Herzlich Willkommen!

GFU Cyrus AG

- IT-Architekt und -Berater
- Cloud Engineering mit AWS und GCP
- Softwareentwicklung mit Java und Kotlin
- Studium der Geographie und Informatik in Bonn und Hagen
- Tätig für FUJIFILM, ImmoScout24 und RTL

Dot voting

Sticky stack

So gut kenne ich mich mit dem GCP aus

NEW → PRO

Das sind meine bisherigen Erfahrungen mit Google Cloud Platform

Ich erhoffe mir von dieser Schulung...

Themenübersicht

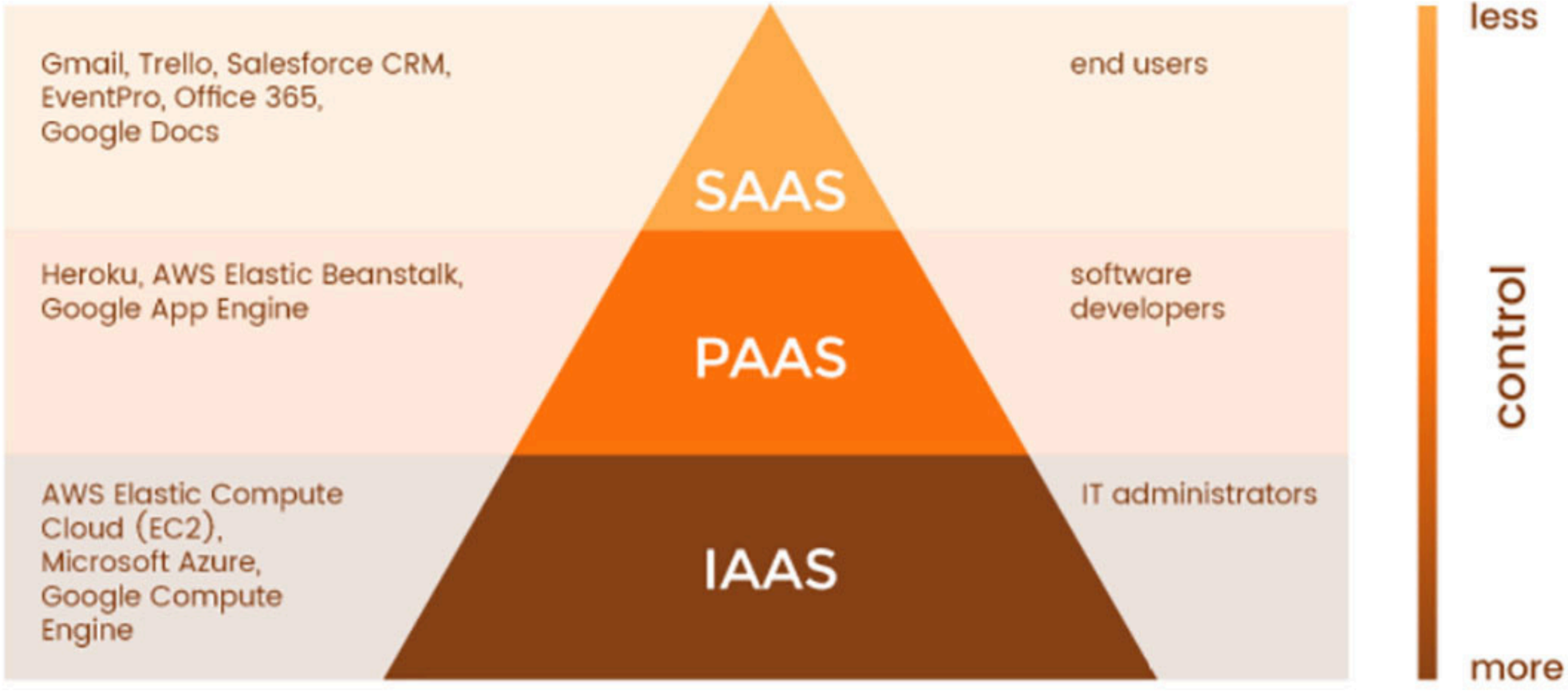
Tag 1

- Übersicht über GCP
- GCP-Konto und -Konsole
- IAM
- Compute
- AppEngine
- Cloud Functions & Run
- Kubernetes Engine
- Cloud Storage
- Cloud SQL

Tag 2

- Firestore
- BigQuery
- Dataproc & Dataflow
- Networking
- Key Management
- Load Balancing & CDN
- Artifact Registry & Build
- AI Services

9:00 – 12:00 & 13:00 – 16:00 (ungefähr)

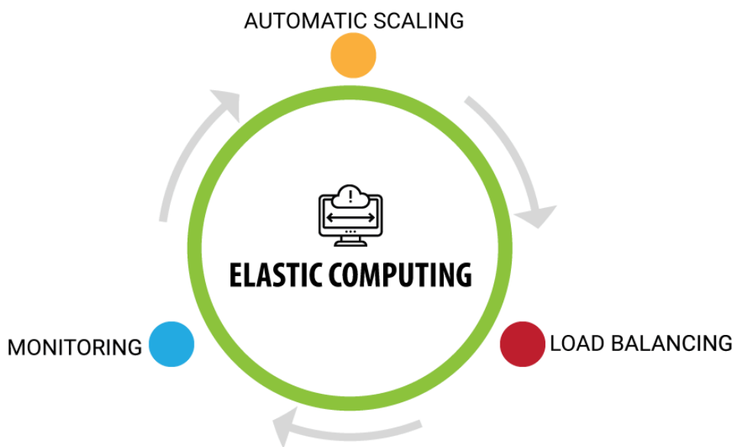


gigacloud.eu

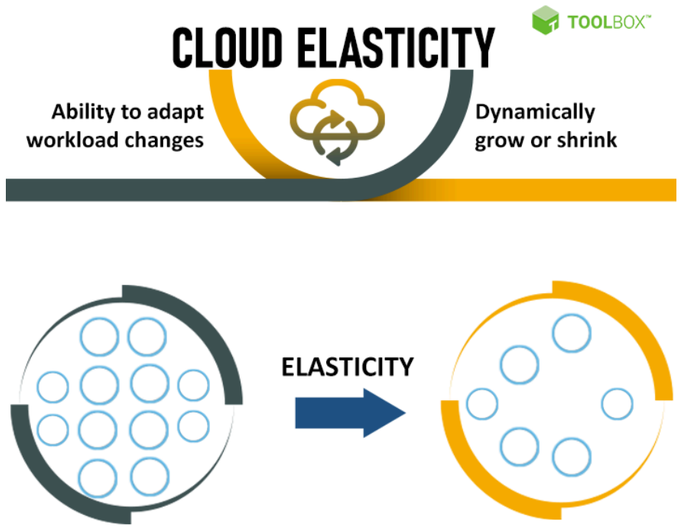
oud pyramid: IaaS, . aaS and SaaS

Explore the foundational concepts of the cloud computing pyramid, including IaaS, PaaS, and SaaS, on GigaCloud Education. Gain insights into these essential cloud service models and their roles in modern IT infrastructure.

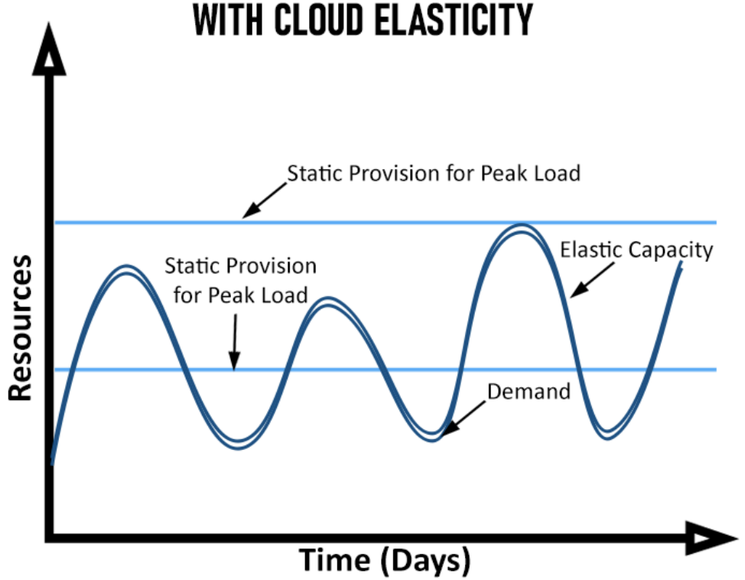
HOW ELASTIC COMPUTING WORKS



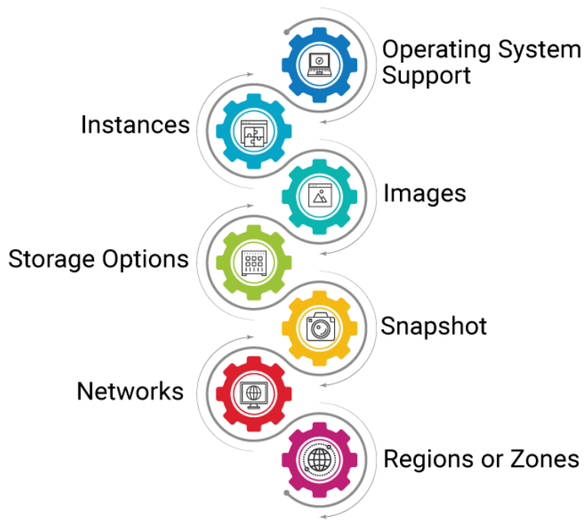
CLOUD ELASTICITY



COMPARISON OF STATIC CAPACITY WITH CLOUD ELASTICITY



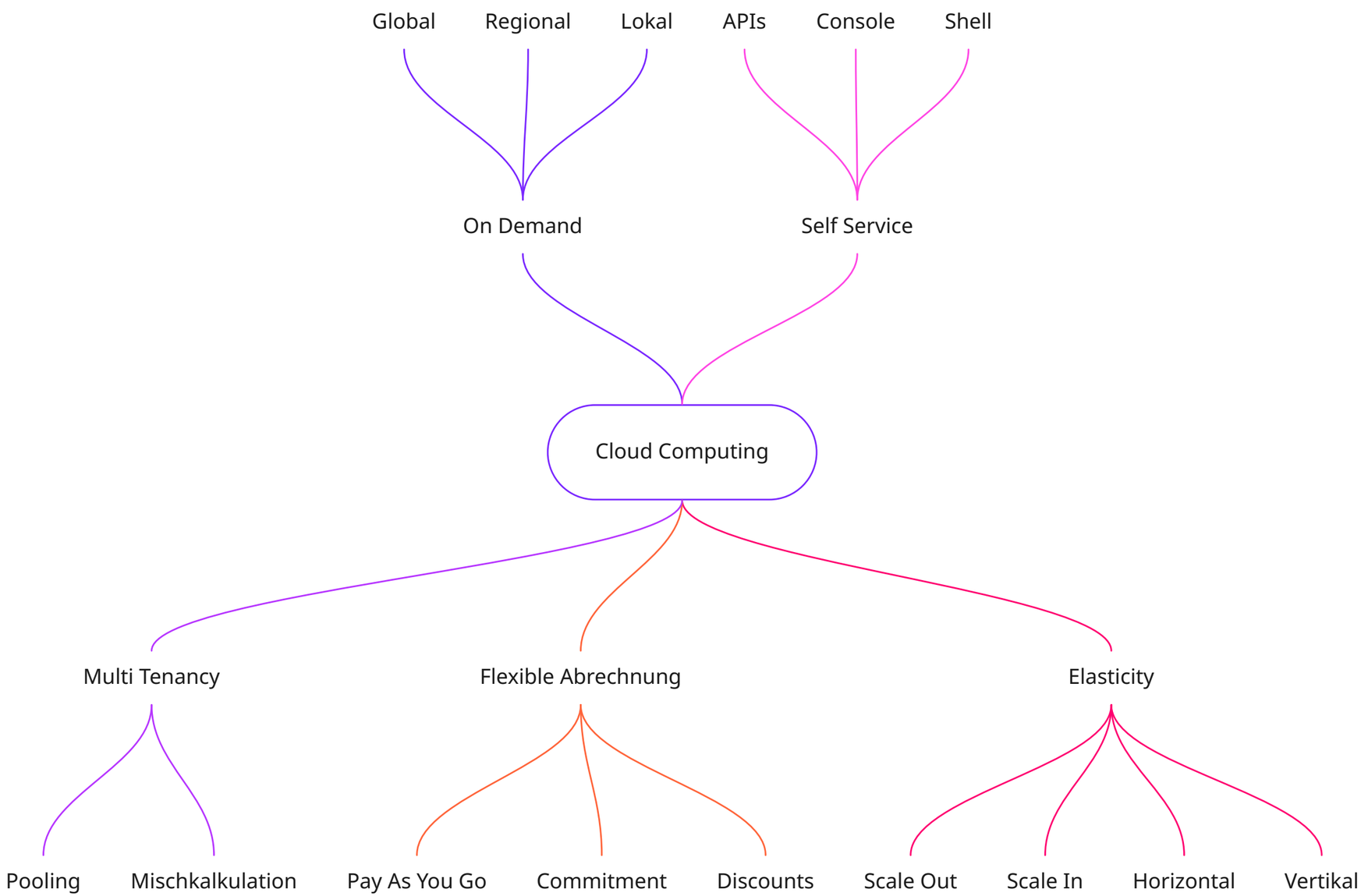
KEY COMPONENTS OF ELASTIC COMPUTING



www.spiceworks.com

What Is Elastic Computing? Definition, Examples, and Best Practices - Spiceworks

Elastic computing is the ability of a system to adapt and manage resources according to workload requirements. Read this article to understand elastic computing in detail.


Global
Regional
Lokal
APIs
Console
Shell
On Demand
Self Service
Cloud Computing
Multi Tenancy
Flexible Abrechnung
Elasticity
Pooling
Mischkalkulation
Pay As You Go
Commitment
Discounts
Scale Out
Scale In
Horizontal
Vertikal

Basics

Google Cloud Platform

- Angekündigt im April 2008
- November 2011 veröffentlicht
- Latecomer
- AWS startete schon 2002 und führte 2006 EC2 ein
- Drittgrößter Public Cloud-Anbieter nach AWS und Azure

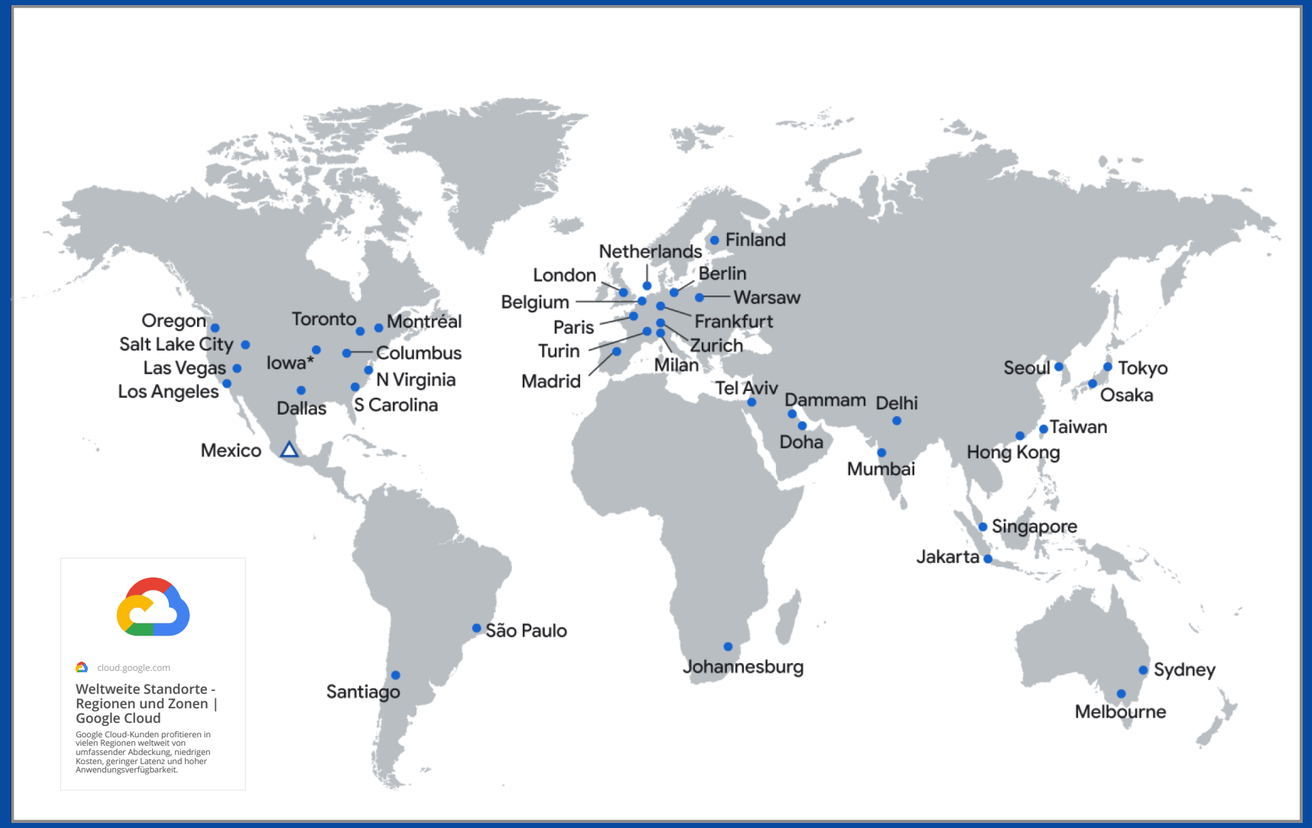
Google Cloud Platform

- Legte zuerst Fokus auf Plattform-Dienste (Paas) wie AppEngine
- Keine direkte Konkurrenz zu den Infrastruktur-Diensten (IaaS) von AWS
- Ging später dann doch auch Richtung IaaS
- Generell starker Fokus auf Container-Technologien (k8s) und Integration anderer Google-Dienste (GMail, Google Analytics, Google Workspace...)

Markt

- Diese Firmen setzen wahrscheinlich aber mehrere Cloud-Provider ein
- Dennoch: GCP ist in vielen Bereichen technologisch führend
    - Container
    - AI
    - AdTech und MarTech
    - PaaS

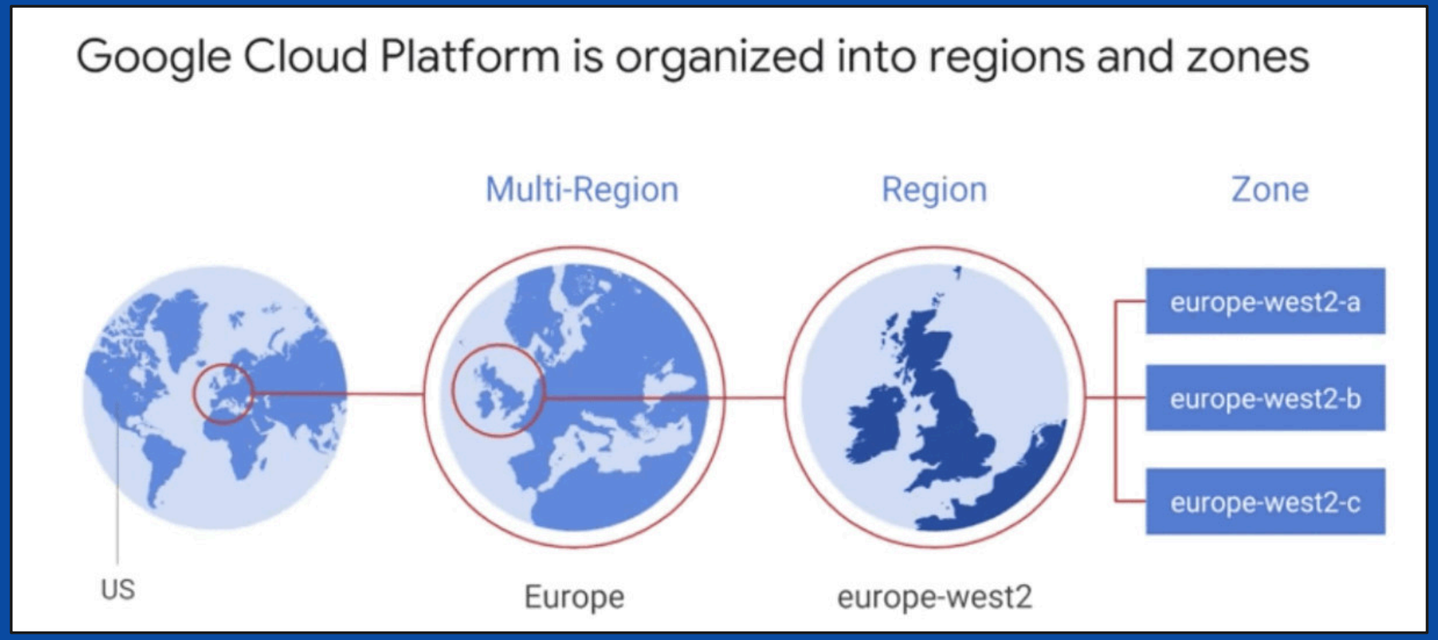
Regionen



- Google nutzt weltweit verteilte Rechenzentren
- Vermutlich nutzen sie ihre eigenen Gebäude, die sie auch für die Suche und Gmail brauchen
- GCP ist in geographische Regionen aufgeteilt
- Es gibt etwa 40 davon

Zonen

- Unterteilung von Regionen zwecks Hochverfügbarkeit
- i.d.R. mindestens drei pro Region
- Ressourcen in einer Zone haben maximale Netzwerkbandbreite
- Wichtig für Disaster Recovery: Meistens fällt maximal eine Zone aus



Regionale Zuordnung von Diensten

- Dienste sind entweder global, regional oder zonal
- Regionale Dienste können zwischen Zonen verschoben werden
- Zonale Dienste fallen aus, wenn Zone ausfällt
- Globale Dienste sind die robustesten

Beispiele

Global	Regional	Zonal
VPC: Virtuelles Netzwerk	App Engine: PaaS-Dienst für Anwendungen	Einzelne Instanz (VM)
CDN: Content Delivery Network	Managed Instance Groups	Persistent Disk

