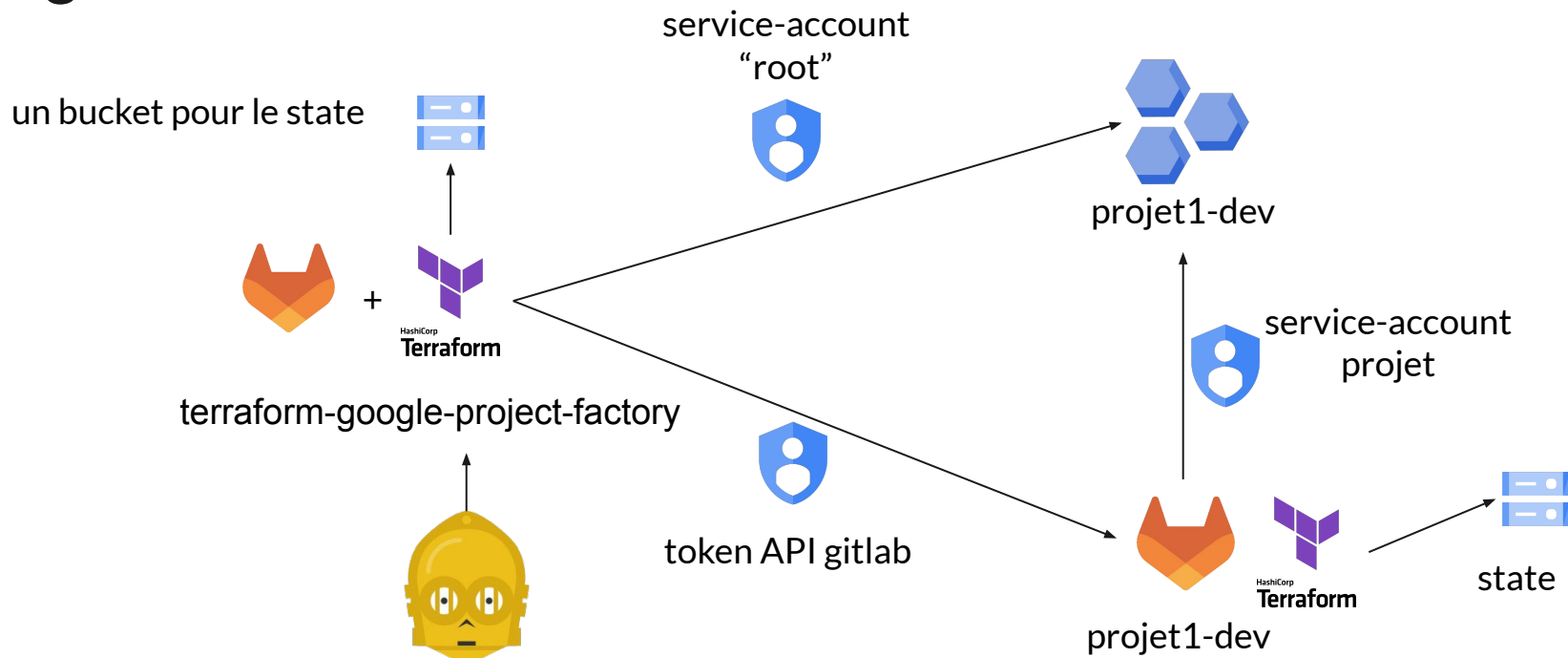
Reveal values

La Project Factory

un bucket pour le state



La "glue"





</> main

Edit

import-gitlab-project

project

gcp-project.tf

gitlab-project.tf

outputs.tf

providers.tf

variables.tf

.gitlab-ci.yml

backend.tf

main.tf

outputs.tf

projects.auto.tfvars

variables.tf

```
1  locals {
2    roles = [
3      "roles/storage.admin",
4      "roles/resourcemanager.projectIamAdmin"
5    ]
6  }
7
8  module "gcp-project" {
9    source = "terraform-google-modules/project-factory/google"
10   version = "~> 13.0"
11
12   name = var.project_name
13
14   org_id           = "xxxx-xxx"
15   billing_account = "xxxx-xxx-xxx-xxxx"
16
17   activate_apis = [
18     "compute.googleapis.com",
19     "storage-component.googleapis.com",
20     "pubsub.googleapis.com",
21   ]
22
23   bucket_name     = "terraform-state-${var.project_name}"
24   bucket_project = var.project_name
25   bucket_location = "eu"
26
27   project_sa_name = "terraform"
28 }
29
30 resource "google_project_iam_member" "terraform_service_account_roles" {
31   for_each = toset(local.roles)
32
33   project = module.gcp-project.project_id
34   role    = each.value
35   member  = "serviceAccount:${module.gcp-project.service_account_email}"
36 }
```

création d'un bucket "state"

