

Foundation Factory

Übersicht

Die **Foundation Factory** ist eine zentrale Automatisierungsstruktur, die den Aufbau und Betrieb der gesamten Google Cloud Plattform (GCP) Foundation eines Unternehmens sicherstellt. Dabei kommen **Terraform** und **GitOps-Prinzipien** zum Einsatz.

Ziel ist es, eine skalierbare, wartbare und mandantenfähige Struktur aufzubauen, bei der alle GCP-Komponenten - von Organisationsebene bis zu projektspezifischen Ressourcen - **infrastrukturell als Code verwaltet** werden.

Repository-Struktur

1. `<root>-FF-GCP-FOUNDATION-GITOPS`

- **Einziges Repository, das manuell erstellt wird**
- Verwaltet zentral alle nachgelagerten GitOps-Repositories der Foundation.
- Führt Terraform-Code aus, um:
 - GitOps-Repositories für die Foundation zu erstellen (`<root>-ff-gcp-gitops`)
 - GitOps-Repositories für die Project Factorys zu erstellen (`<kunde>-pf-gcp-gitops`)

“ **Hinweis:** `<ROOT>` steht für das zentrale IT Unternehmen.

2. `<root>-FF-GCP-GITOPS`

- Wird vom `ROOT-FF-GCP-FOUNDATION-GITOPS` erstellt
- Verwaltet sämtliche GitOps-Repositories der Google Cloud **Foundation Layer**.

Erstellt folgende Repositories (Können weitere jederzeit ergänzt werden):

Repository Name	Funktion
<kunde>-ff-gcp-billing-alerts	Billing Alerts und Budgets konfigurieren
<kunde>-ff-gcp-vpc-[n]	Virtual Private Clouds (Netzwerkstruktur)
<kunde>-ff-gcp-cloud-identity-groups	Identity-Gruppen & IAM-Berechtigungen
<kunde>-ff-gcp-public-dns	Public DNS Zonen & Records
<kunde>-ff-gcp-organization-hierarchy	Organisationsebenenstruktur (Folder)
<kunde>-ff-gcp-organization-policies	Org Policies (Constraints, Restrictions)
<kunde>-ff-gcp-project-factory	Project Factory Verwaltung für Kundenprojekte
<kunde>-ff-gcp-custom-roles	Definierte benutzerdefinierte IAM Rollen
<kunde>-ff-gcp-fortigate-firewall	Firewall-Regeln (z. B. Third Party Integration)

“ **Berechtigungen auf Organisationsebene** werden **nicht automatisch** über Gitops vergeben und müssen **manuell** erfolgen!

Project Factory

3. <KUNDE> - PF - GCP - GITOPS

- Wird vom Foundation GitOps Repository (<kunde>-ff-gcp-gitops) erstellt
- Erstellt die Service Projects in denen der Gesamte Code des jeweiligen Projektes abgebildet ist (<kunde>-gcp-<project-name>)
- IAM-Service Accounts werden generiert

4. <KUNDE> - PF - GCP - PROJECT - FACTORY

- Terraform-Repository zur eigentlichen Erstellung der GCP-Projekte

Service Projects

5. <KUNDE> - GCP - <PROJECT - NAME>

- **Echte Kundenprojekte**, z. B. SAP-Systeme, Data Lake, etc.
- Enthält Terraform-Code für:
 - Projektinterne Ressourcen
 - Weitere IAM-Konfiguration
 - Speicher, Netzwerk, GKE, etc.

IAM & Berechtigungen

Bereich	Verwaltet durch	Beschreibung
Organisationsebene	Manuell	Wird per Hand vergeben indem man den nötigen Principal einer jeweiligen Gruppe zuweist.
Projekt & Folder IAM	GitOps via Terraform	Wird automatisiert über GitOps-Repos geregelt
Service Accounts	Automatisch erstellt	Durch GitOps-Repositories

GitOps Flow – Zusammenfassung

```
A[<root>-FF-GCP-FOUNDATION-GITOPS] --> B1[<KUNDE>-FF-GCP-GITOPS]
A[<root>-FF-GCP-FOUNDATION-GITOPS] --> B2[<KUNDE>-PF-GCP-GITOPS]
B1 --> C1[Billing, VPC, Identity, Policies...]
B2 --> D1[<KUNDE>-PF-GCP-PROJECT-FACTORY]
B2 --> E1[<KUNDE>-GCP-<PROJECT1>]
B2 --> E2[<KUNDE>-GCP-<PROJECT2>]
```

Vorteile dieser Struktur

- **Modularisierung**: Trennung von Foundation, Project Factory & Kundenprojekten
- **Wiederverwendbarkeit**: Templates können auf beliebige Kunden repliziert werden
- **GitOps-Konformität**: Änderungsverfolgung über GitLab Repos
- **Skalierbarkeit**: Neue Mandanten/Kunden können leicht hinzugefügt werden

- **Sicherheitskonform:** Rollen- und Berechtigungsstruktur zentral steuerbar
-
-

Revision #1

Created 2025-12-27 16:33:22 UTC by Manuel Regli [Owner]

Updated 2025-12-27 16:54:10 UTC by Manuel Regli [Owner]