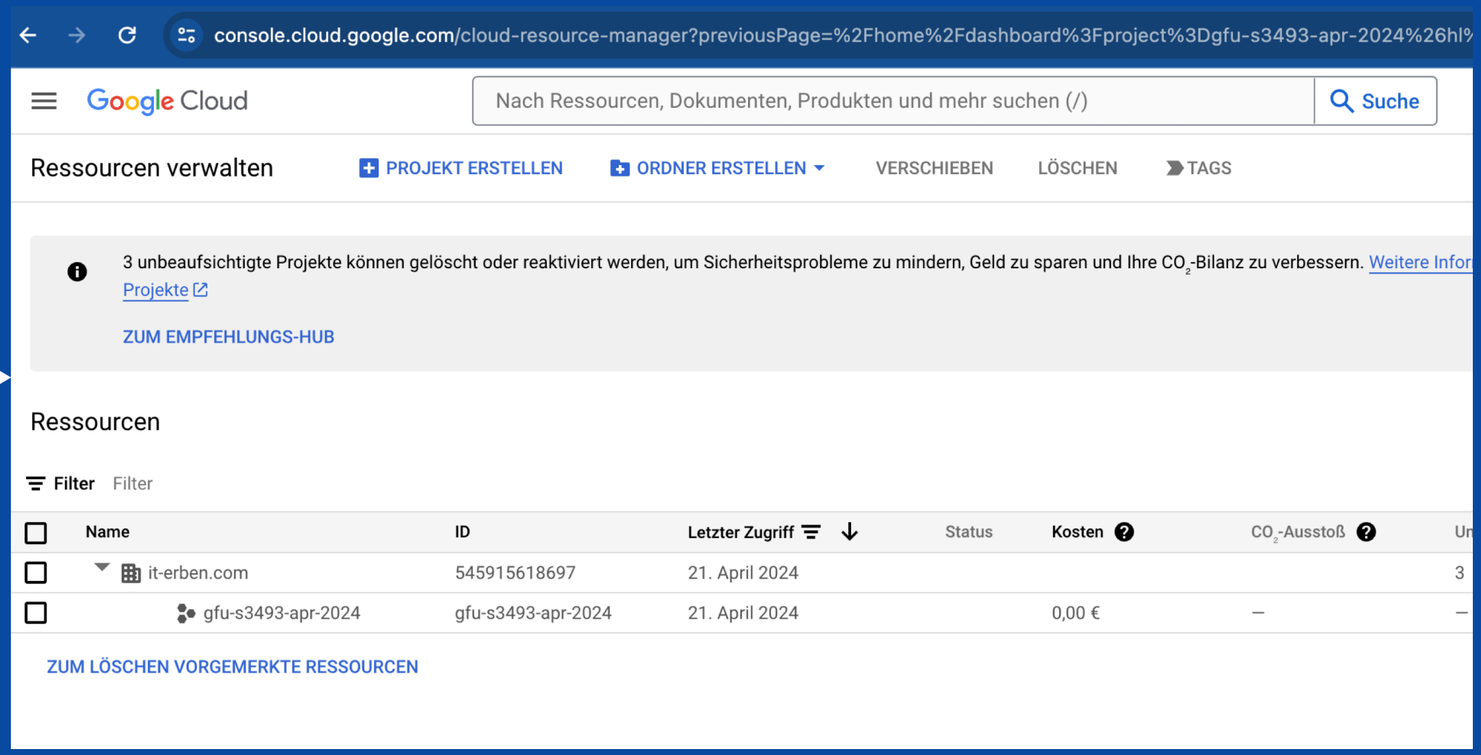
Demo: Gemini, APIs und Budgets

Ressourcen-Übersicht

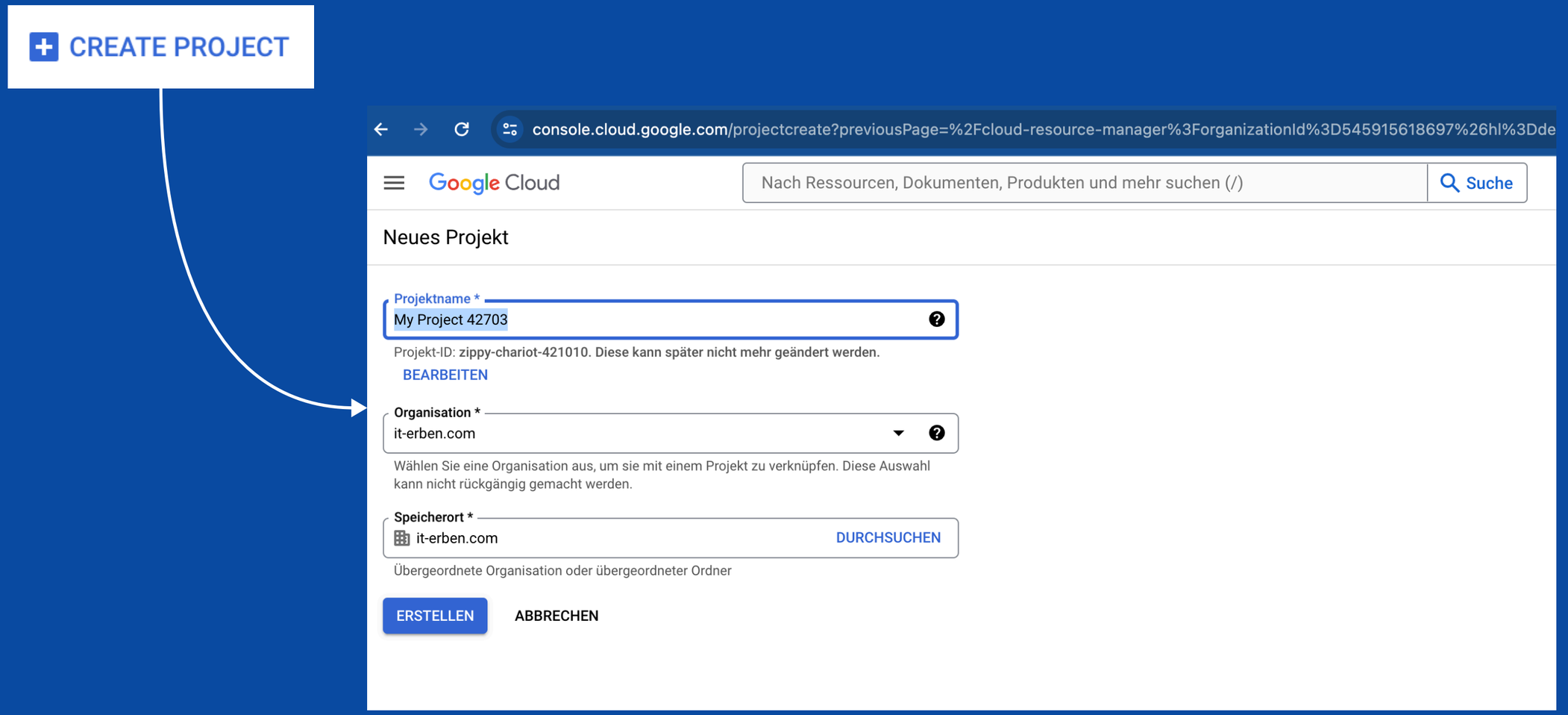
console.cloud.google.com

Google Cloud Platform

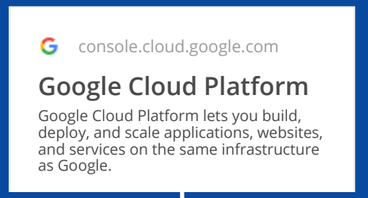
Google Cloud Platform lets you build, deploy, and scale applications, websites, and services on the same infrastructure as Google.

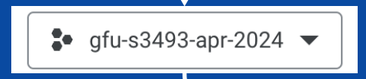


Projekt erstellen

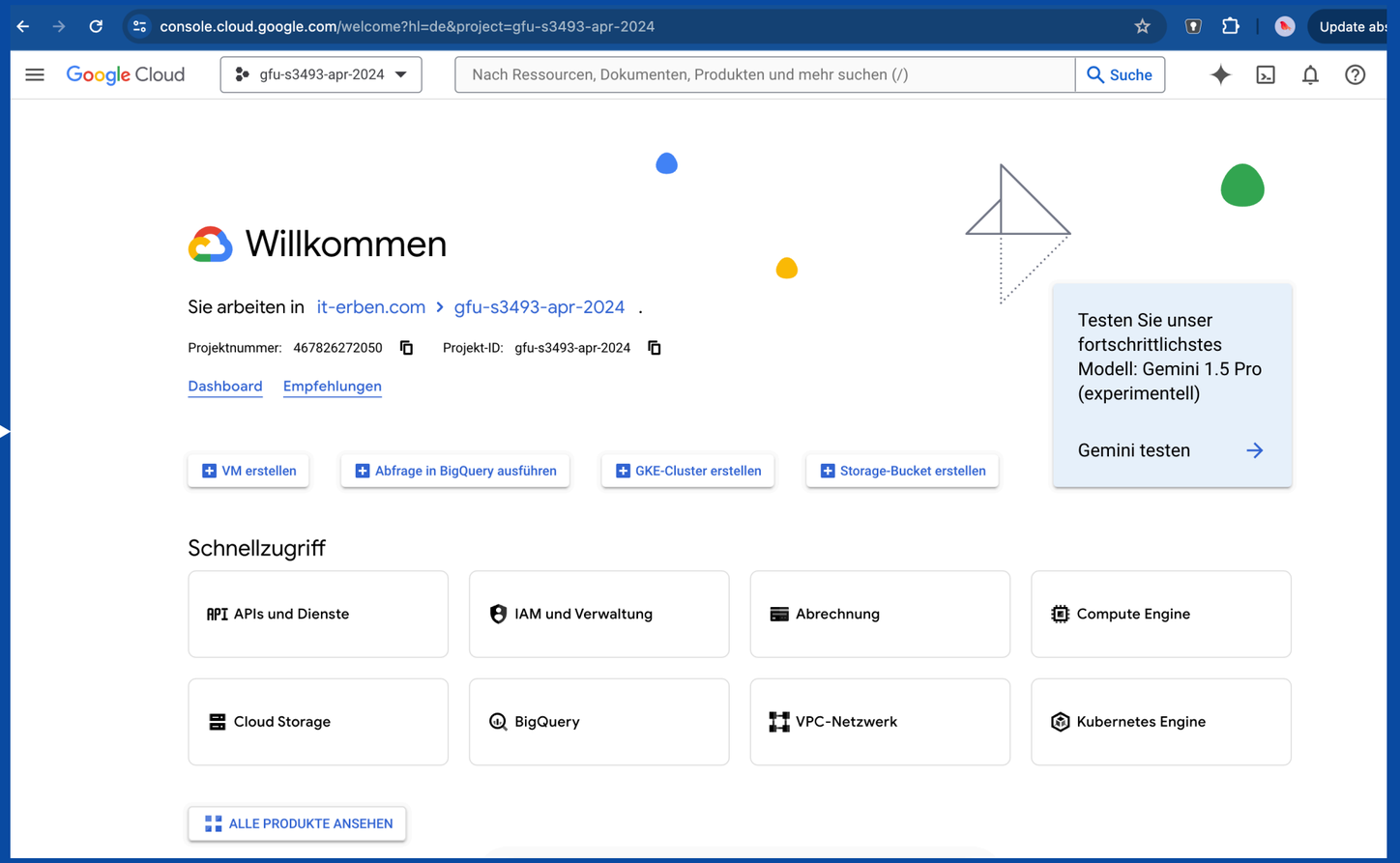


Startseite

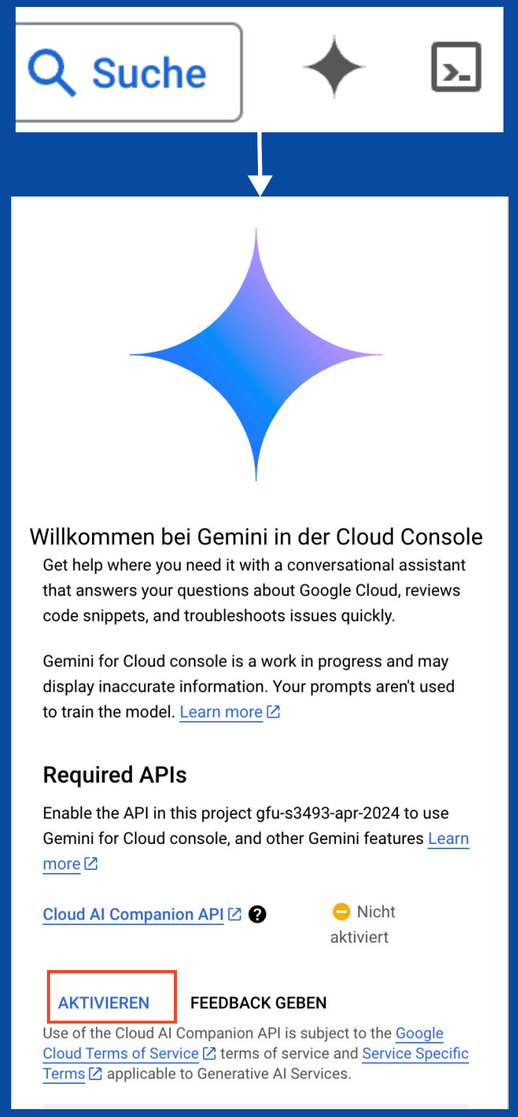

console.cloud.google.com
Google Cloud Platform
Google Cloud Platform lets you build, deploy, and scale applications, websites, and services on the same infrastructure as Google.


gfu-s3493-apr-2024


Ressource auswählen
IT-ERBEN.COM
Projekte und Ordner suchen
AKTUELL
MARKIERT
ALLE
Name
ID
gfu-s3493-apr-2024
gfu-s3493-apr-2024
my-firebase-project
my-firebase-project-428308
it-erben.com
545915618697
veolia-jun-2024
veolia-jun-2024


console.cloud.google.com/welcome?hl=de&project=gfu-s3493-apr-2024
Google Cloud
gfu-s3493-apr-2024
Nach Ressourcen, Dokumenten, Produkten und mehr suchen (/)
Suche
Willkommen
Sie arbeiten in it-erben.com › gfu-s3493-apr-2024 .
Projektnummer: 467826272050
Projekt-ID: gfu-s3493-apr-2024
Dashboard
Empfehlungen
Testen Sie unser fortschrittlichstes Modell: Gemini 1.5 Pro (experimentell)
Gemini testen
VM erstellen
Abfrage in BigQuery ausführen
GKE-Cluster erstellen
Storage-Bucket erstellen
Schnellzugriff
APIs und Dienste
IAM und Verwaltung
Abrechnung
Compute Engine
Cloud Storage
BigQuery
VPC-Netzwerk
Kubernetes Engine
ALLE PRODUKTE ANSEHEN

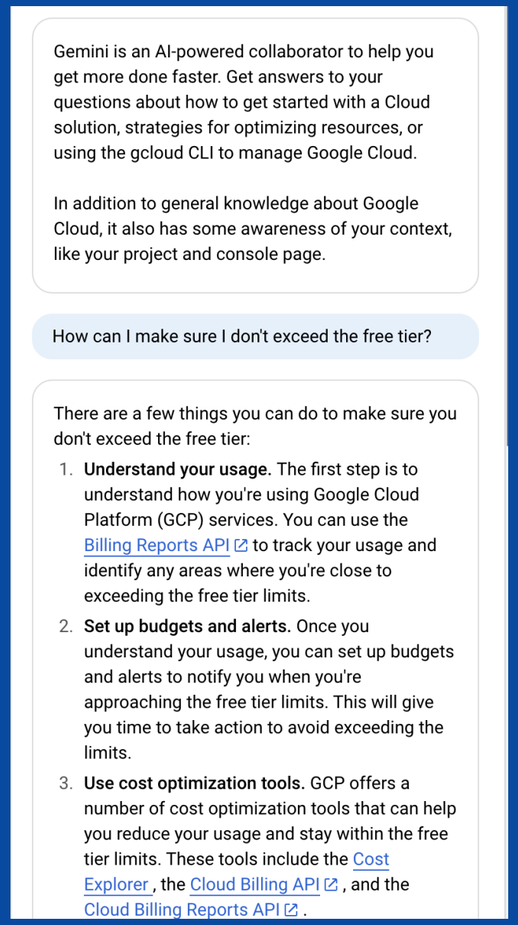
Gemini: Erste API aktivieren

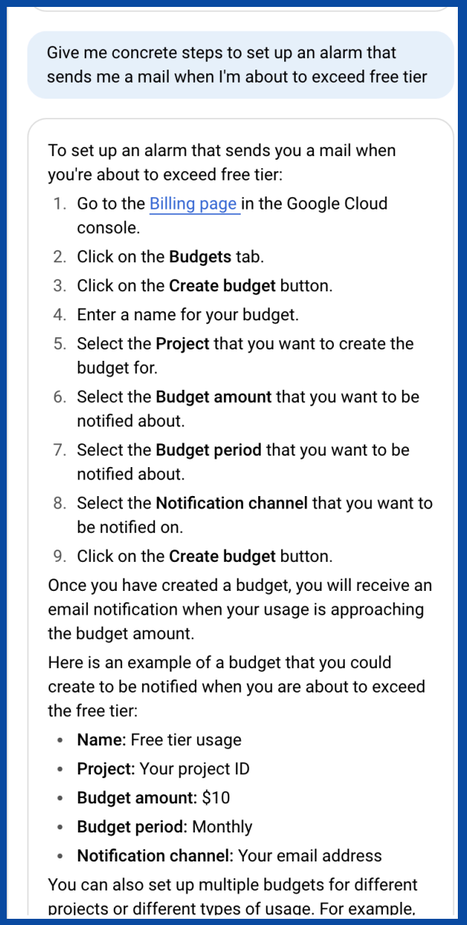


- Jede Ressource in GCP wird über eine API verwaltet
- APIs müssen für jedes Projekt erst aktiviert werden
- Dies kann mehrere Minuten dauern
- Großer Unterschied zu AWS

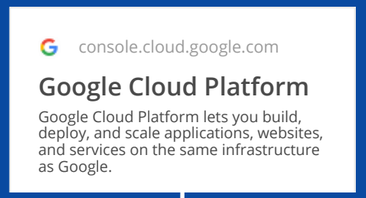
Gemini nutzen, um Kostenalarm zu setzen

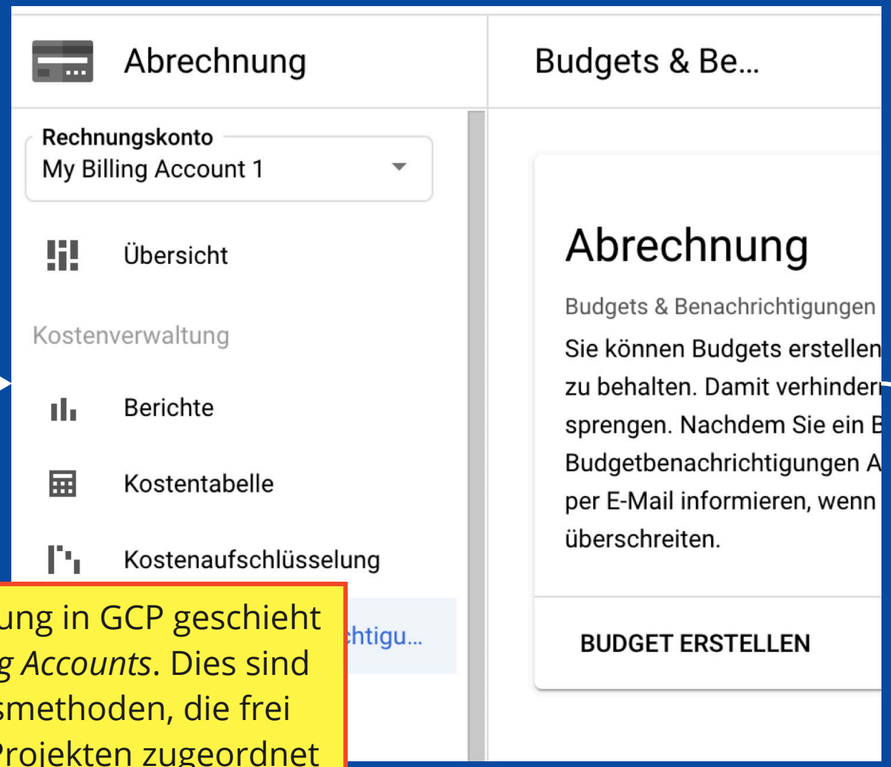
- Gemini kann uns bei vielen einfachen Aufgaben helfen
- In diesem Beispiel legen wir einen *Budget Alarm* zur Kostenkontrolle an
- Eingebettet in GCP mit Links



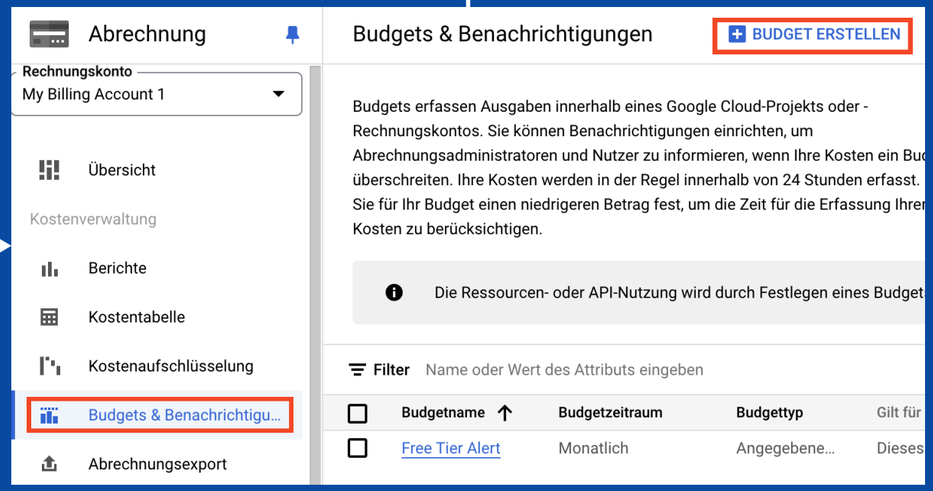


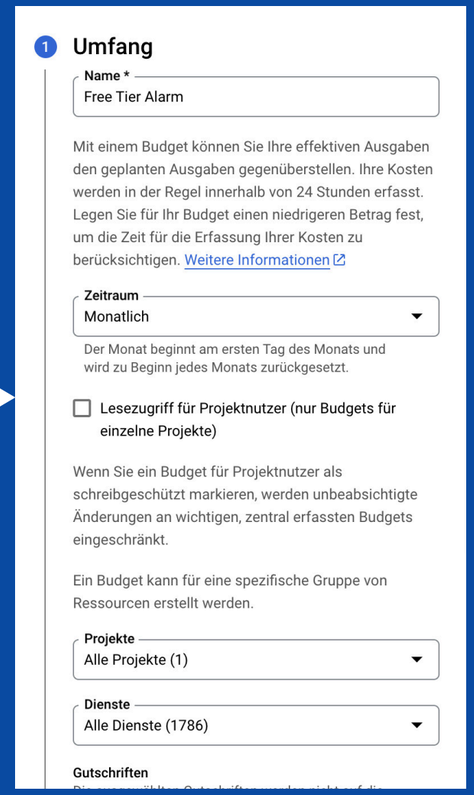
Kostenalarm setzen



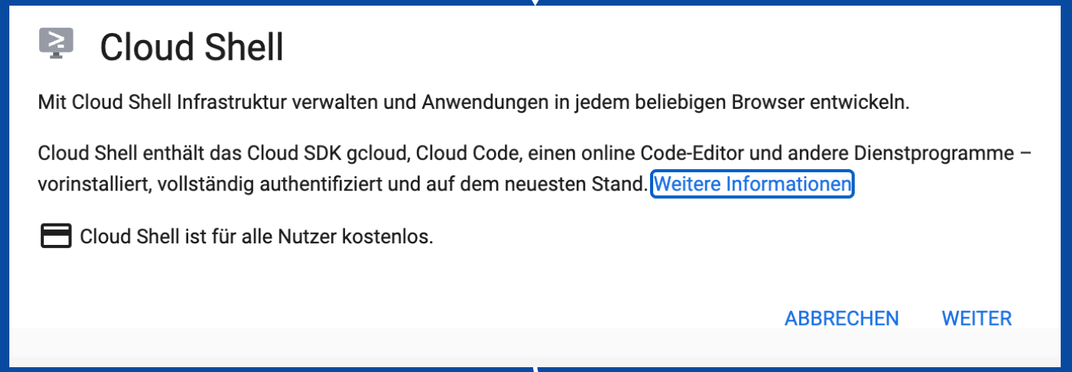


Abrechnung in GCP geschieht mit *Billing Accounts*. Dies sind Zahlungsmethoden, die frei zu GCP-Projekten zugeordnet werden können.