création d'un service account + roles

gcp-project-factory
codekaio/devfest-2022/gcp-project-factory

main

Edit

- import-gitlab-project
- project
 - gcp-project.tf
 - gitlab-project.tf**
 - outputs.tf
 - providers.tf
 - variables.tf
- .gitlab-ci.yml
- backend.tf
- main.tf
- outputs.tf
- projets.auto.tfvars
- variables.tf

```
1 data "gitlab_group" "group" {
2   full_path = "codekaio/devfest-2022"
3 }
4
5 resource "gitlab_project" "this" {
6   name           = var.project_name
7   visibility_level = "private"
8   namespace_id   = data.gitlab_group.group.id
9   shared_runners_enabled = true
10 }
11
12 resource "google_service_account_key" "key" {
13   service_account_id = module.gcp-project.service_account_email
14 }
15
16 resource "gitlab_project_variable" "ci_variable" {
17   project = gitlab_project.this.id
18   key     = "GOOGLE_CREDENTIALS"
19   value   = base64decode(google_service_account_key.key.private_key)
20   variable_type = "file"
21 }
22
23 resource "gitlab_project_variable" "google_project_variable" {
24   project = gitlab_project.this.id
25   key     = "GOOGLE_PROJECT"
26   value   = module.gcp-project.project_id
27 }
28
```

extraction d'une clé du service account "terraform" créé par le module

injection de la clé en variable de Gitlab CI

Démo ?



DevFest 2022 - 888.25

https://github.com/codecademy/devfest2022


Menu

Search GitHub

DevFest 2022

- Subgroup information
- Issues
- Merge requests
- Security
- Discussions
- Packages & Registries
- Settings


Columns > DevFest 2022

 **DevFest 2022** Group ID: 58162322 Leave group

New subgroup New project

Subgroups and projects Shared projects Archived projects

Search by name Updated date

-  gcp-project-factory 4 minutes ago

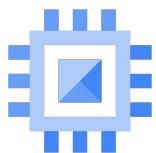
© Collapse sidebar

Le projet créé

The screenshot shows the GitLab interface for a newly created project named "projet-devfest-2022". The left sidebar contains navigation options such as Project information, Repository, Issues, Merge requests, CI/CD, Security & Compliance, Deployments, Packages & Registries, Infrastructure, Monitor, Analytics, Wiki, Snippets, and Settings. The main content area displays the project name, ID (36873012), and statistics: 2 Commits, 1 Branch, 0 Tags, and 23 KB Project Storage. A commit by Julien WITTOUCK is highlighted, with a commit hash of aa5dc6c7. Below the commit, there are buttons for adding project files like README, LICENSE, CHANGELOG, and CONTRIBUTING, as well as options for CI/CD configuration and Kubernetes cluster integration. At the bottom, a table lists the project's files and their commit history.

Name	Last commit	Last update
.gitlab-ci.yml	: init project from template	1 hour ago
backend.tf	: init project from template	1 hour ago
main.tf	: add demo bucket	1 hour ago
outputs.tf	: init project from template	1 hour ago
provider.tf	: init project from template	1 hour ago

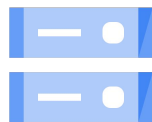
Pour aller encore plus vite et propre : un catalogue de modules fournis par 🤖



VM



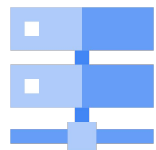
PostgreSQL



Bucket



Dataset



DNS Record



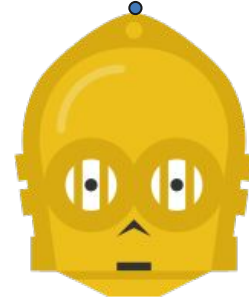
MongoDb



Pub/Sub

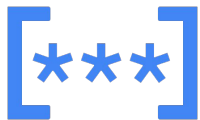


Namespace

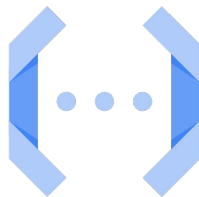




Les modules à venir



Secret



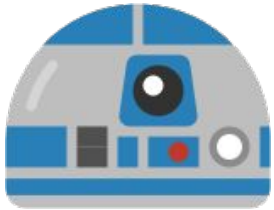
Functions



MemoryStore

C'est qu'on a appris de tout ça

Ce qui fonctionne bien



R2 - Développeur

“C’est rapide,
Mon projet en ~ 15 minutes
Mes premières ressources
en ~ 30 minutes”

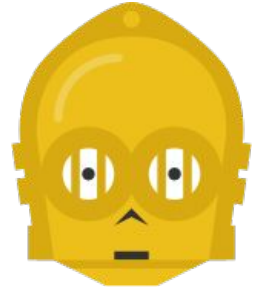
“Le premier projet est difficile, les
autres c’est facile”

~ 115

projets GCP + Gitlab
créés

~ 350

instances de modules



C3 - Opérateur

“Les projets sont créés en
suivant les bonnes
pratiques, sécurité,
backups”

Ce qui reste à améliorer



SOS le state terraform grossit
SOS les pipelines de la project factory de plus en plus longs

→ SOON bascule sur des workspaces plus fins, au projet



SOS des clés de service-account en variables de CI

→ SOON utilisation de workload identity dans nos pipelines pour supprimer les clés



→ SOON politiques sur les plan terraform pour éviter les destroys accidentels

→ SOON mise à jour des modules à systématiser (dependabot)



🙏 Merci ❤️



Les tweets



Le code



Le feedback

$$\text{GitHub} + \text{Vercel} + \text{Google Cloud} = \text{❤️}$$