Arbeit mit Cloud Shell: Shell starten




```
alex@cloudshell:~ (gfu-s3493-apr-2024)$ gcloud projects describe gfu-s3493-apr-2024
createTime: '2024-04-21T10:03:14.981095Z'
lifecycleState: ACTIVE
name: gfu-s3493-apr-2024
parent:
  id: '545915618697'
  type: organization
projectId: gfu-s3493-apr-2024
projectNumber: '467826272050'
alex@cloudshell:~ (gfu-s3493-apr-2024)$
```

Google-Accounts anlegen

- Für die Übungsaufgaben stellen wir euch GCP-Projekte zur Verfügung
- Um sie zu nutzen, braucht ihr einen **Google-Account**
- Ihr könnt euren privaten verwenden…
- …oder einen neuen anlegen unter https://accounts.google.com/
- Schickt mir bitte euren Accountnamen im Zoom-Chat und ich lade euch zu einem Projekt ein

Aufgabe: Cloud Shell

Aufgabe: Cloud Shell Editor

Projekte

Ressourcen-Hierarchie

Organisation

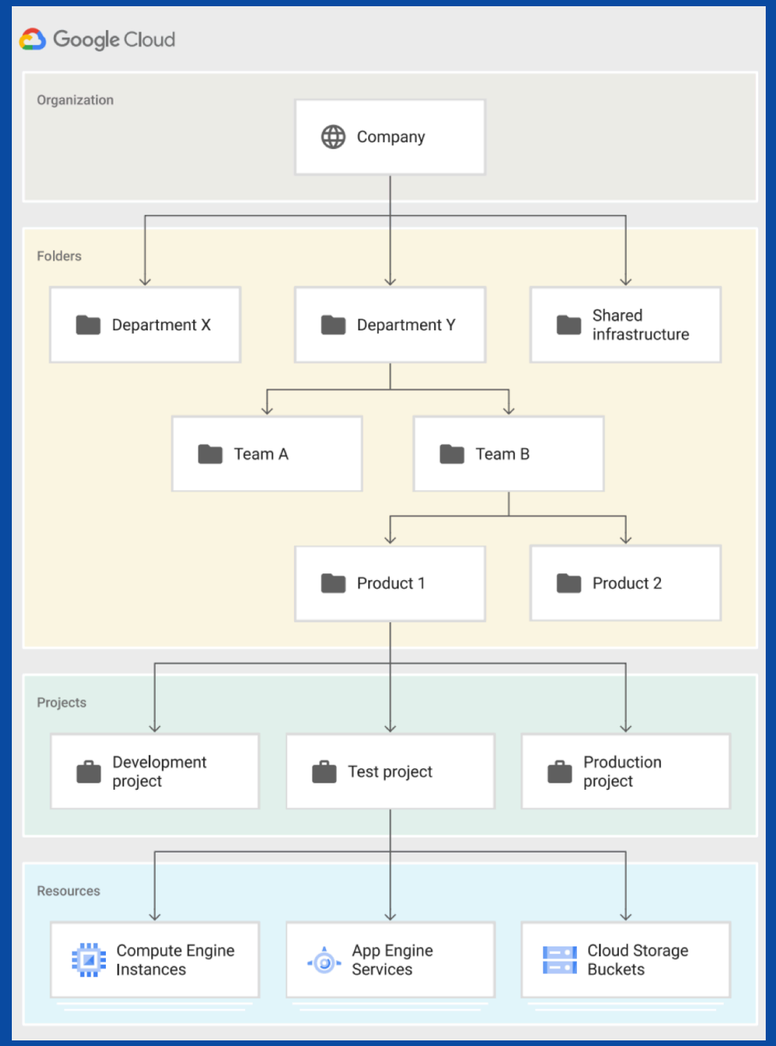
- Oberste Ebene
- Meistens die Firma
- Zugriff auf alle Ressourcen

Verzeichnis

- Logische Aufteilung
- Gruppierung z.B. nach Abteilungen
- optional

Projekt

- Container für Einzelressourcen
- Haupt-Arbeitseinheit
- Unterste Struktur-Einheit

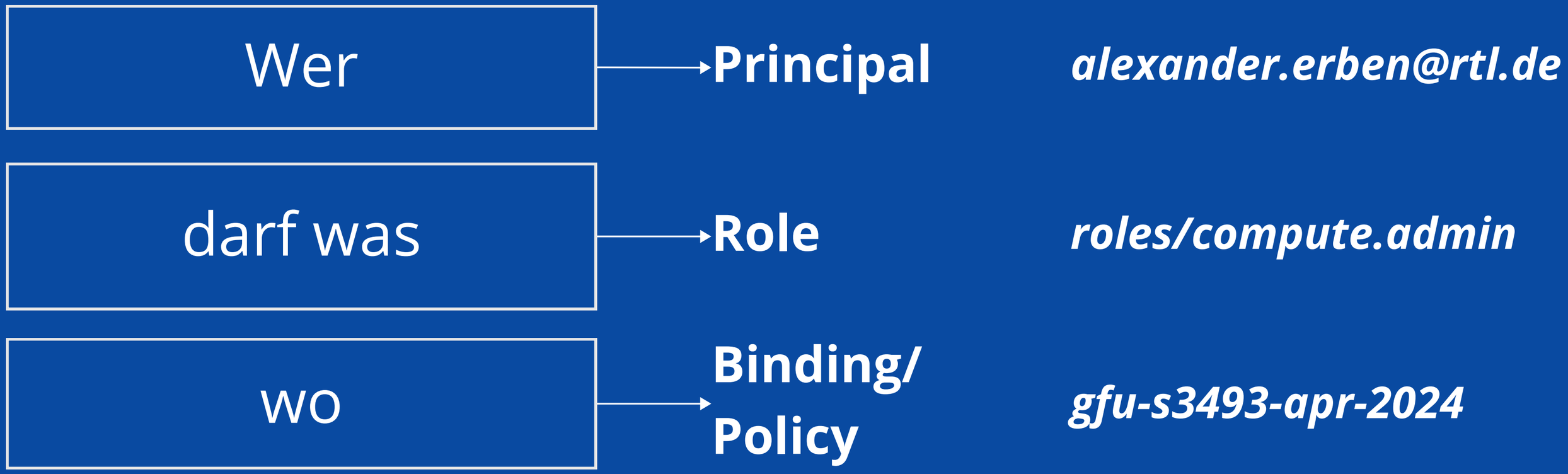


Identity Management

Rollensegmentierung: Principle of least privilege

Rolle	Sollte…	Sollte nicht…
Systems Engineer	• VMs aufsetzen • GKE Cluster • Cloud SQL aufsetzen	• Code zu AppEngine hochladen • Projekte anlegen und löschen
Entwickler	• Code zu Cloud Run hochladen • Logs ansehen • VMs bedienen	• VM löschen • Projekt anlegen oder löschen
Organisations-Administrator	• Projekte anlegen und löschen • Benutzer hinzufügen und löschen • Alle Ressourcen sehen	• VMs installieren oder löschen • BigQuery-Dataset löschen
Budget-Administrator	• Alle Ressourcen sehen • Budget einsehen	… alles andere

Cloud IAM Basiskonzepte



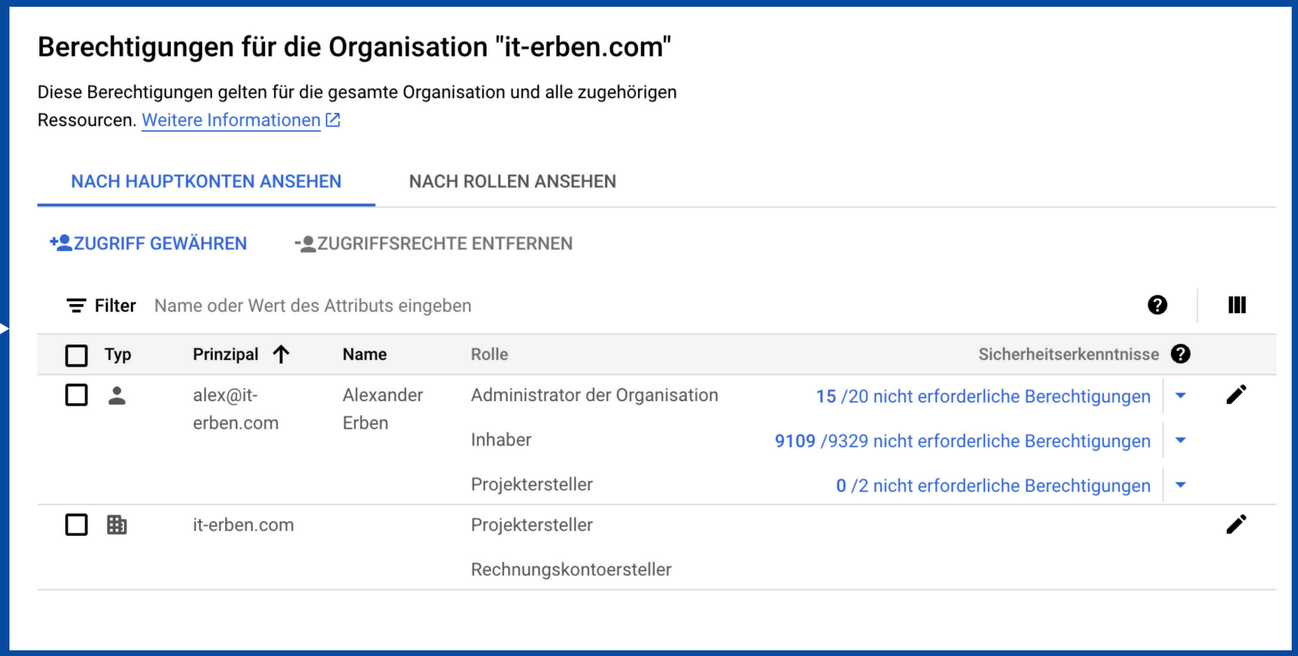
Demo: Google Accounts und Service Accounts

Principles auf Organisationsebene

console.cloud.google.com

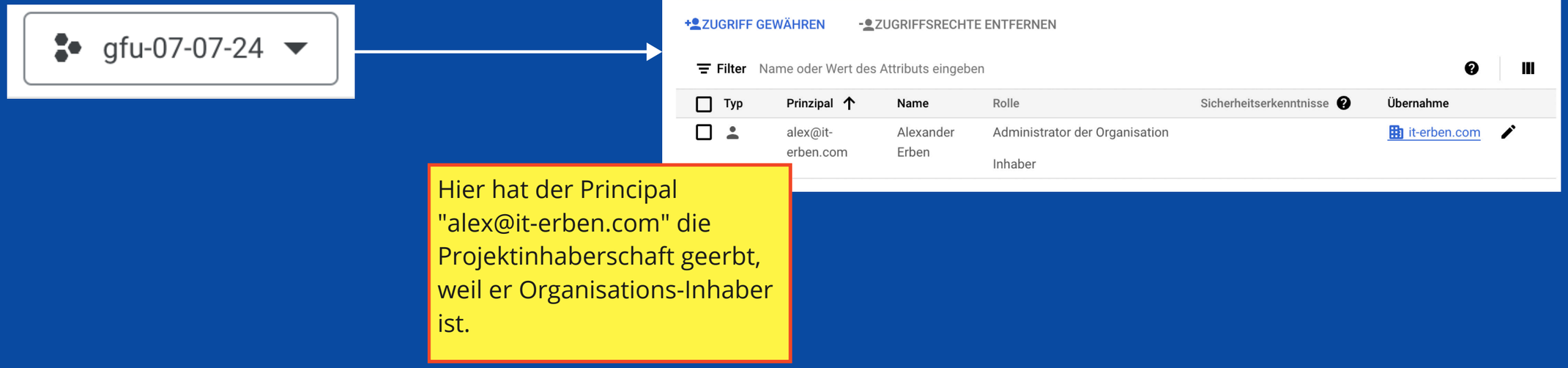
Google Cloud Platform

Google Cloud Platform lets you build, deploy, and scale applications, websites, and services on the same infrastructure as Google.



Demo: Google Accounts und Service Accounts

Principles auf Projektebene

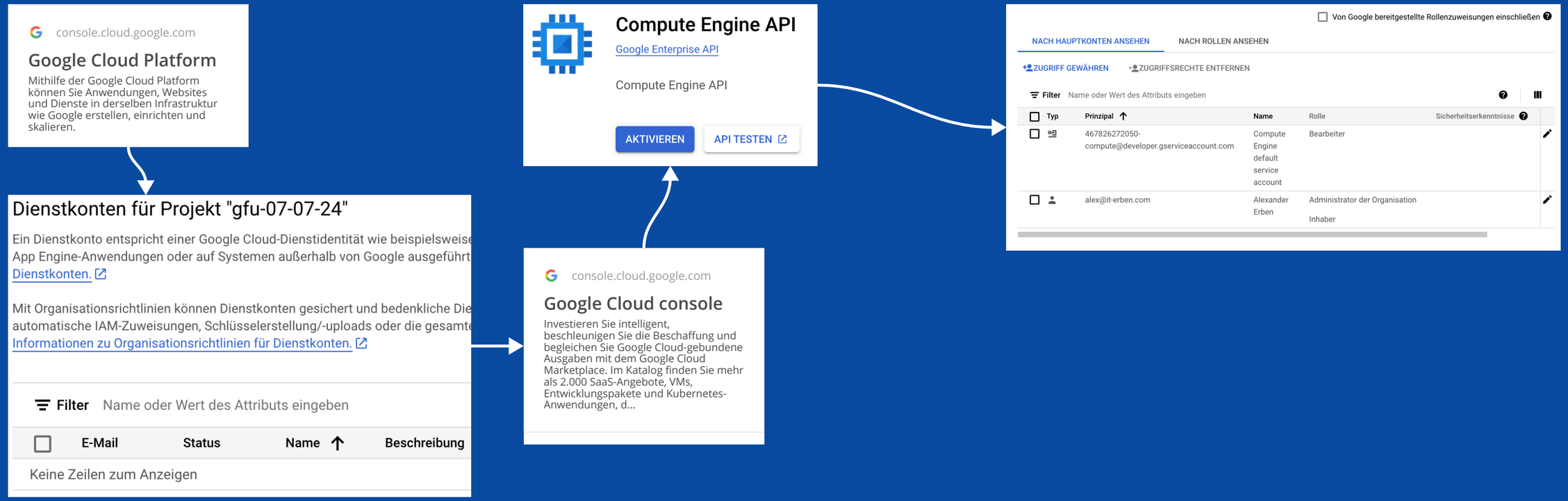


Hier hat der Principal "alex@it-erben.com" die Projektinhaberschaft geerbt, weil er Organisations-Inhaber ist.

Demo: Google Accounts und Service Accounts

APIs benutzen oft Service Accounts

Diese Demo funktioniert nur bei einem neuen Projekt!



Rollen in IAM

- Es gibt Basic Roles (legacy!) und Predefined Roles
- Basic Rollen sind meist sehr breit angelegt
    - Beispiel: roles/viewer, roles/editor, roles/owner
- Predefined Roles sind spezifischer

Compute Admin `roles/compute.admin`	Vollzugriff auf Google Compute Engine
Cloud SQL instance user `roles/cloudsql.instanceUser`	Zugriff auf eine Cloud SQL-Instanz
Storage Object Creator `roles/storage.objectCreator`	Erlaubt es, Objekte in Cloud Storage anzulegen

Rollen und Permissions

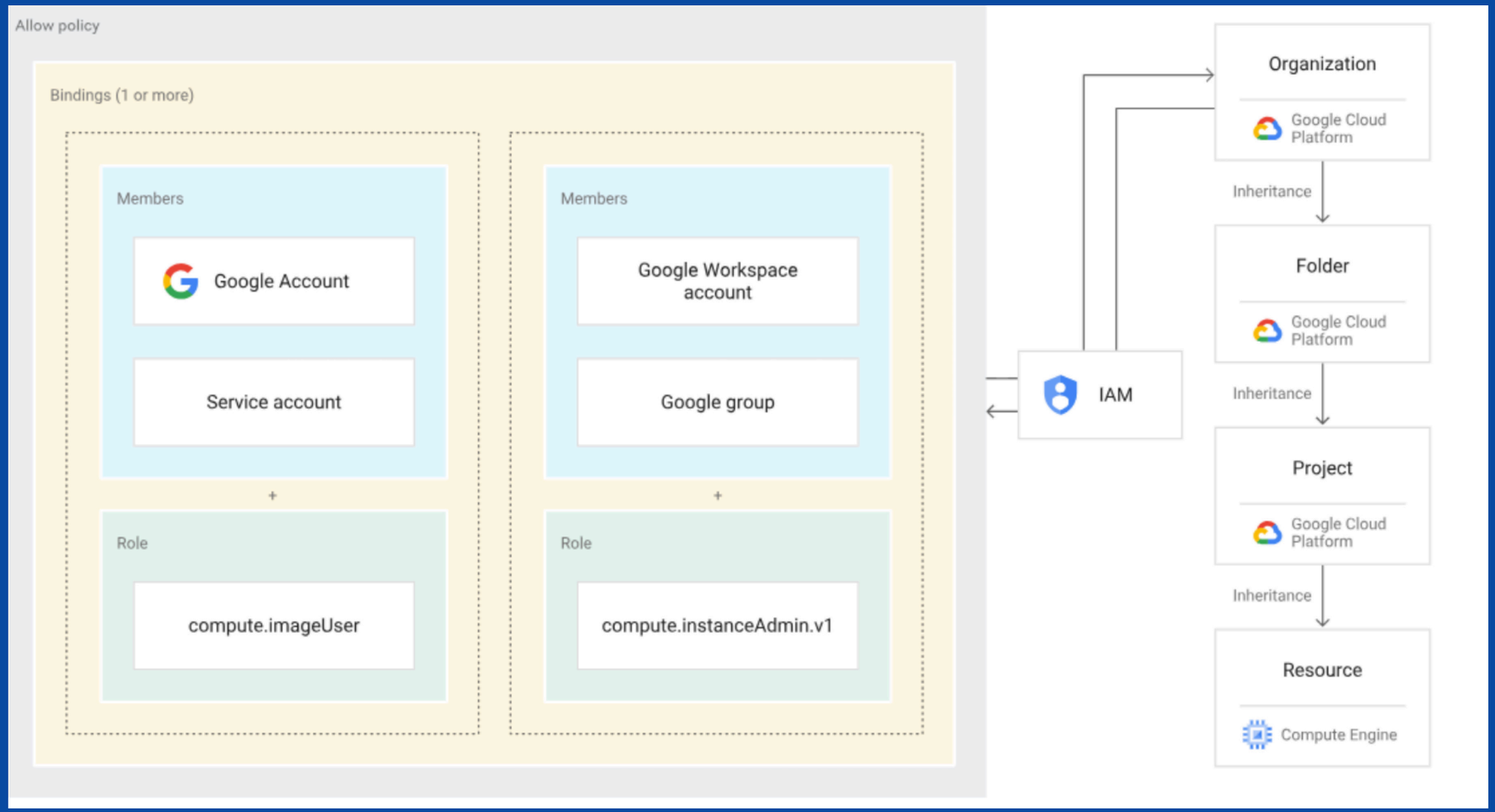
- Im Kern sind Rollen eine Liste von *Permissions*
- Permissions sind granular bezogen auf genau einen Service
- Allgemeines Format:

```
service.resource.verb
```

```
cloudsql.databases.list
appengine.applications.create
```

Allow Policies

Binden Principals und Rolle an Ressourcen



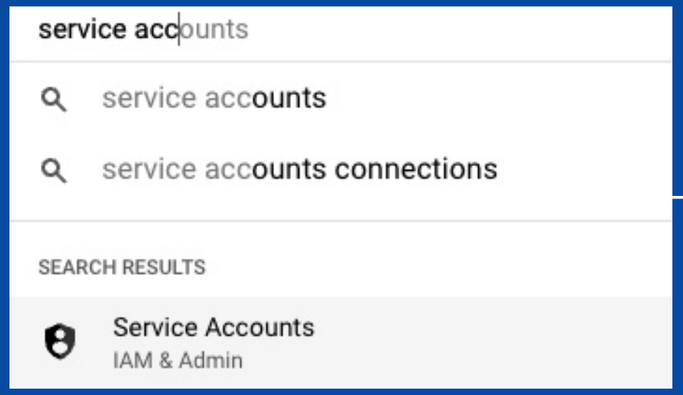
Strukturierung von Projekten

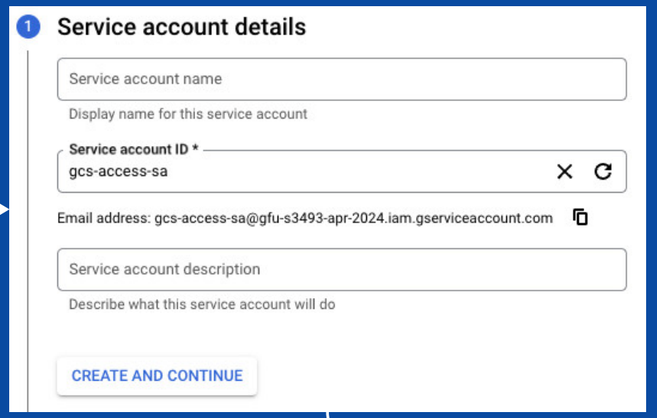
- Google Cloud bietet mehrere Hierarchie-Ebenen zur Strukturierung von Projekten
- Projekte gehören zu einer **Organisation**
- Innerhalb einer Organisation können sie in **Verzeichnisse (Folder)** gruppiert werden
- Berechtigungen können auf jede dieser Einheiten definiert werden

Identity Management und Berechtigungen

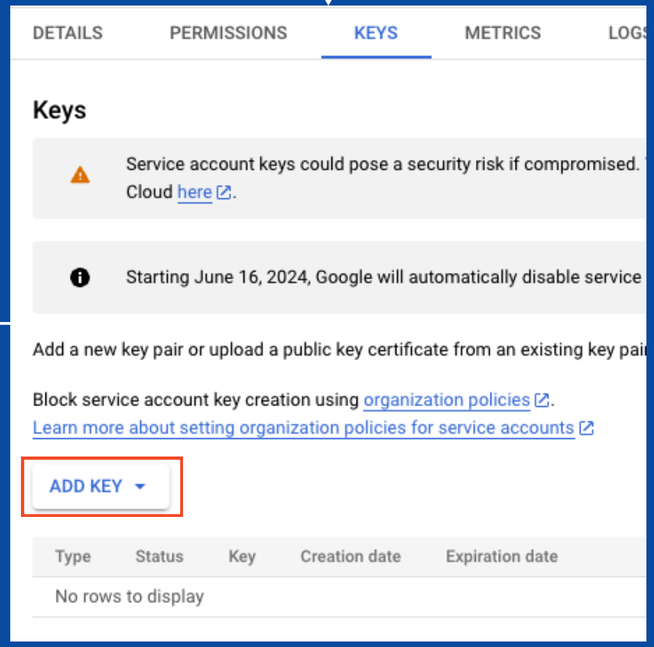
- Eng verbunden mit der Ressourcenhierarchie sind die Berechtigungen
- Benutzer entstehen normalerweise aus Organisationen
- … können aber auch Google-Accounts sein
- Ihnen werden auf verschiedenen Ebenen Rollen zugewiesen

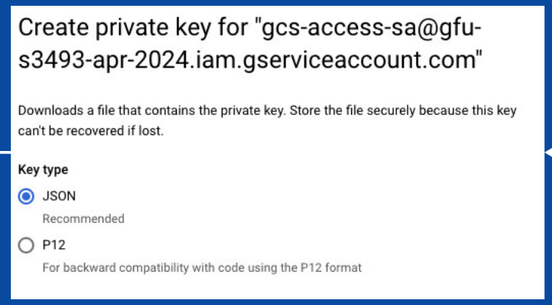
Demo: Role Bindings mit Cloud Shell

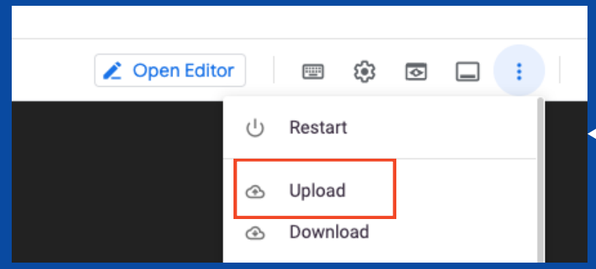




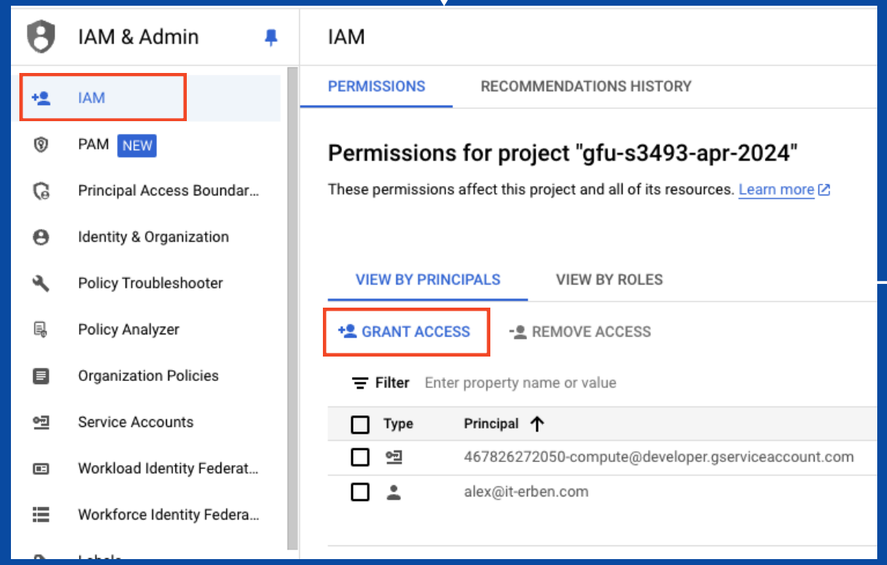
Anlegen eines Service Accounts, generieren eines Keys und Upload in Cloud Shell, um den SA nutzen zu können. Erstmal ohne Permissions!

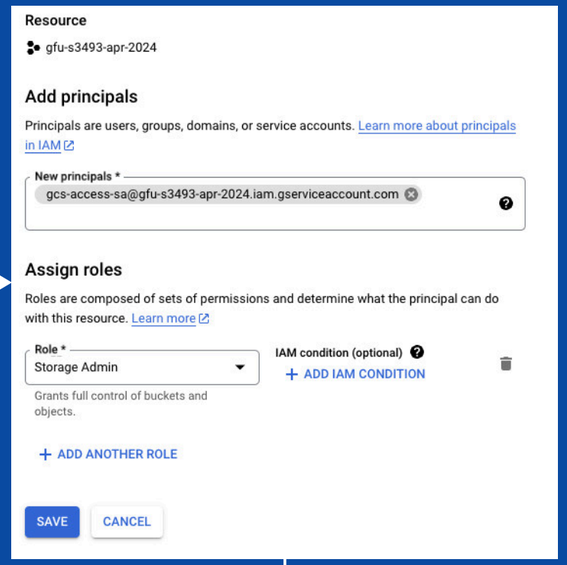






```
alex@cloudshell:~ (gfu-s3493-apr-2024)$ gcloud auth activate-service-account  --key-file=gfu-s3493-apr-2024-2229db8a0492.json
Activated service account credentials for: [gcs-access-sa@gfu-s3493-apr-2024.iam.gserviceaccount.com]
alex@cloudshell:~ (gfu-s3493-apr-2024)$ gcloud storage ls
ERROR: (gcloud.storage.ls) HTTPError 403: gcs-access-sa@gfu-s3493-apr-2024.iam.gserviceaccount.com does not have storage.buckets.list access to the Google Cloud project
). This command is authenticated as gcs-access-sa@gfu-s3493-apr-2024.iam.gserviceaccount.com which is the active account specified by the [core/account] property.
alex@cloudshell:~ (gfu-s3493-apr-2024)$
```



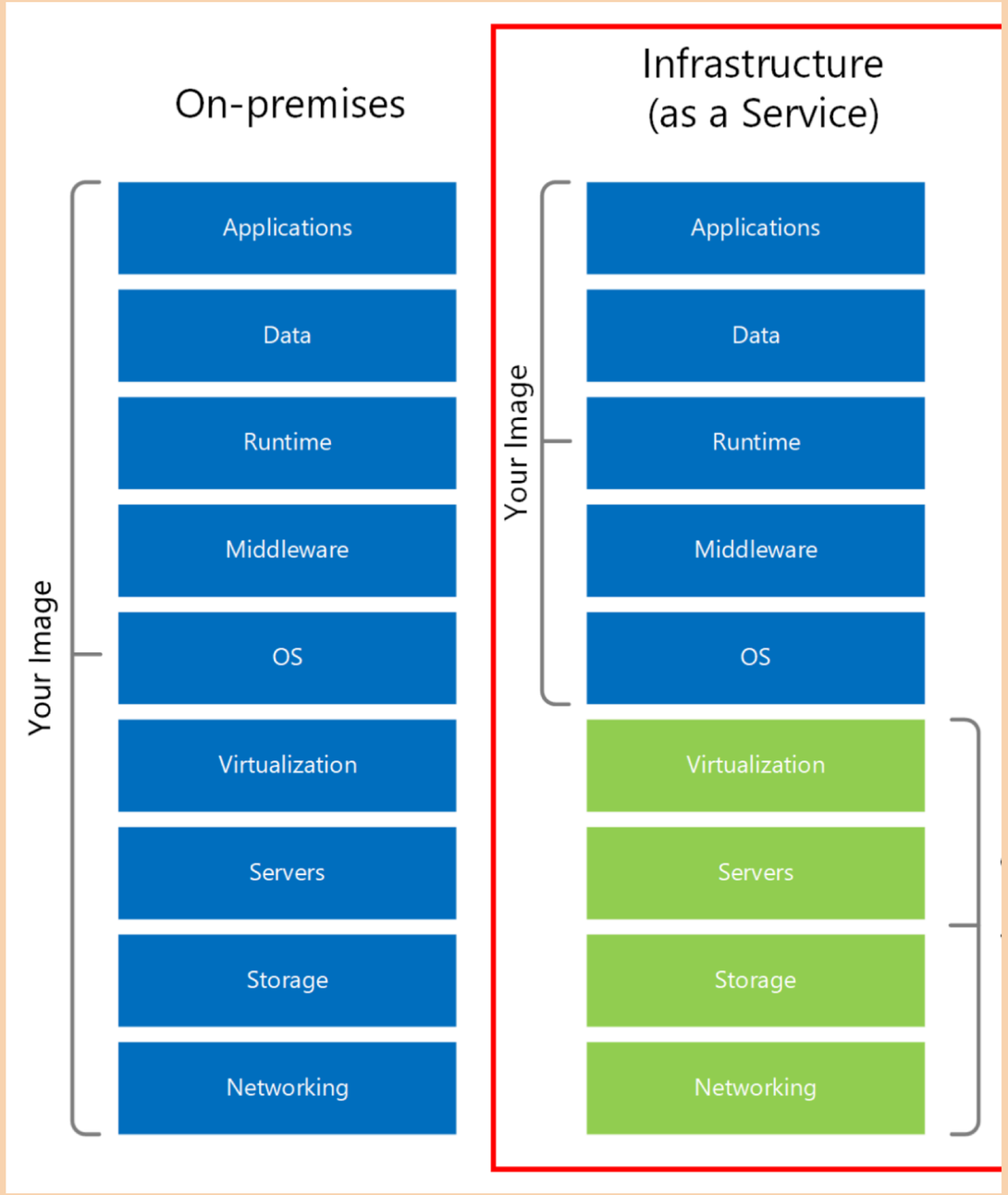



```
alex@cloudshell:~ (gfu-s3493-apr-2024)$ gcloud storage ls
gs://mybucket-gfu-15744/
alex@cloudshell:~ (gfu-s3493-apr-2024)$
```

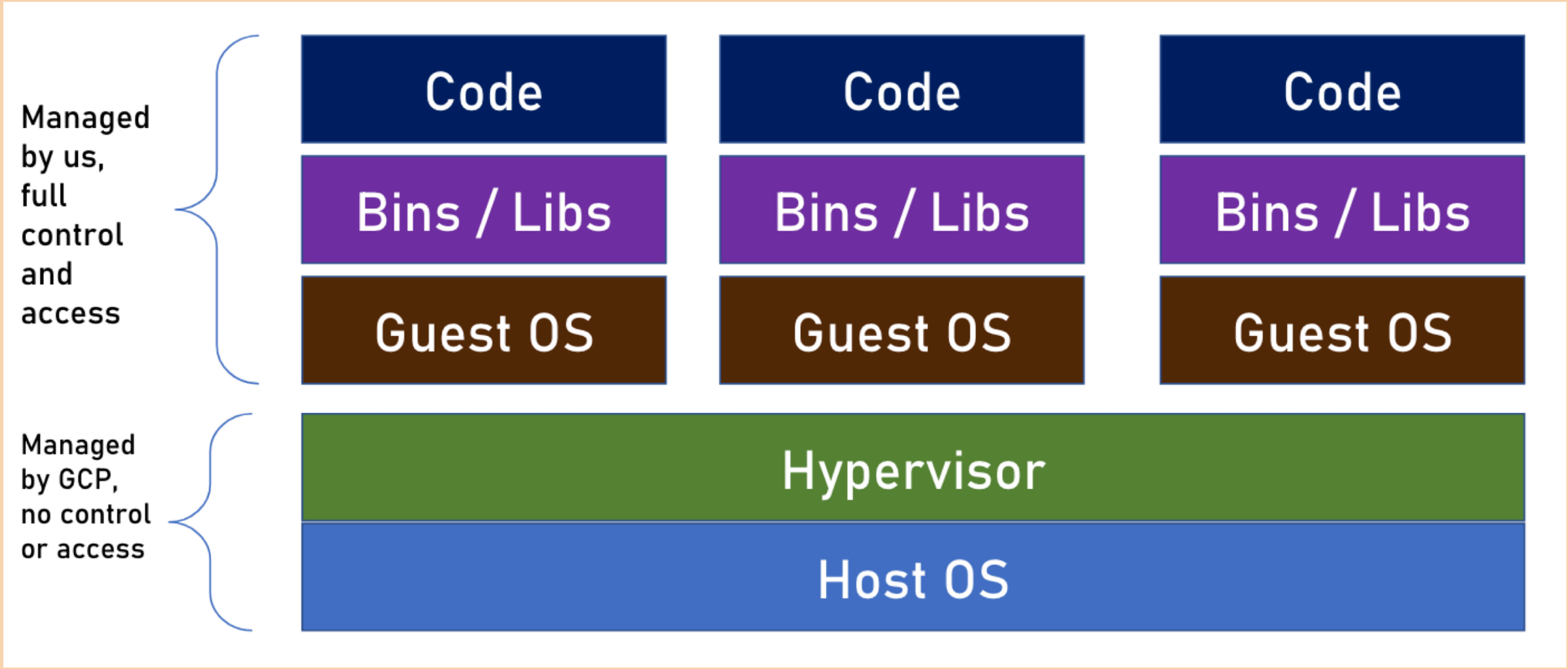
Compute Engine

Google Compute Engine

- Dienst zur Erstellung und Verwaltung von VMs in der Cloud
- Infrastructure as a service
- Vergleichbar mit AWS EC2



Virtuelle Maschinen in GCP



Konfigurationsoptionen für VMs in GCP

- Location der VM
- Image (Betriebssystem und Software)
- Leistung
- Netzwerk
- weitere Einstellungen

VM-Familien

- GCP unterteilt VMs in Familien
- Jede Familie ist für bestimmte Use Cases ausgelegt
- Weitere Unterteilung nach Serie und Generation
- Es ist wichtig, die richtige Familie zu wählen

General Purpose	Webserver, Virtuelle Desktops
Compute Optimized	High Performance Computing, Media Transcoding, Spieleserver
Memory Optimized	In-Memory-Datenbanken, SAP HANA
Accelerator Optimized	Machine Learning

VM-Familien: Beispiel

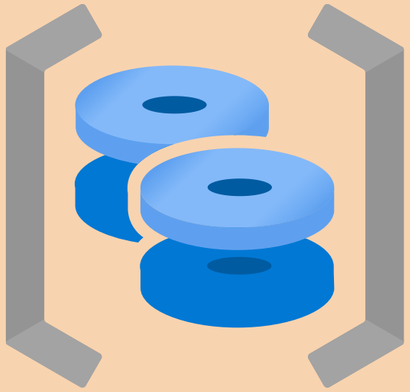
Machine name	vCPUs[1]	Memory (GB)	Max number of persistent disks (PDs)[2]	Max total PD size (TB)	Local SSD	Maximum egress bandwidth (Gbps)[3]
e2-standard-2	2	8	128	257	No	4
e2-standard-4	4	16	128	257	No	8
e2-standard-8	8	32	128	257	No	16
e2-standard-16	16	64	128	257	No	16
e2-standard-32	32	128	128	257	No	16

e2-standard-2:

- *e2*: Machine Type Family
- *standard*: Art der Arbeitslast
- *2*: Anzahl der CPUs

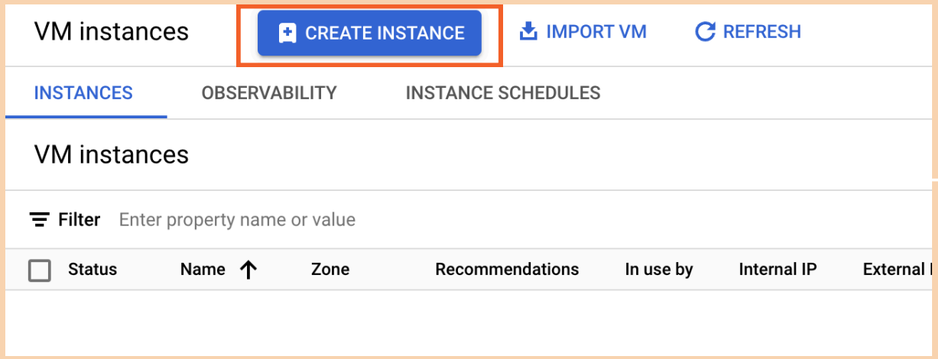
Storage und Netzwerk-Optionen abhängig von Machine!

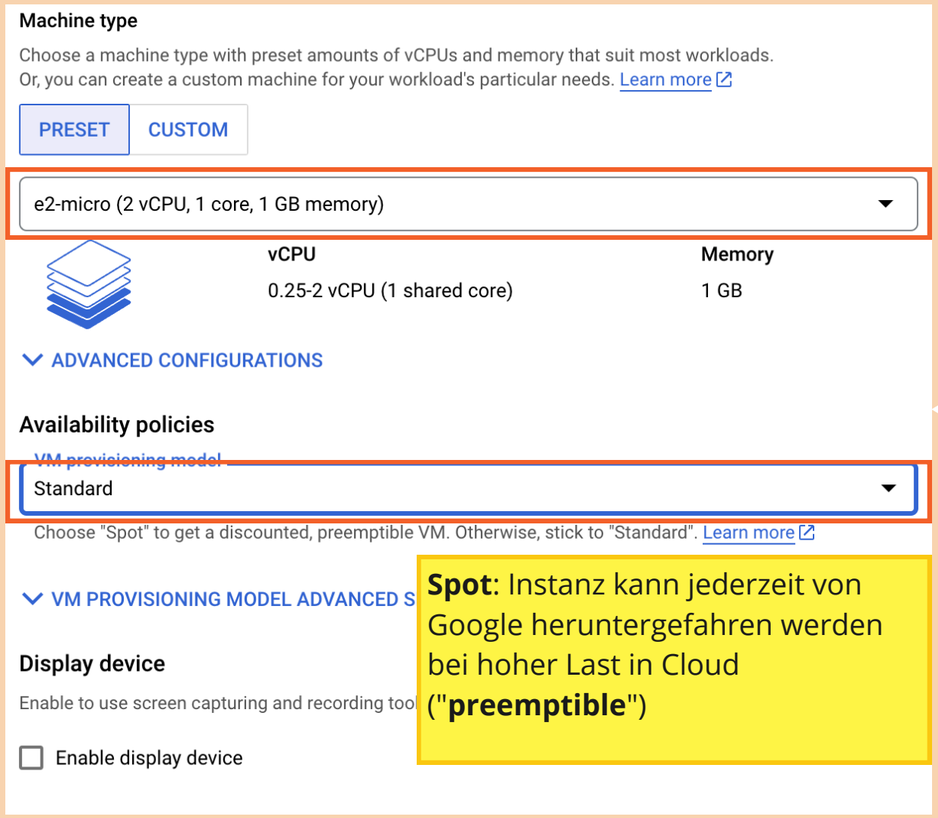
Images



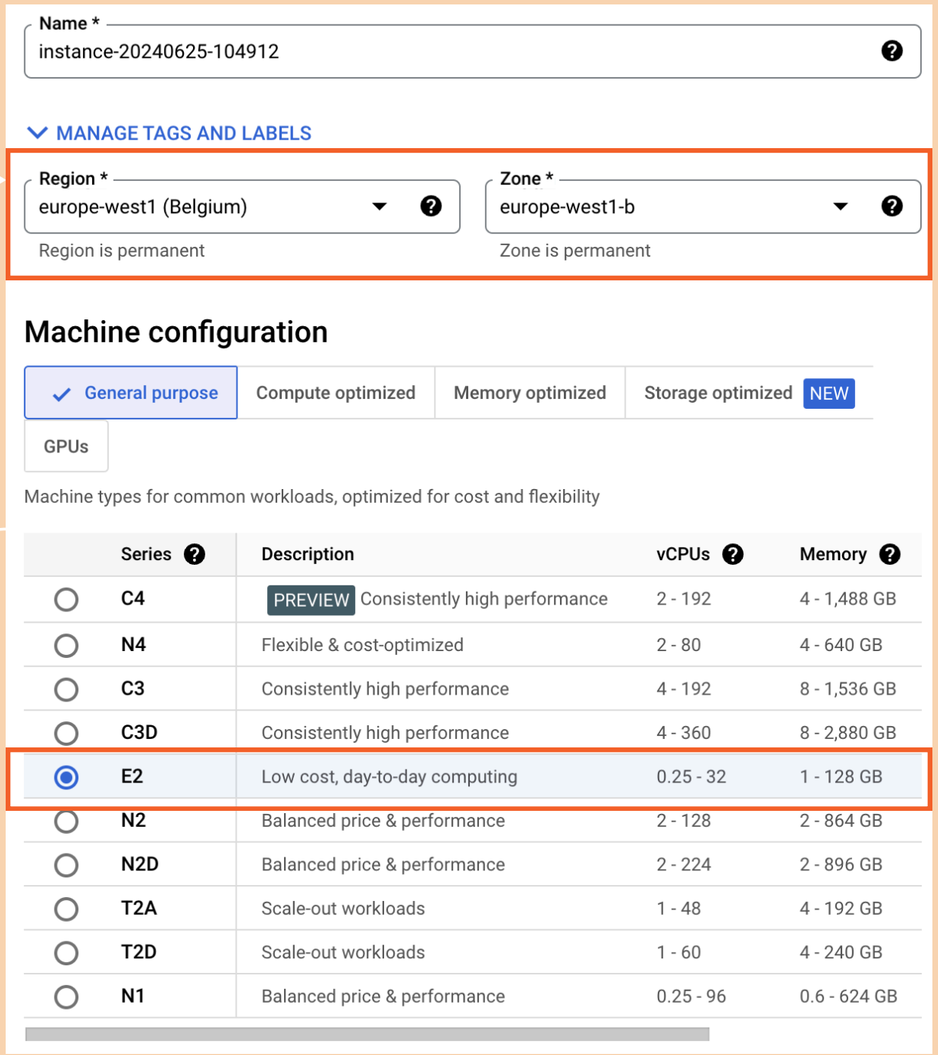
- Bestimmen, welches OS auf der Maschine installiert ist
- Es gibt öffentliche und private Images
- Öffentliche Images sind u.A. von Google verwaltet

Demo: Compute Engine





Spot: Instanz kann jederzeit von Google heruntergefahren werden bei hoher Last in Cloud ("**preemptible**")



Identity and API access

Service accounts

Service account: Compute Engine default service account

Requires the Service Account User role (roles/iam.serviceAccountUser) to be set for users who want to access VMs with this service account. Learn more

Access scopes

- (•) Allow default access
- ( ) Allow full access to all Cloud APIs
- ( ) Set access for each API

Standardmäßig sind nur wenige APIs wie Storage und Stackdriver aktiv für die VMs

Firewall

Add tags and firewall rules to allow specific network traffic from the Internet

- [x] Allow HTTP traffic
- [ ] Allow HTTPS traffic
- [ ] Allow Load Balancer Health Checks

Wir öffnen HTTP für unsere Tests

Name * instance-20240625-20240625-171729

MANAGE TAGS AND LABELS

Region * us-central1 (Iowa) — Region is permanent

Zone * us-central1-a — Zone is permanent

Machine configuration

General purpose | Compute optimized | Memory optimized | Storage optimized NEW | GPUs

Machine types for common workloads, optimized for cost and flexibility

Series	Description	vCPUs	Memo
C4	PREVIEW Consistently high performance	2 - 192	4 - 1,4
N4	Flexible & cost-optimized	2 - 80	4 - 64
C3	Consistently high performance	4 - 192	8 - 1,5
C3D	Consistently high performance	4 - 360	8 - 2,8
E2	Low cost, day-to-day computing	0.25 - 32	1 - 12
N2	Balanced price & performance	2 - 128	2 - 86
N2D	Balanced price & performance	2 - 224	2 - 89
T2A	Scale-out workloads	1 - 48	4 - 19
T2D	Scale-out workloads	1 - 60	4 - 24
N1	Balanced price & performance	0.25 - 96	0.6 - 6

CREATE | CANCEL | EQUIVALENT CODE

COMMAND LINE | REST | TERRAFORM

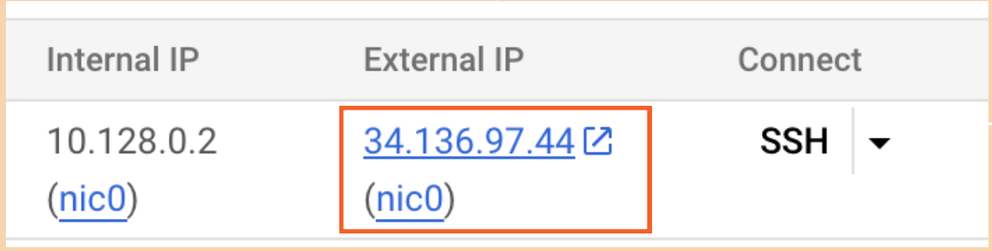
```
gcloud compute instances create instance-20240625-20240625-171729 \
    --project=gfu-s3493-apr-2024 \
    --zone=us-central1-a \
    --machine-type=e2-micro \
    --network-interface=network-tier=PREMIUM,stack-type=IPV4_ONLY,subnet=default \
    --maintenance-policy=MIGRATE \
    --provisioning-model=STANDARD \

    --service-account=467826272050-compute@developer.gserviceaccount.com \
    --scopes=https://www.googleapis.com/auth/cloud-platform \
    --tags=http-server \
    --create-disk=auto-delete=yes,boot=yes,device-name=instance-20240625-171150,image=projects/debian-cloud/global/images/debian-12-bookworm-v20240617,mode=rw,size=10,type=projects/gfu-s3493-apr-2024/zones/us-central1-a/diskTypes/pd-balanced \
    --no-shielded-secure-boot \
    --shielded-vtpm \
    --shielded-integrity-monitoring \
    --labels=goog-ec-src=vm_add-gcloud \
    --reservation-affinity=any
```

COPY | RUN IN CLOUD SHELL | View gcloud reference

Internal IP	External IP	Connect
10.128.0.2 (nic0)	34.136.97.44 (nic0)	SSH

Wir können nur dank der externen IP aus dem Internet auf die Instanz zugreifen

```
sudo apt-get update
sudo apt-get install nginx
sudo systemctl start nginx
```



Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

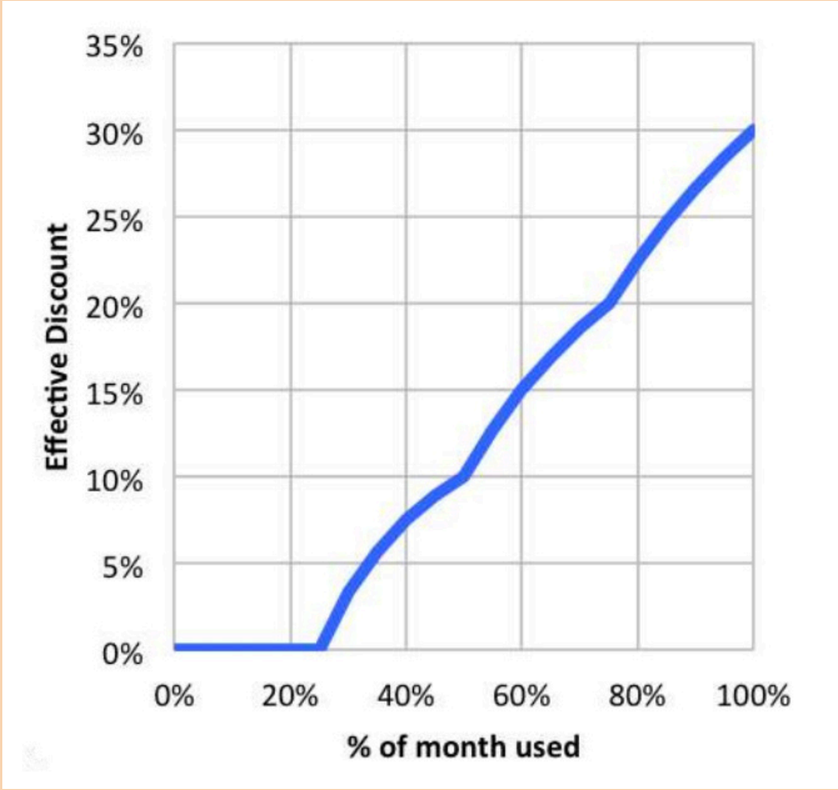
For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

```
gcloud compute instances create instance-20240625-172419 \
    --project=gfu-s3493-apr-2024 \
    --zone=europe-west1-b \
    --machine-type=e2-micro \
    --network-interface=network-tier=PREMIUM,stack-type=IPV4_ONLY,subnet=default \
    --maintenance-policy=MIGRATE \
    --provisioning-model=STANDARD \
    --service-account=467826272050-compute@developer.gserviceaccount.com \
    --scopes=https://www.googleapis.com/auth/devstorage.read_only,https://www.googleap
    is.com/auth/logging.write,https://www.googleapis.com/auth/monitoring.write,https:/
    /www.googleapis.com/auth/servicecontrol,https://www.googleapis.com/auth/service.ma
    nagement.readonly,https://www.googleapis.com/auth/trace.append \
    --tags=http-server \
    --create-disk=auto-delete=yes,boot=yes,device-name=instance-20240625-172419,image=
    projects/debian-cloud/global/images/debian-12-bookworm-v20240617,mode=rw,size=10,t
    ype=projects/gfu-s3493-apr-2024/zones/europe-west1-b/diskTypes/pd-balanced \
    --no-shielded-secure-boot \
    --shielded-vtpm \
    --shielded-integrity-monitoring \
    --labels=goog-ec-src=vm_add-gcloud \
    --reservation-affinity=any
```

Sustained Use Discount

- Lange laufende VMs werden automatisch günstiger
- Beispiel: Wird eine VM des Machine Type N1 für mehr als 25% der Zeit eines Monats genutzt, sinkt der Preis pro Minute um 20-50%
- Gilt auch für Google Kubernetes Engine
- NICHT für ALLE Machine Types verfügbar
- Gilt nicht für AppEngine Flexible



Committed Use Discount

- Ist die Arbeitslast bekannt, kann man für ein bis drei Jahre Compute Instances vorausbezahlen
- Discounts von bis zu 70%
- Gilt auch für Google Kubernetes Engine

Preemptible Instances

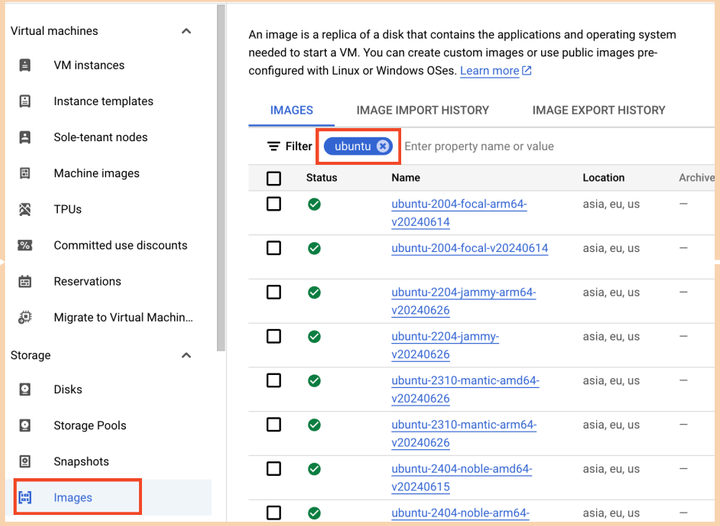
- Kurzlebige, stark verbilligte Instanzen
- "Resterampe" von GCP
- Bis zu 80% günstiger
- Nur sinnvoll wenn die Anwendung ausfallsicher ist
- … und nicht 24/7 laufen muss
- Ideal für nächtliche Batch-Jobs

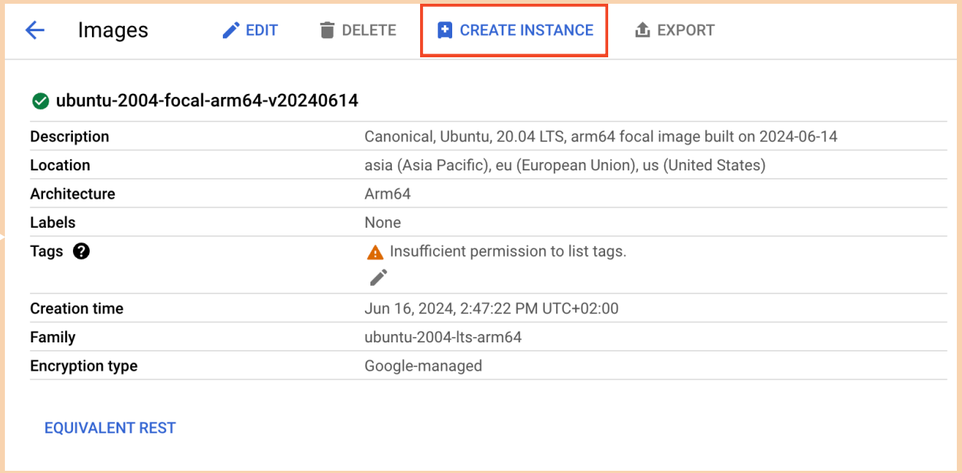
Öffentliche Images

console.cloud.google.com

Google Cloud Platform

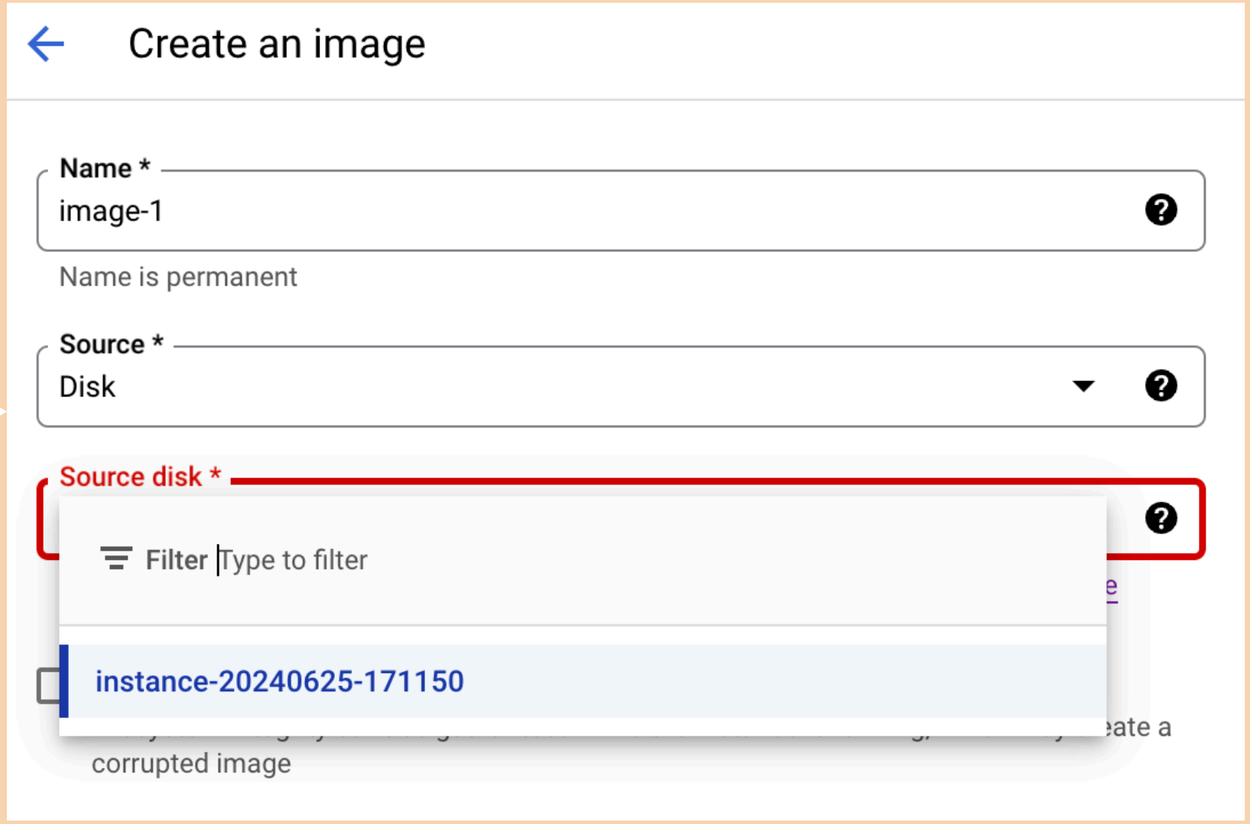
Mithilfe der Google Cloud Platform können Sie Anwendungen, Websites und Dienste in derselben Infrastruktur wie Google erstellen, einrichten und skalieren.





Demo: Image von Instance erstellen

[+] CREATE IMAGE



Aufgabe: IAM + Compute Engine

Mit der Konsole

Mit der Shell

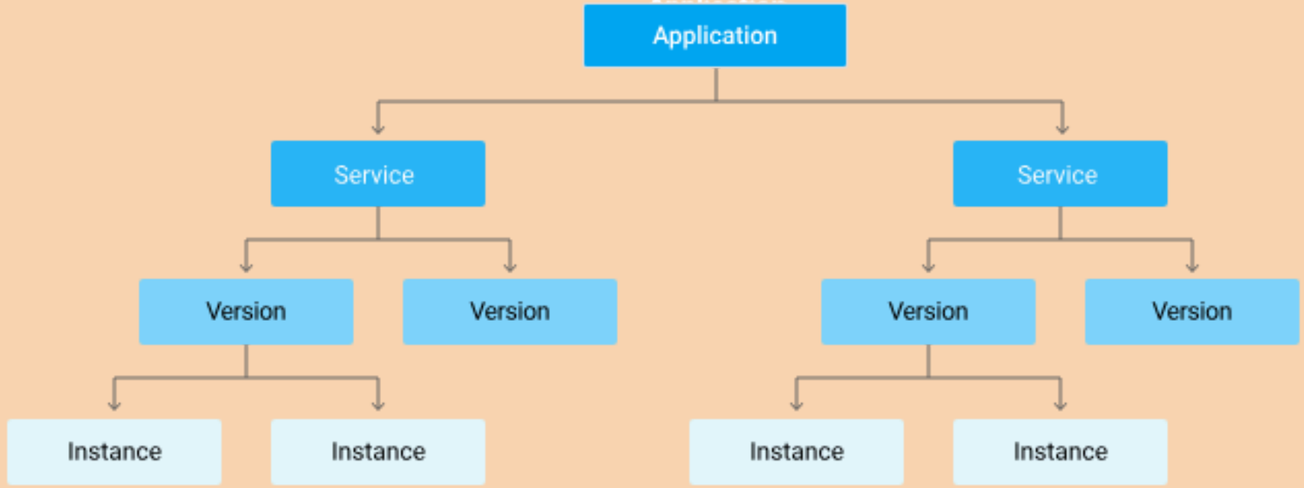
App Engine

Google App Engine

- Platform as a Service für Anwendungshosting
- Ende-zu-Ende-Management
- Unterstützt:
    - Go, Java, .NET, node.js, PHP, Python und Ruby out of the box
    - Unterstützt custom runtimes für jede Sprache
    - In Google-Dienste integriert
- Kosten entstehen nur durch die genutzten Cloud-Ressourcen
- Features:
    - Automatisches Load Balancing und Scaling
    - Managed Updates der Laufzeit und Hosts
    - Versionierung
    - Traffic Split

Google App Engine - Konzepte

- Eine Application wird in einem GCP-Projekt angelegt
- Jede App ist eine Art "Container" und kann aus mehreren Services bestehen
- Für jeden Service können mehrere Versionen parallel existieren
- Für Versionen werden Instanzen angelegt
- Versionen können inaktiv sein



Google App Engine - Umgebungen

- **Standard:** Sprachspezifische Laufzeiten als Sandbox
  - Eingeschränkt, aber besser isoliert
  - Funktioniert ohne eigenes Image
- **Flexible:** Bring-your-own-Docker-Image
  - Verwendet Compute VMs
  - Jede Laufzeit unterstützt
  - Kann Hintergrundprozesse und Volumes nutzen

Google App Engine - Umgebungen

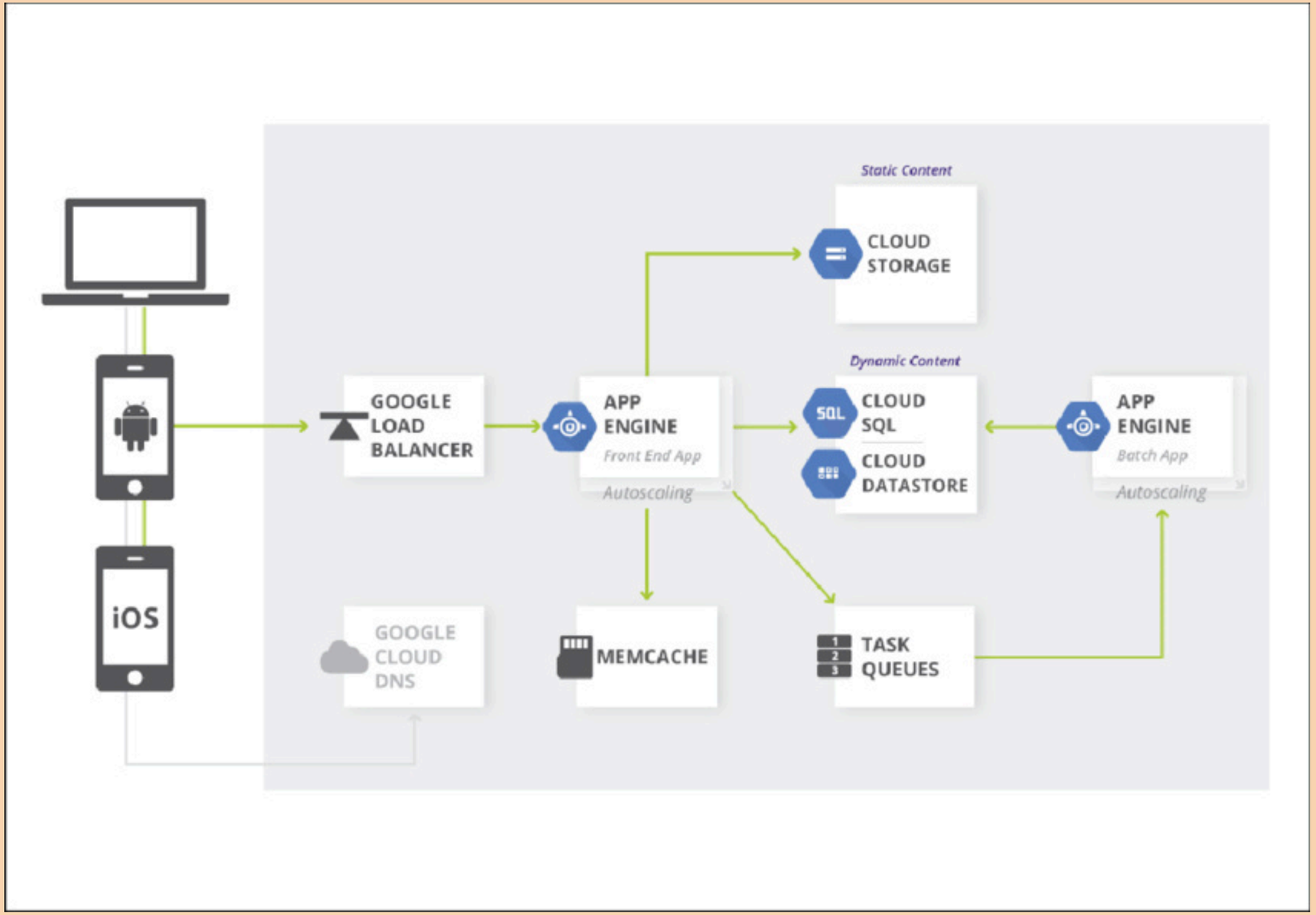
New table

Feature	Standard	Flexible
Kosten	Instanz-Stunden	vCPU, Memory und Disks
Scaling	Manuel, Vereinfacht, Automatisch	Manuell, Automatisch
Scaling auf 0	Ja	Nein
Startzeit	Sekunden	Minuten
Schnelles Skalieren	Ja	Nein
Max. Timeout	bis zu 10 Minuten	bis zu 60 Minuten
SSH für Debugging	Nein	Ja

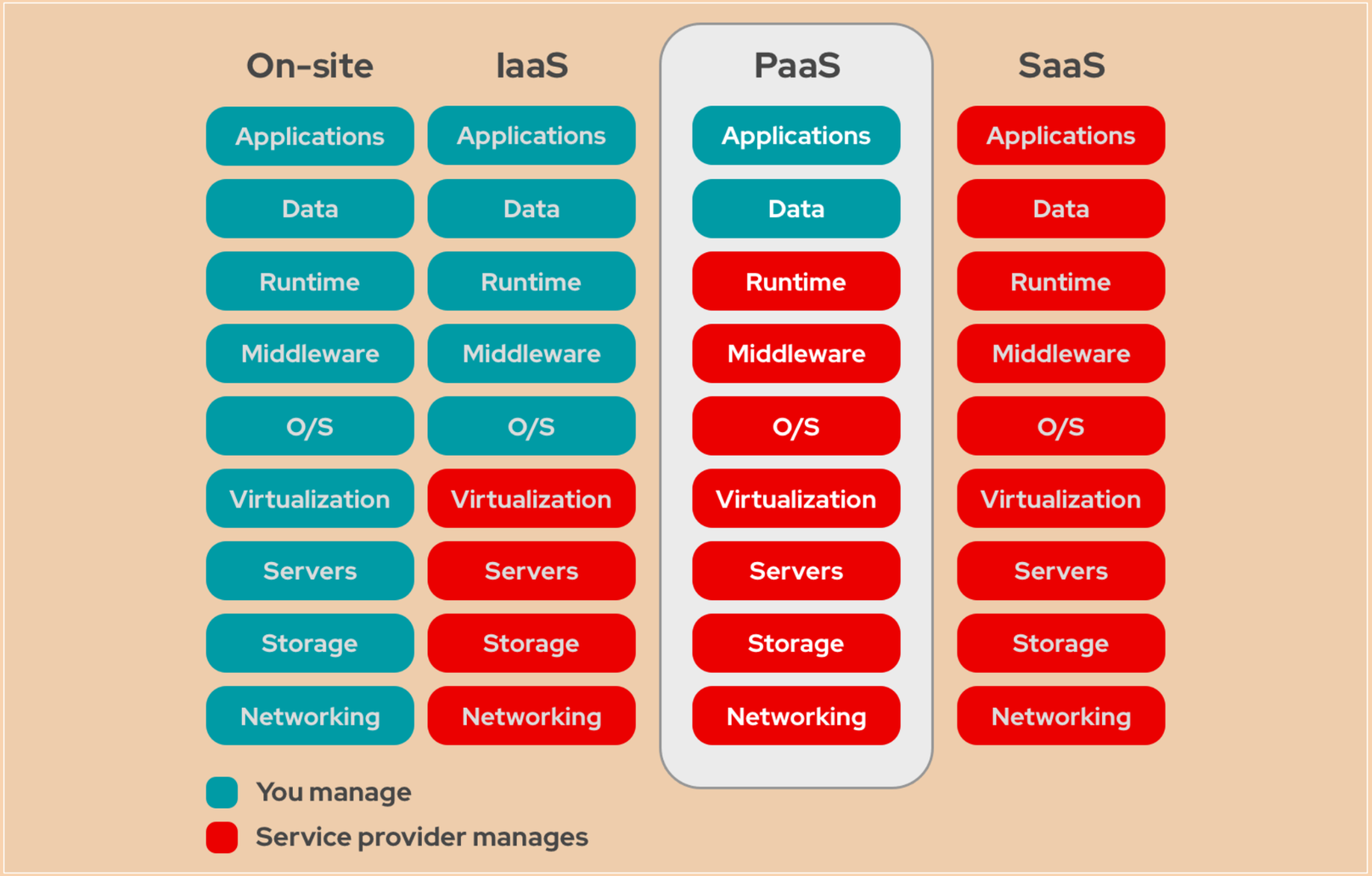
Google App Engine - Scaling

- **Automatisch:** Lastbasiert für dauernd laufende Services
  - Nach CPU-Auslastung, Target Throughput und Max Concurrent Requests
  - Min und Max Instance Count kann konfiguriert werden
- **Basic:** Instanzen werden nur bei Anfragen angelegt
  - Instanzen werden heruntergefahren, wenn keine Requests eingehen
  - Nicht für Flexible Environment verfügbar
  - Max Instances und Idle Timeout konfigurierbar
  - De-Facto-Serverless
- **Manual:** Skalieren via API oder Konsole

Google App Engine



Google App Engine



Demo: Google App Engine

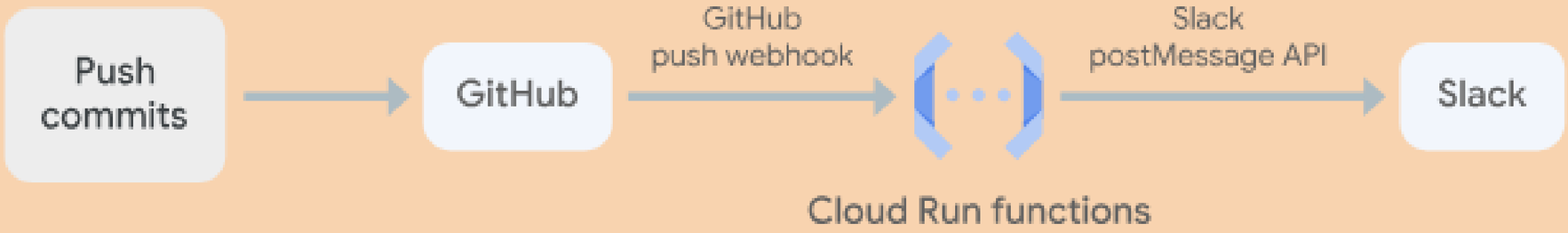
Cloud Run Functions

Serverless Computing in Google Cloud Platform

- Function as a Service
- Eventbasierte Codeausführung
    - z.B. neues Objekt in Cloud Storage
    - oder neue Nachricht in Pub/Sub
- Nutzungsbasierte Abrechnung
    - Anzahl Aufrufe
    - Konsumierte CPU-Zeit
    - Reservierter Speicher
- Ausführungszeit maximal 60 Minuten (mit Default von 1 Minute)

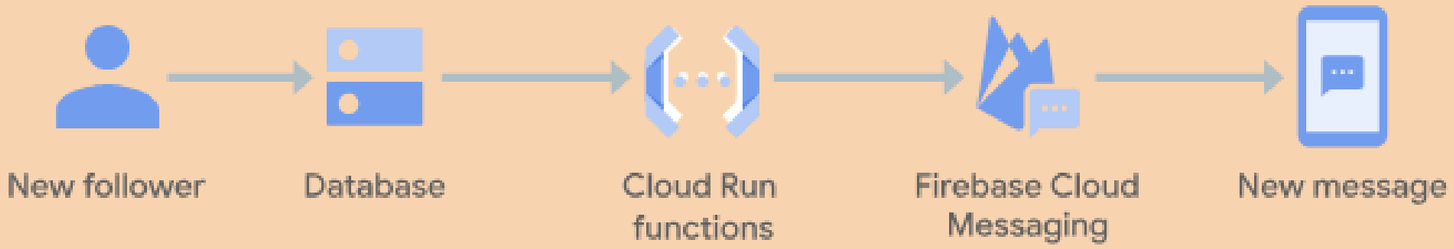
Use Cases

Slack WebHook für neue Commits in GitHub

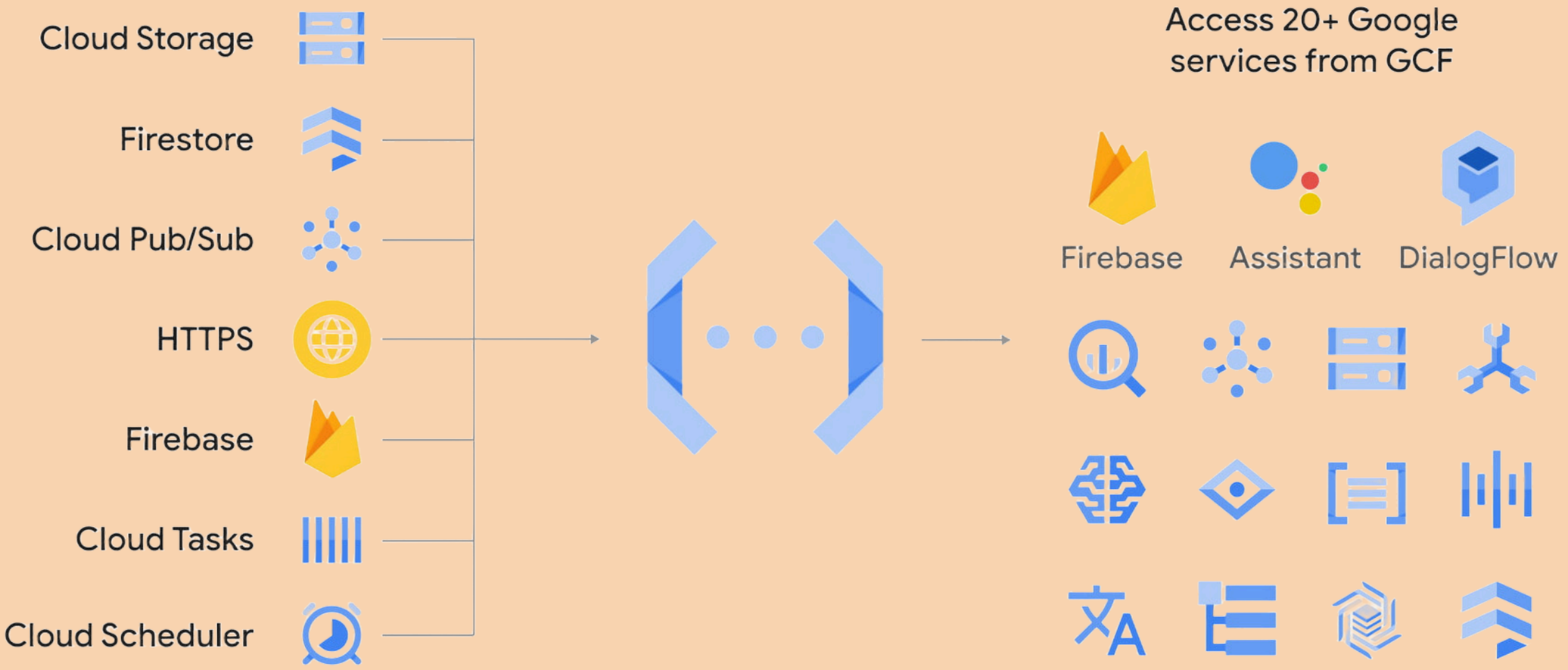


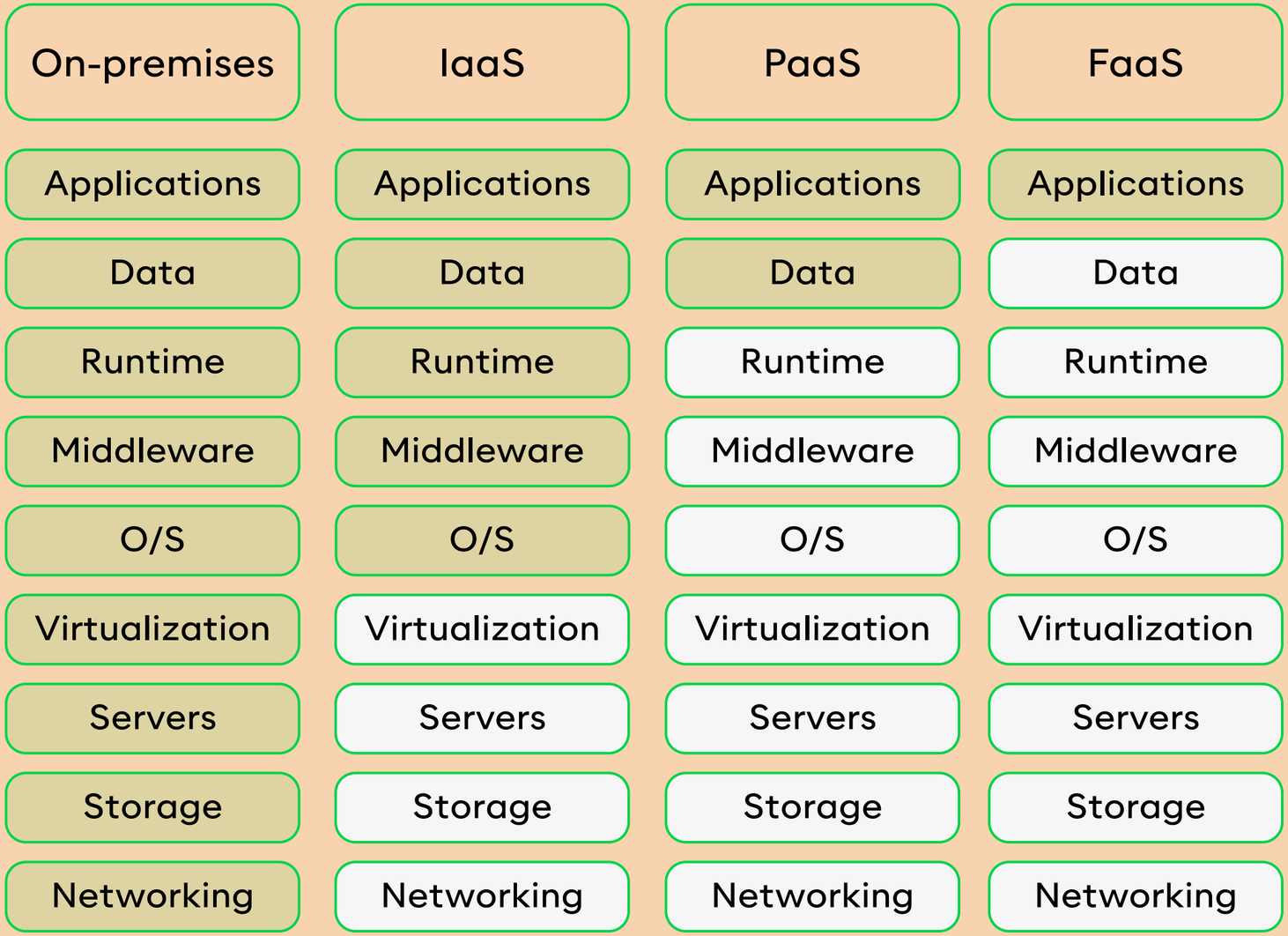
Use Cases

Event Notification für Mobile Apps



Cloud Functions: the glue that connects cloud services

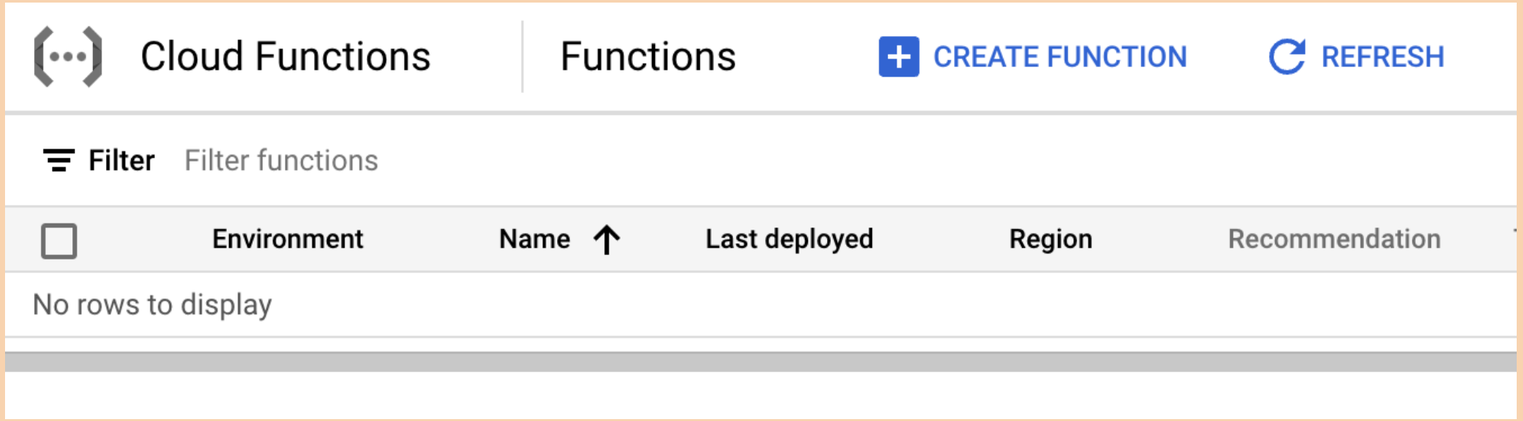



On-premises
IaaS
PaaS
FaaS
Applications
Applications
Applications
Applications
Data
Data
Data
Data
Runtime
Runtime
Runtime
Runtime
Middleware
Middleware
Middleware
Middleware
O/S
O/S
O/S
O/S
Virtualization
Virtualization
Virtualization
Virtualization
Servers
Servers
Servers
Servers
Storage
Storage
Storage
Storage
Networking
Networking
Networking
Networking

Demo: Google Cloud Functions

APIs aktivieren

https://console.cloud.google.com/flows/enableapi?apiid=cloudfunctions,cloudbuild.googleapis.com,artifactregistry.googleapis.com,run.googleapis.com,logging.googleapis.com,pubsub.googleapis.com&redirect=https://cloud.google.com/functions/docs/console-quickstart&_ga=2.53724334.784773541.1719565355-160061942.1716540050



Basics

Environment
2nd gen

Function name *
function-1

[redacted]

Trigger

Trigger type
HTTPS

URL

https://europe-west1-gfu-s3493-apr-2024.cloudfunctions.net/function-1

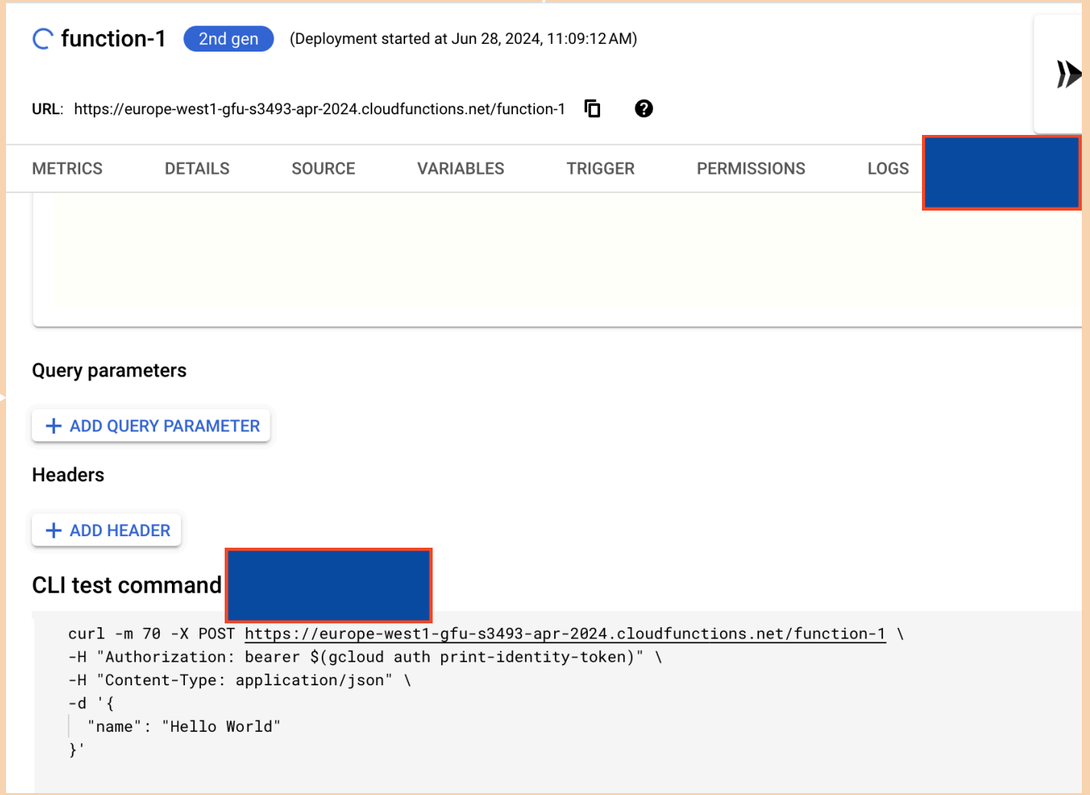
Authentication

Allow unauthenticated invocations
Check this if you are creating a public API or website.

[redacted]

Leave Default Function

Change Function and re-test



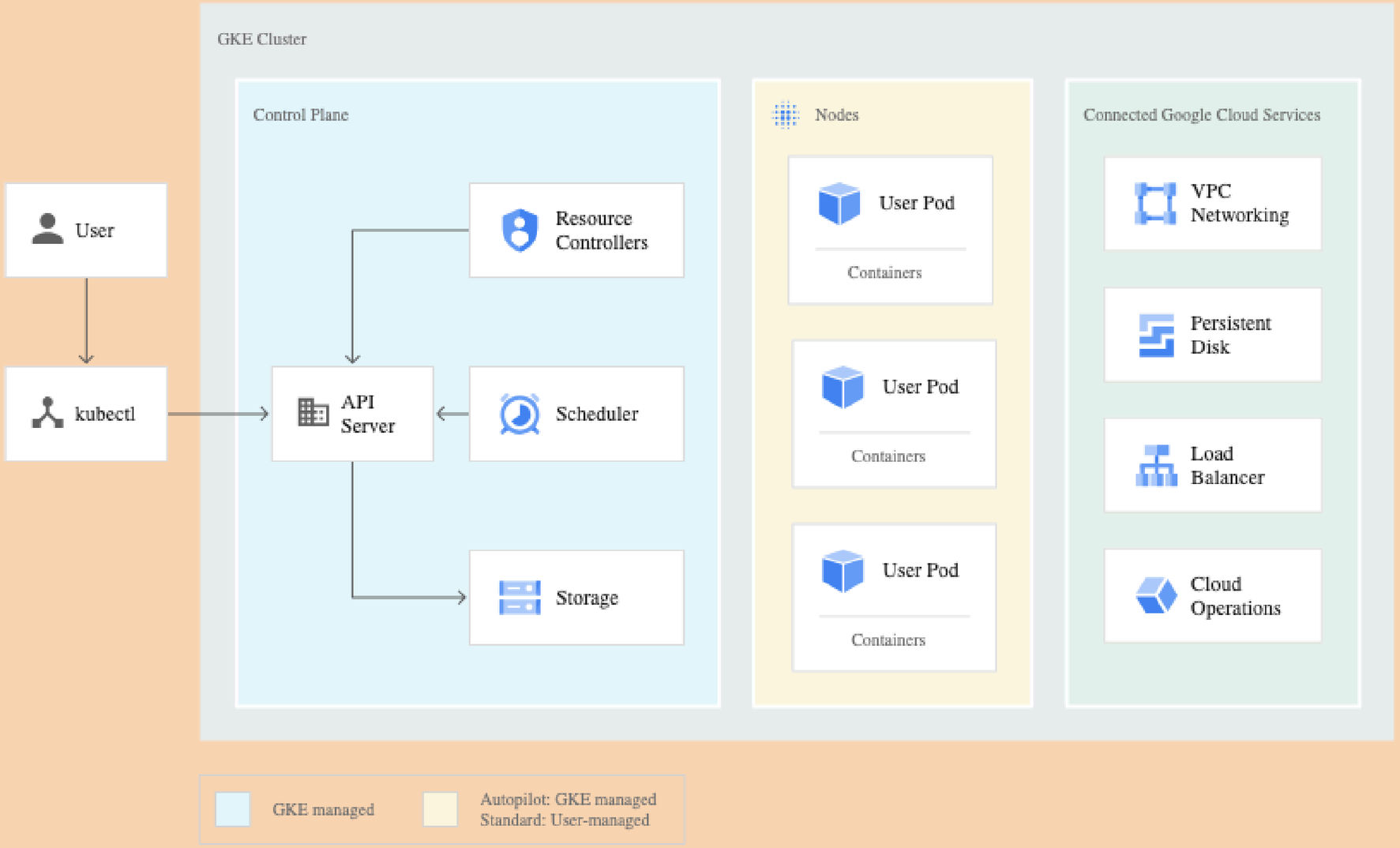
Aufgabe: Google Cloud Functions

Kubernetes Engine

Google Kubernetes Engine

- Vollständig verwaltete Kubernetes-Plattform auf Google Cloud
- Automatisierte Cluster-Erstellung, Upgrades, Skalierung und Reparatur
- Native Integration mit GCP-Diensten (Cloud Load Balancing, IAM, Cloud Monitoring)
- Unterstützt sowohl **Standard-** als auch **Autopilot-Modus**
- Ideal für containerisierte Anwendungen mit hoher Verfügbarkeit und Portabilität

Google Kubernetes Engine



Cloud Storage

Google Cloud Storage Basics

- Flexibler und günstiger Cloud-Speicher
- Speicher mit Key-Value-Ansatz
    - Dateien ("Objekte") sind Einheiten mit einem Schlüssel
    - Daher auch "Objektspeicher" genannt
- Gegensatz zu Blockspeicher ("Volumes")
- REST-API und SDKs verfügbar
- Unterstützt alle Dateitypen und viele Use-Cases
    - Textdateien
    - Medien
    - Archive und Backups

Google Cloud Storage Basics

- Objekte werden in Buckets gespeichert
    - Bucket-Namen sind **global unique – für alle Kunden**
    - Bucket-Namen müssen URL-kompatibel sein
    - 3-63 Zeichen
- Ein Bucket kann (nahezu) unendlich viele Objekte halten
- Keys in einem Bucket sind unique
- Maximale Objektgröße: 5TB

Google Cloud Storage
Storage Classes

Verschiedene Arten von Objekten – unterschiedliche Anforderungen an Verfügbarkeit und Zugriffsmustern

Speicherklasse	Name für APIs und Befehlszeilen	Mindestspeicherdauer	Abrufgebühren	Typische monatliche Verfügbarkeit[1]
Standard Storage	`STANDARD`	–	–	• > 99,99 % in Mehrfachregionen und Dual-Regionen • 99,99 % in Regionen
Nearline Storage	`NEARLINE`	30 Tage	Ja	• 99,95 % in Mehrfachregionen und Dual-Regionen • 99,9 % in Regionen
Coldline Storage	`COLDLINE`	90 Tage	Ja	• 99,95 % in Mehrfachregionen und Dual-Regionen • 99,9 % in Regionen
Archive Storage	`ARCHIVE`	365 Tage	Ja	• 99,95 % in Mehrfachregionen und Dual-Regionen • 99,9 % in Regionen

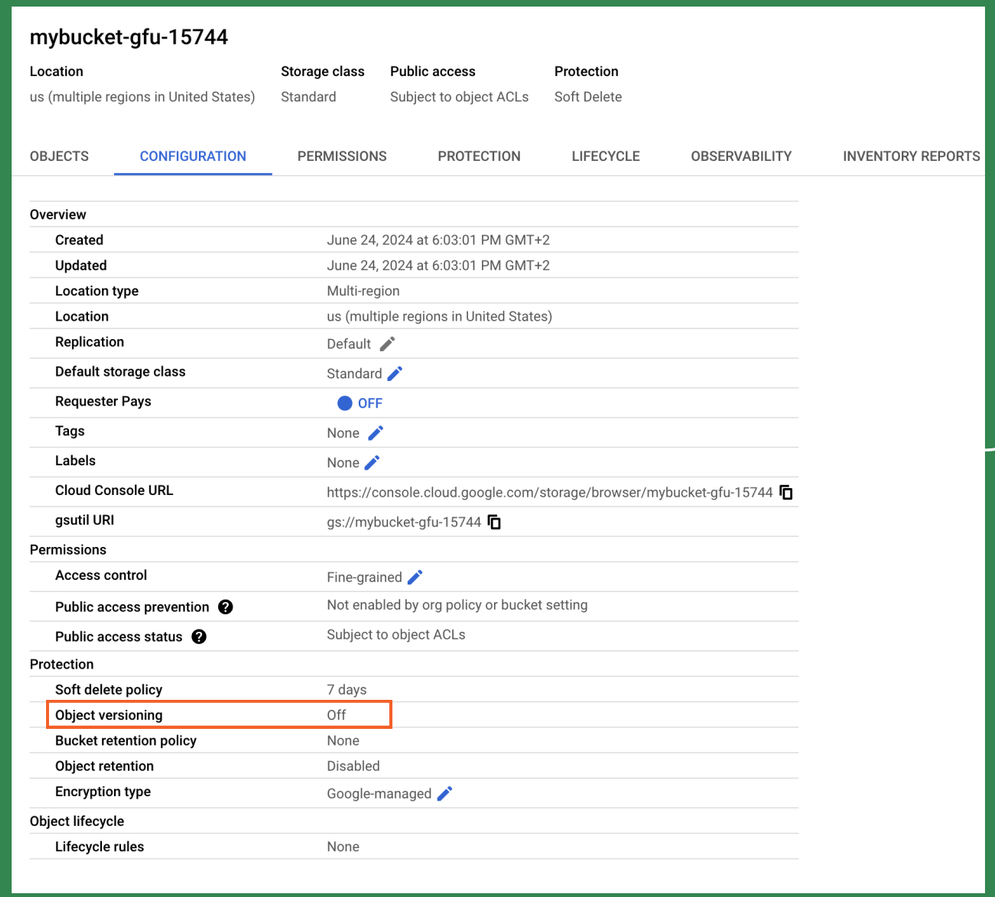
cloud.google.com

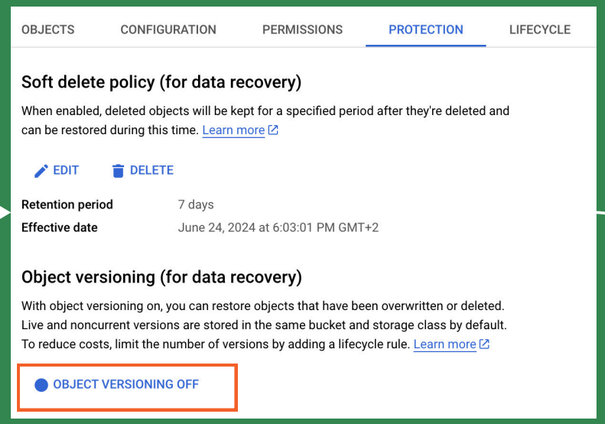
Speicherklassen | Cloud Storage | Google Cloud

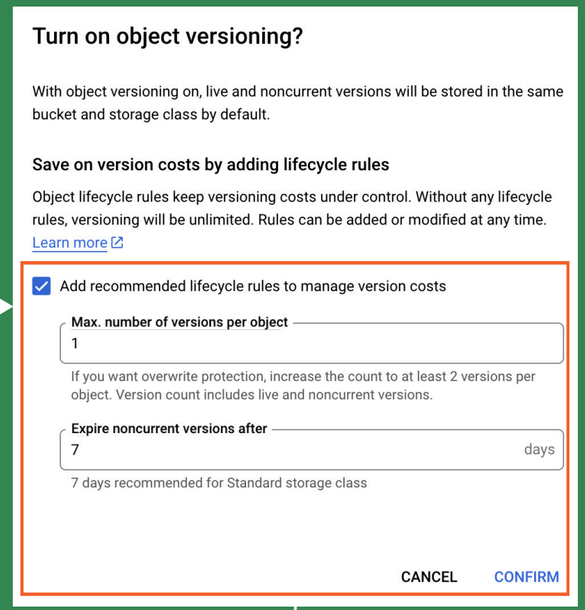
Auf dieser Seite werden das Konzept der Speicherklasse und die Unterschiede zwischen verschiedenen Speicherklassen erklärt. Eine Speicherklasse ist ein Metadatenelement, das von jedem Objekt verwendet wird. Welche Speicherklasse für ein Objekt festgeleg...

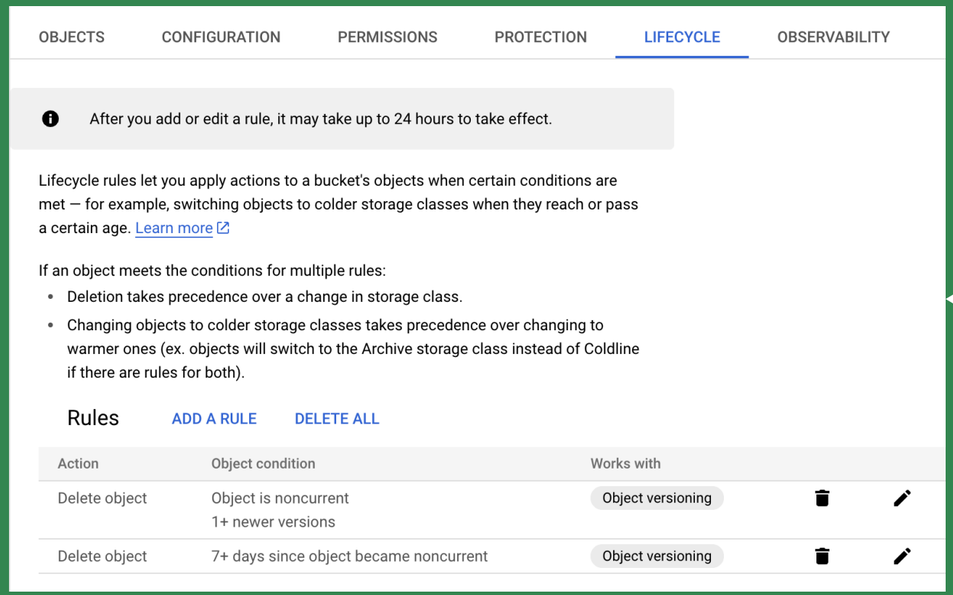
Google Cloud Storage
Versioning

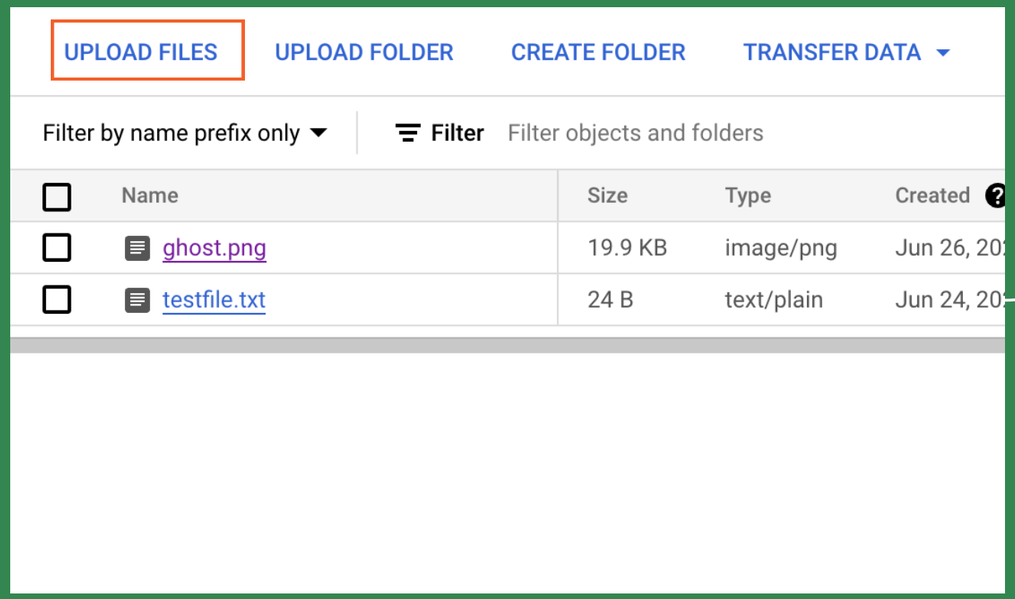
- Wird auf Bucket-Ebene aktiviert/deaktiviert
- *Live Version* ist die neuste Version
- Ältere Versionen werden mit einer Generation Number gekennzeichnet
- Kosten sparen: ältere Versionen löschen

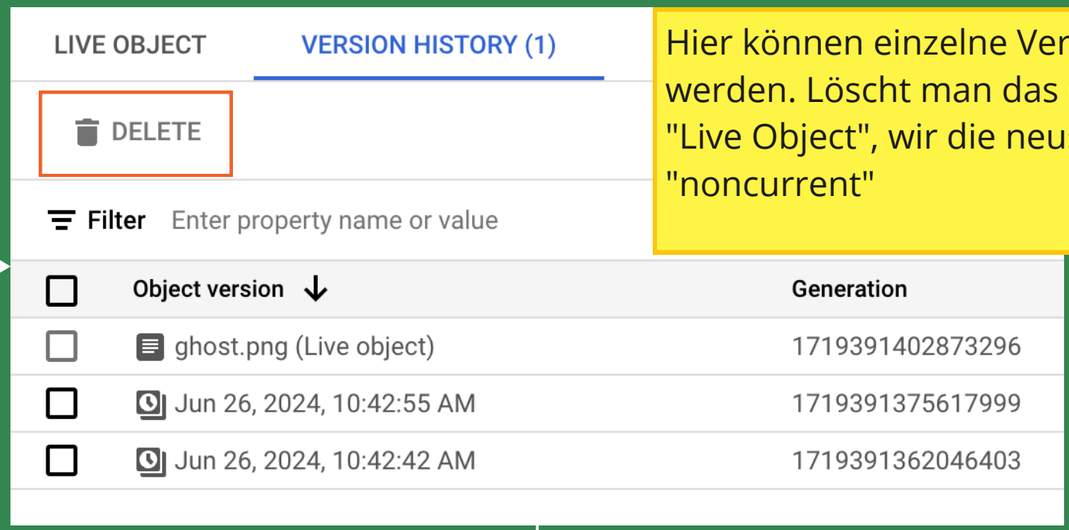

mybucket-gfu-15744
Location
us (multiple regions in United States)
Storage class
Standard
Public access
Subject to object ACLs
Protection
Soft Delete
OBJECTS
CONFIGURATION
PERMISSIONS
PROTECTION
LIFECYCLE
OBSERVABILITY
INVENTORY REPORTS
Overview
Created
June 24, 2024 at 6:03:01 PM GMT+2
Updated
June 24, 2024 at 6:03:01 PM GMT+2
Location type
Multi-region
Location
us (multiple regions in United States)
Replication
Default
Default storage class
Standard
Requester Pays
OFF
Tags
None
Labels
None
Cloud Console URL
https://console.cloud.google.com/storage/browser/mybucket-gfu-15744
gsutil URI
gs://mybucket-gfu-15744
Permissions
Access control
Fine-grained
Public access prevention
Not enabled by org policy or bucket setting
Public access status
Subject to object ACLs
Protection
Soft delete policy
7 days
Object versioning
Off
Bucket retention policy
None
Object retention
Disabled
Encryption type
Google-managed
Object lifecycle
Lifecycle rules
None


OBJECTS
CONFIGURATION
PERMISSIONS
PROTECTION
LIFECYCLE
Soft delete policy (for data recovery)
When enabled, deleted objects will be kept for a specified period after they're deleted and can be restored during this time. Learn more
EDIT
DELETE
Retention period
7 days
Effective date
June 24, 2024 at 6:03:01 PM GMT+2
Object versioning (for data recovery)
With object versioning on, you can restore objects that have been overwritten or deleted. Live and noncurrent versions are stored in the same bucket and storage class by default. To reduce costs, limit the number of versions by adding a lifecycle rule. Learn more
OBJECT VERSIONING OFF

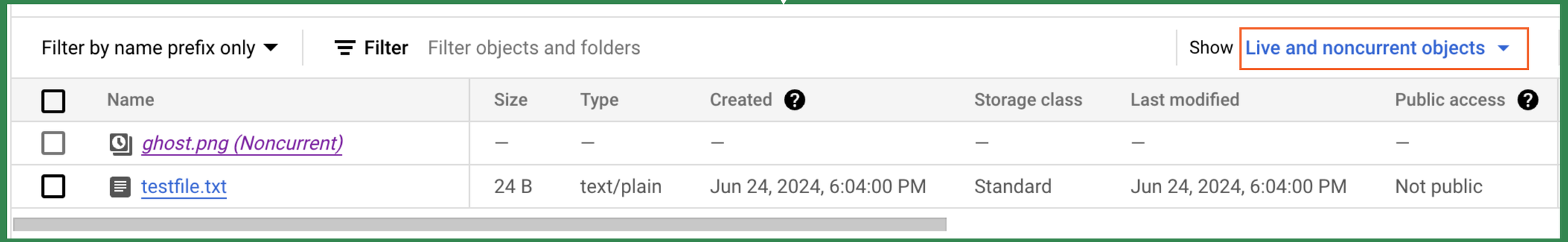

Turn on object versioning?
With object versioning on, live and noncurrent versions will be stored in the same bucket and storage class by default.
Save on version costs by adding lifecycle rules
Object lifecycle rules keep versioning costs under control. Without any lifecycle rules, versioning will be unlimited. Rules can be added or modified at any time.
Learn more
Add recommended lifecycle rules to manage version costs
Max. number of versions per object
1
If you want overwrite protection, increase the count to at least 2 versions per object. Version count includes live and noncurrent versions.
Expire noncurrent versions after
7
days
7 days recommended for Standard storage class
CANCEL
CONFIRM


OBJECTS
CONFIGURATION
PERMISSIONS
PROTECTION
LIFECYCLE
OBSERVABILITY
After you add or edit a rule, it may take up to 24 hours to take effect.
Lifecycle rules let you apply actions to a bucket's objects when certain conditions are met — for example, switching objects to colder storage classes when they reach or pass a certain age. Learn more
If an object meets the conditions for multiple rules:
Deletion takes precedence over a change in storage class.
Changing objects to colder storage classes takes precedence over changing to warmer ones (ex. objects will switch to the Archive storage class instead of Coldline if there are rules for both).
Rules
ADD A RULE
DELETE ALL
Action
Object condition
Works with
Delete object
Object is noncurrent
1+ newer versions
Object versioning
Delete object
7+ days since object became noncurrent
Object versioning





Hier können einzelne Versionen gelöscht werden. Löscht man das Object unter "Live Object", wir die neuste Version "noncurrent"



Ein Objekt ist endgültig gelöscht, wenn *alle* noncurrent Versions gelöscht sind

Google Cloud Storage
Lifecycle Management

- Objekte können regelbasiert gelöscht oder in andere Klassen verschoben werden
- Das spart Kosten
- Verfügbare Filter: Age, CreatedBefore, IsLive, MatchesStorageClass...
- Es gibt zwei Aktionen: SetStorageClass und Delete

Google Cloud Storage Lifecycle Management

```
alex@cloudshell:~ (gfu-s3493-apr-2024)$ gsutil lifecycle get gs://mybucket-gfu-15744 | jq
{
  "rule": [
    {
      "action": {
        "type": "Delete"
      },
      "condition": {
        "isLive": false,
        "numNewerVersions": 1
      }
    },
    {
      "action": {
        "type": "Delete"
      },
      "condition": {
        "daysSinceNoncurrentTime": 7
      }
    }
  ]
}
```

Diese Regel sorgt dafür, dass ältere Versionen von Objekten nach 7 Tagen gelöscht werden, sofern es eine neuere Version gibt. Das bedeutet, dass immer nur die aktuellste Version eines Objekts im Bucket gespeichert wird.

--> Die Regel werden logisch verUNDet

```
{
  "rule": [
    {
      "action": {
        "type": "SetStorageClass",
        "storageClass": "NEARLINE"
      },
      "condition": {
        "age": 30,
        "isLive": true
      }
    }
  ]
}
```

Diese Regel sorgt dafür, dass das Live Object nach 30 Tagen in die billigere NEARLINE-Storage-Klasse verschoben wird.

Nearline Storage: Nearline Storage ist eine kostengünstige Option für Daten, die nicht häufig benötigt werden, aber innerhalb weniger Stunden wieder verfügbar sein müssen.
Coldline Storage: Coldline Storage ist die günstigste Option für Daten, die selten benötigt werden und mit einer Wiederherstellungsdauer von einigen Tagen auskommen.

```
alex@cloudshell:~ (gfu-s3493-apr-2024)$ vim rule.json
alex@cloudshell:~ (gfu-s3493-apr-2024)$ gsutil lifecycle set rule.json gs://mybucket-gfu-15744
Setting lifecycle configuration on gs://mybucket-gfu-15744/...
alex@cloudshell:~ (gfu-s3493-apr-2024)$ gsutil lifecycle get gs://mybucket-gfu-15744 | jq
{
  "rule": [
    {
      "action": {
        "storageClass": "NEARLINE",
        "type": "SetStorageClass"
      },
      "condition": {
        "age": 30,
        "isLive": true
      }
    }
  ]
}
alex@cloudshell:~ (gfu-s3493-apr-2024)$
```

Google Cloud Storage Encryption

- Dateien werden auf der Serverseite immer verschlüsselt gespeichert
- Konfigurierbar
    - Google-Managed Key
    - Customer Managed Key
- Client-Side Encryption zusätzlich möglich

Google Cloud Storage Encryption

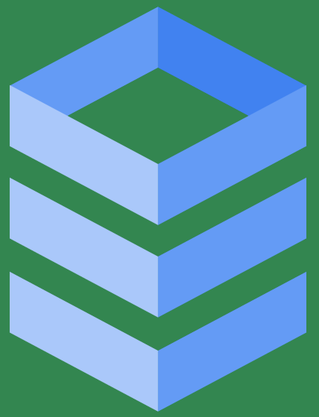
OBJECTS | CONFIGURATION | PERMISSIONS | PROTECTION | LIFECYCLE | OBSERVABILITY

Overview	
Created	June 24, 2024 at 6:03:01 PM GMT+2
Updated	June 26, 2024 at 10:54:50 AM GMT+2
Location type	Multi-region
Location	us (multiple regions in United States)
Replication	Default
Default storage class	Standard
Requester Pays	OFF
Tags	None
Labels	None
Cloud Console URL	https://console.cloud.google.com/storage/browser/mybucket-gfu-15744
gsutil URI	gs://mybucket-gfu-15744
Permissions	
Access control	Fine-grained
Public access prevention	Not enabled by org policy or bucket setting
Public access status	Subject to object ACLs
Protection	
Soft delete policy	7 days
Object versioning	On
Bucket retention policy	None
Object retention	Disabled
Encryption type	Google-managed
Object lifecycle	
Lifecycle rules	1 rule

Aufgabe: Google Cloud Storage

CLOUD SQL

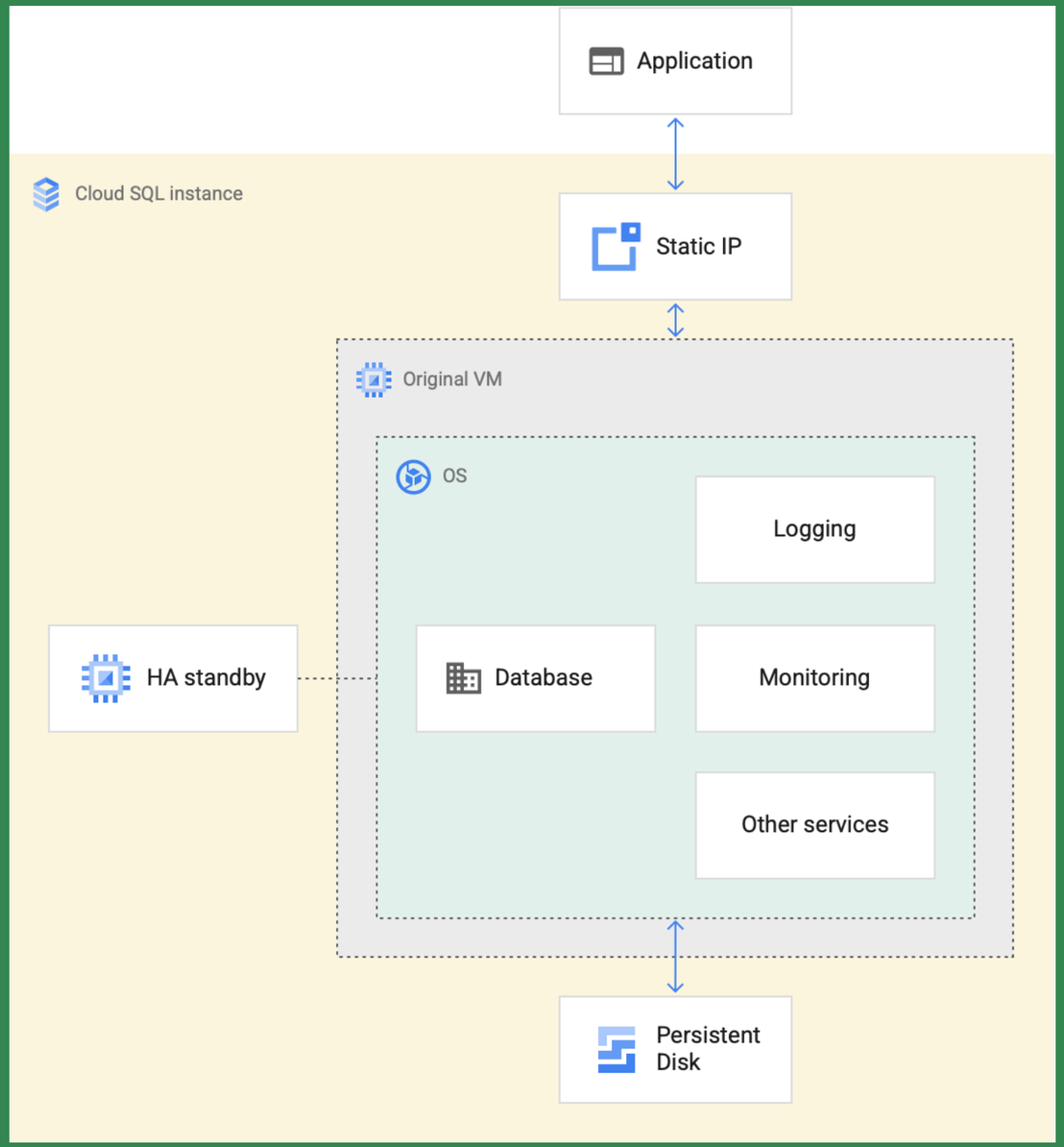
Google Cloud SQL
Basics



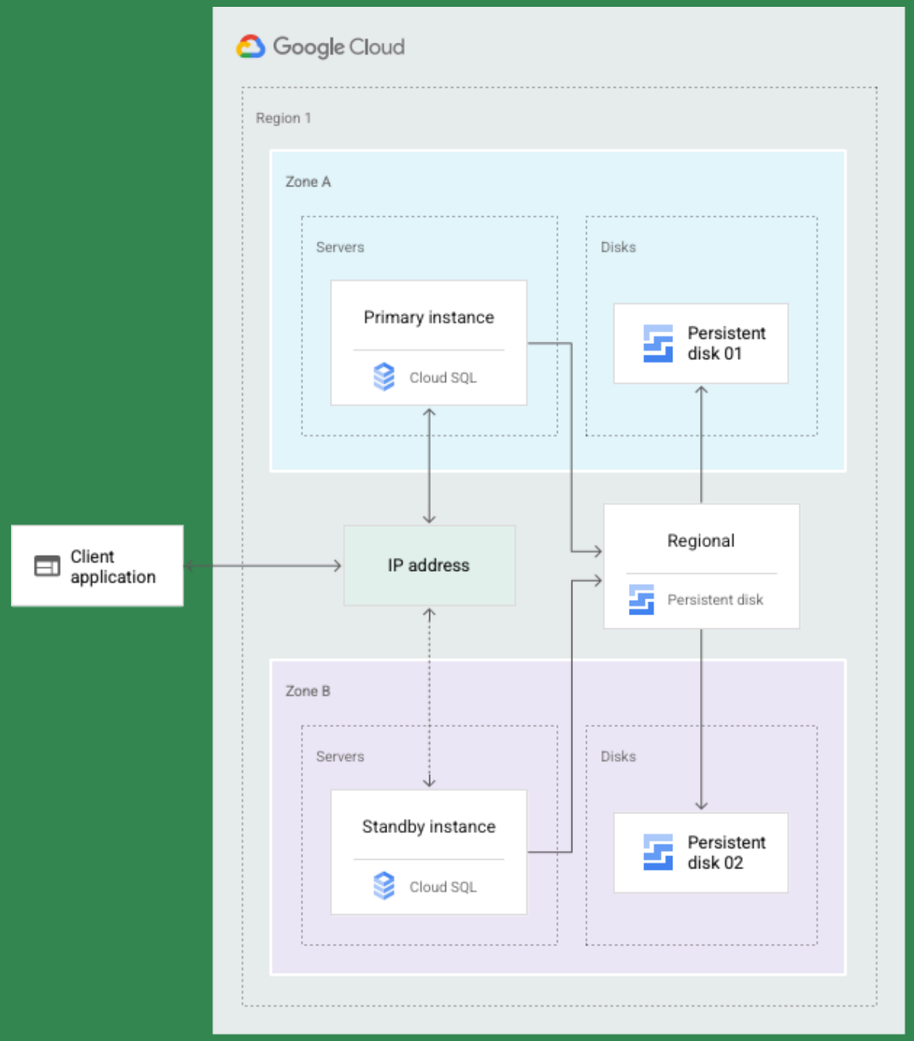
- Vollständig verwalteter relationaler Datenbankdienst
    - Keine Verwaltung der Datenbank nötig
    - Für MySQL, PostgreSQL und SQL Server
    - Regionaler Dienst mit 99.95% Uptime-SLA
    - Wahl zwischen SSD und HDD
    - Bis zu 416 GB RAM und 30 TB Storage
- Sehr gut geeignet für bestehende Anwendungen, die nicht Cloud Native sind
- Typisches Ziel von Datenmigrationen

Google Cloud SQL Features

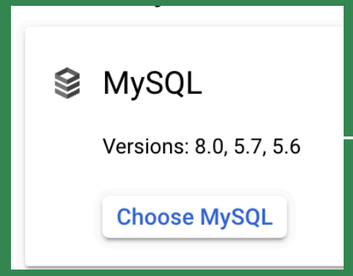
- Automatische Verschlüsselung, Maintenance und Backup
- HA und Failover
    - Standby-Instanz für automatisches Failover möglich
    - Dafür sind Backups und Binary Logging nötig
- Read Replicas
    - Cross-Zone, Cross-Region, External
    - Auch hier sind Backups und Binary Logging nötig
- Automatischer Storage-Increase ohne Downtime
- PIT Recovery bei Binary Logging

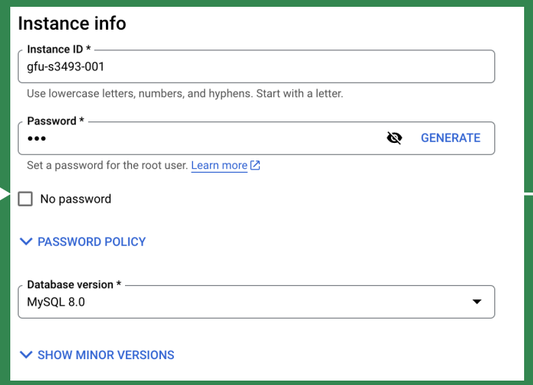


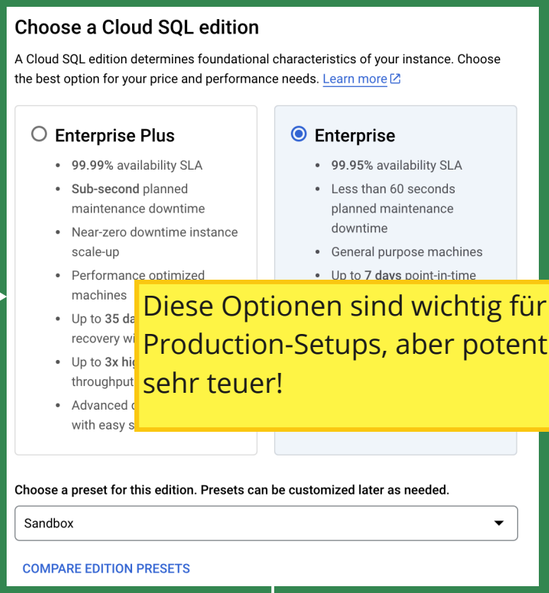
Google Cloud SQL
High Availability



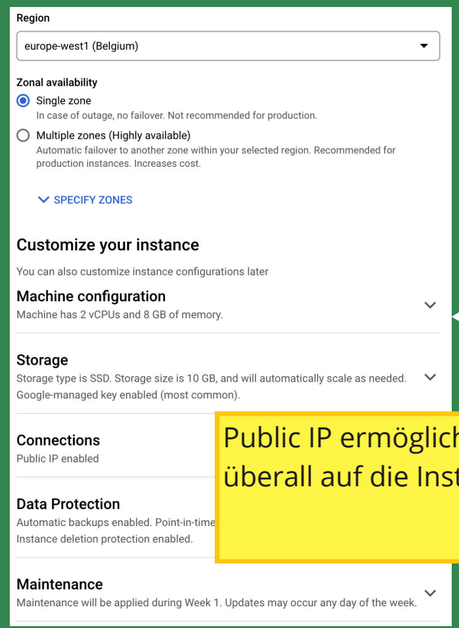
Demo: Cloud SQL







Diese Optionen sind wichtig für Production-Setups, aber potentiell sehr teuer!



Public IP ermöglicht es uns, von überall auf die Instanz zuzugreifen

Connections

Choose how you want your source to connect to this instance, then define which networks are authorized to connect. Learn more

You can use the Cloud SQL Proxy for extra security with either option. Learn more

Instance IP assignment

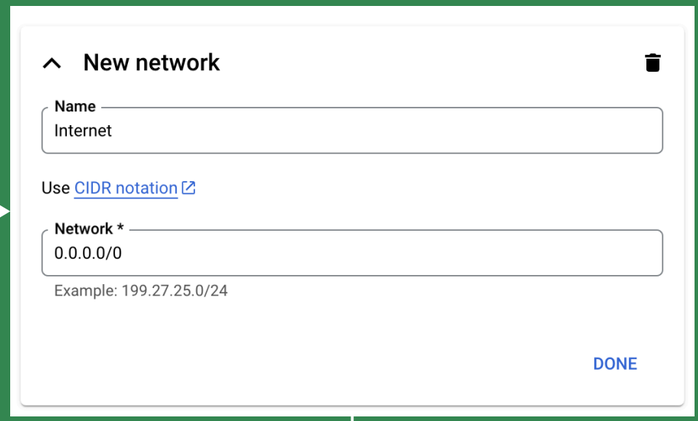
- [ ] Private IP
  Assigns an internal, Google-hosted VPC IP address. Requires additional APIs and permissions. Can't be disabled once enabled. Learn more
- [x] Public IP
  Assigns an external, internet-accessible IP address. Requires using an authorized network or the Cloud SQL Proxy to connect to this instance. Learn more

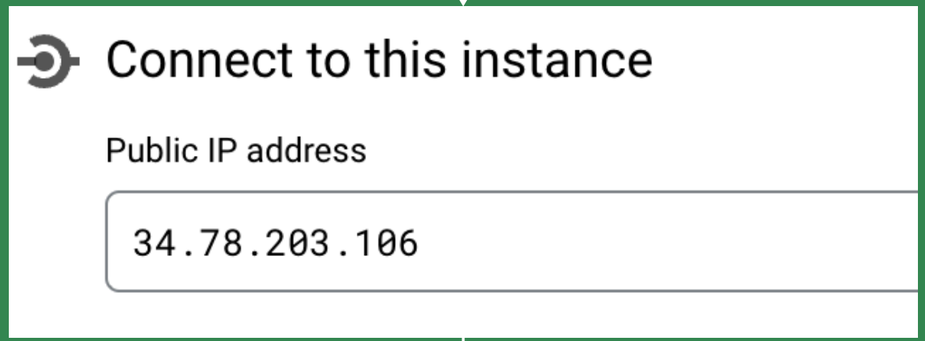
Authorized networks

You can specify CIDR ranges to allow IP addresses in those ranges to access your instance. Learn more

You have not authorized any external networks to connect to your Cloud SQL instance. External applications can still connect to the instance through the Cloud SQL Proxy. Learn more

ADD A NETWORK






```
alex@cloudshell:~ (gfu-s3493-apr-2024)$ mysql --host=34.78.203.106 --user=root --password=gfu
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 55
Server version: 8.0.31-google (Google)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

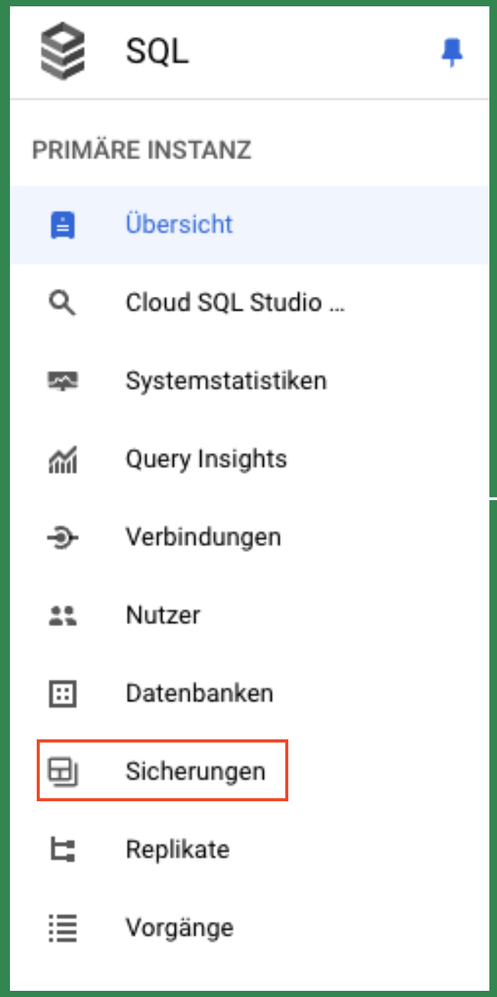
Google Cloud SQL Backups

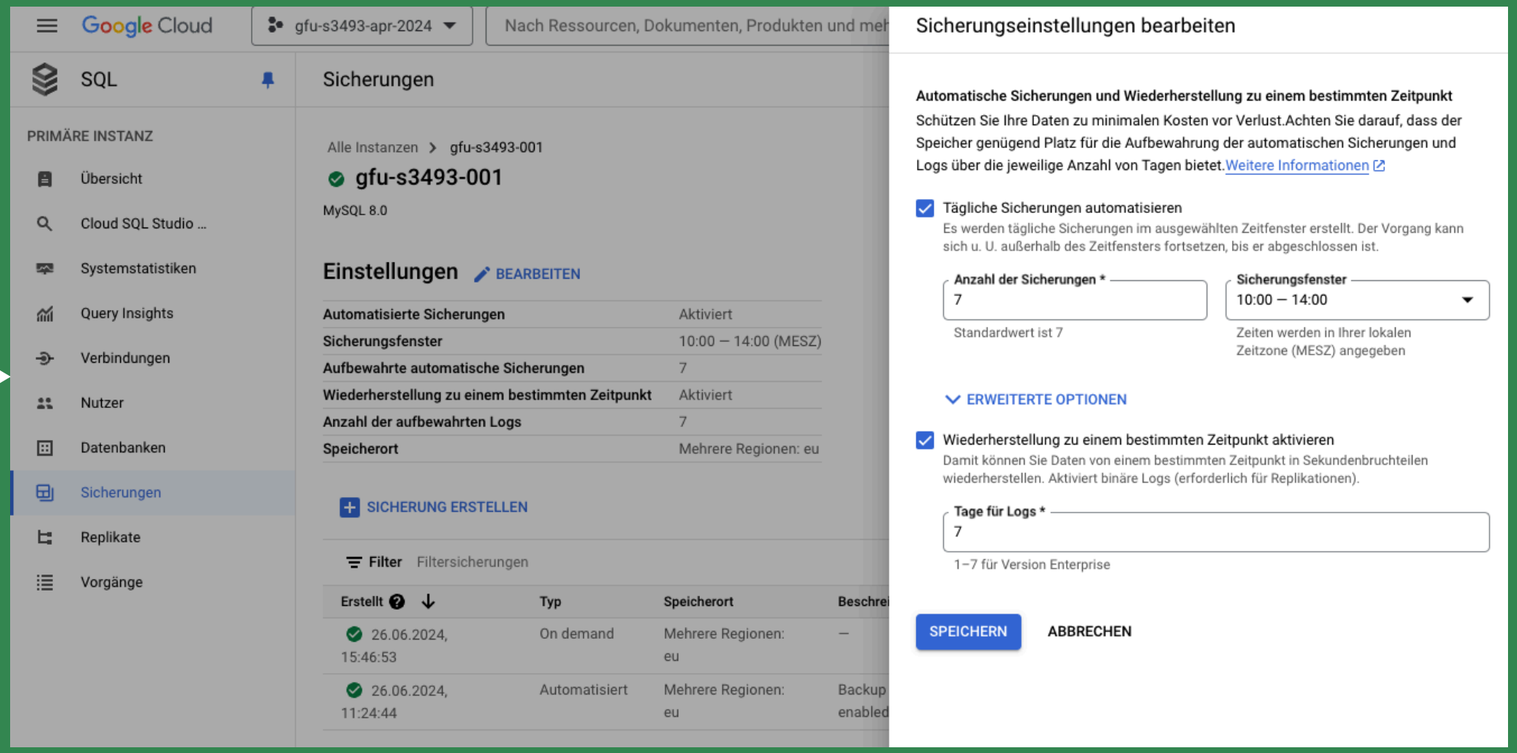
- Automatisierte Backups:
  - Google Cloud SQL bietet automatisierte Backups, die regelmäßig erstellt werden.
  - Diese Backups sind standardmäßig aktiviert und sichern die Datenbanken in regelmäßigen Abständen.
- Manuelle Backups:
  - Nutzer können auch manuelle Backups nach Bedarf erstellen.
  - Dies kann über die Google Cloud Console oder das gcloud-Tool durchgeführt werden.
- Punkt-in-Zeit-Wiederherstellung (PITR):
  - PITR ermöglicht es, die Datenbank zu einem spezifischen Zeitpunkt in der Vergangenheit wiederherzustellen.
  - Diese Funktion verwendet Binärprotokolle, um Änderungen zu speichern und bietet eine granularere Wiederherstellungsoption.

Google Cloud SQL Backups

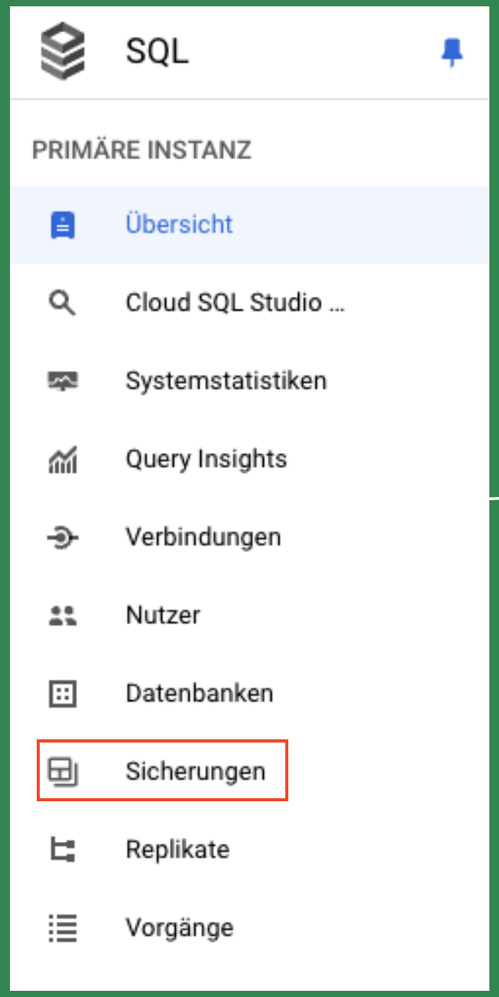
- Wiederherstellung von Backups:
  - Backups können einfach über die Google Cloud Console wiederhergestellt werden.
  - Es ist möglich, die Datenbank entweder auf demselben oder einem neuen Datenbank-Instance wiederherzustellen.
- Speicherung und Kosten:
  - Google Cloud SQL speichert die letzten 7 Backups für jede Datenbank-Instance.
  - Die Kosten für die Backups sind in den Gesamtkosten der Instanz enthalten.
- Sicherheitsaspekte:
  - Backups werden sicher gespeichert und können verschlüsselt werden, um den Datenschutz zu gewährleisten.
  - Zugriffskontrollen und Berechtigungen können konfiguriert werden, um sicherzustellen, dass nur autorisierte Nutzer Zugriff auf die Backup- und Wiederherstellungsfunktionen haben.

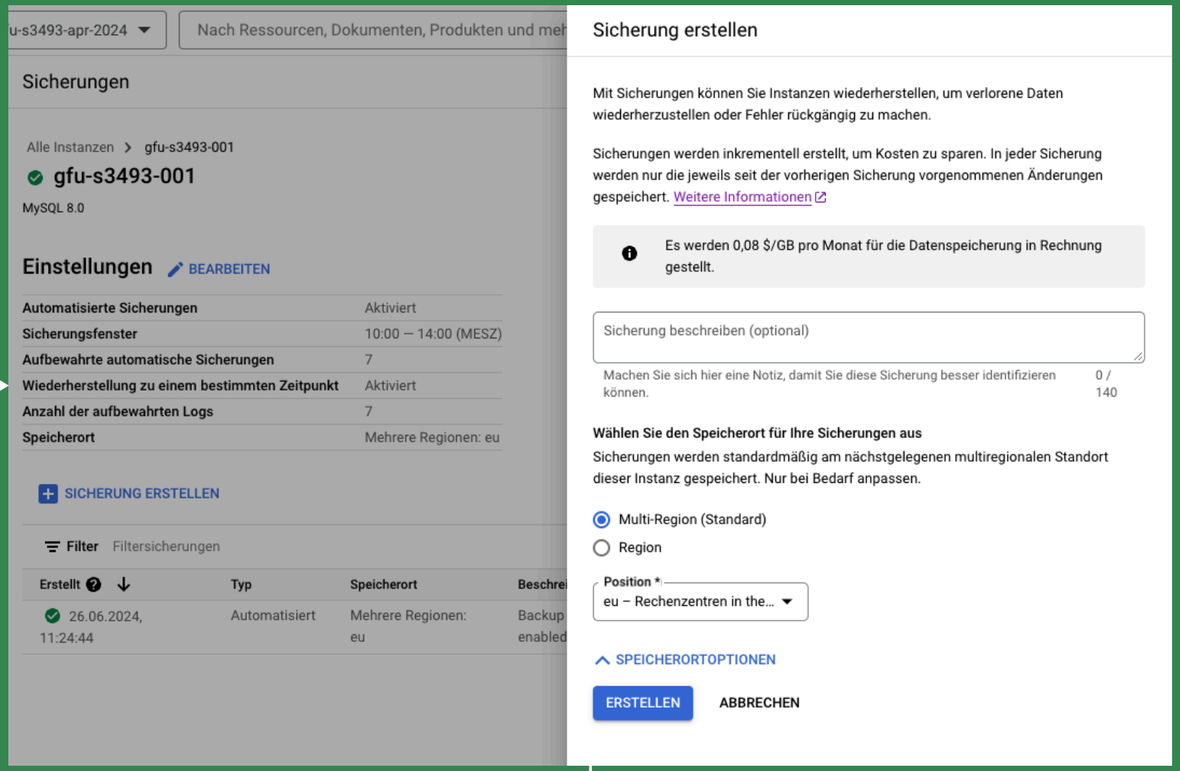
Google Cloud SQL Scheduled Backup

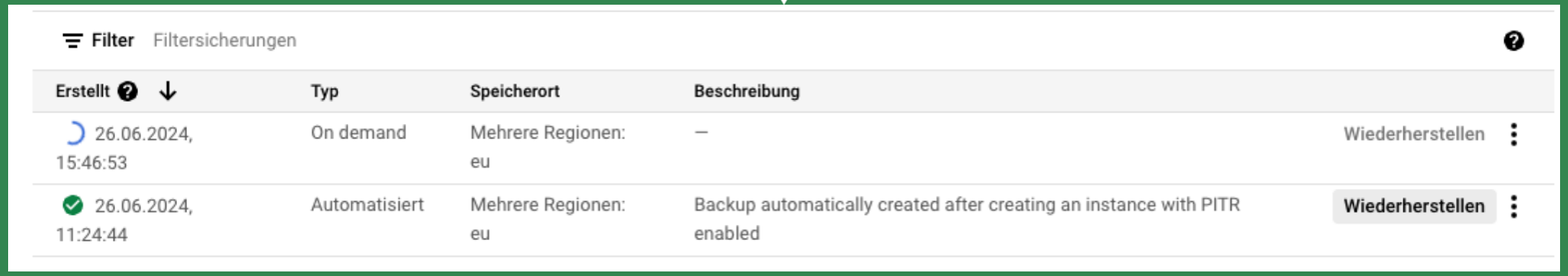




Google Cloud SQL
Manuelles Backup







Cloud Firestore

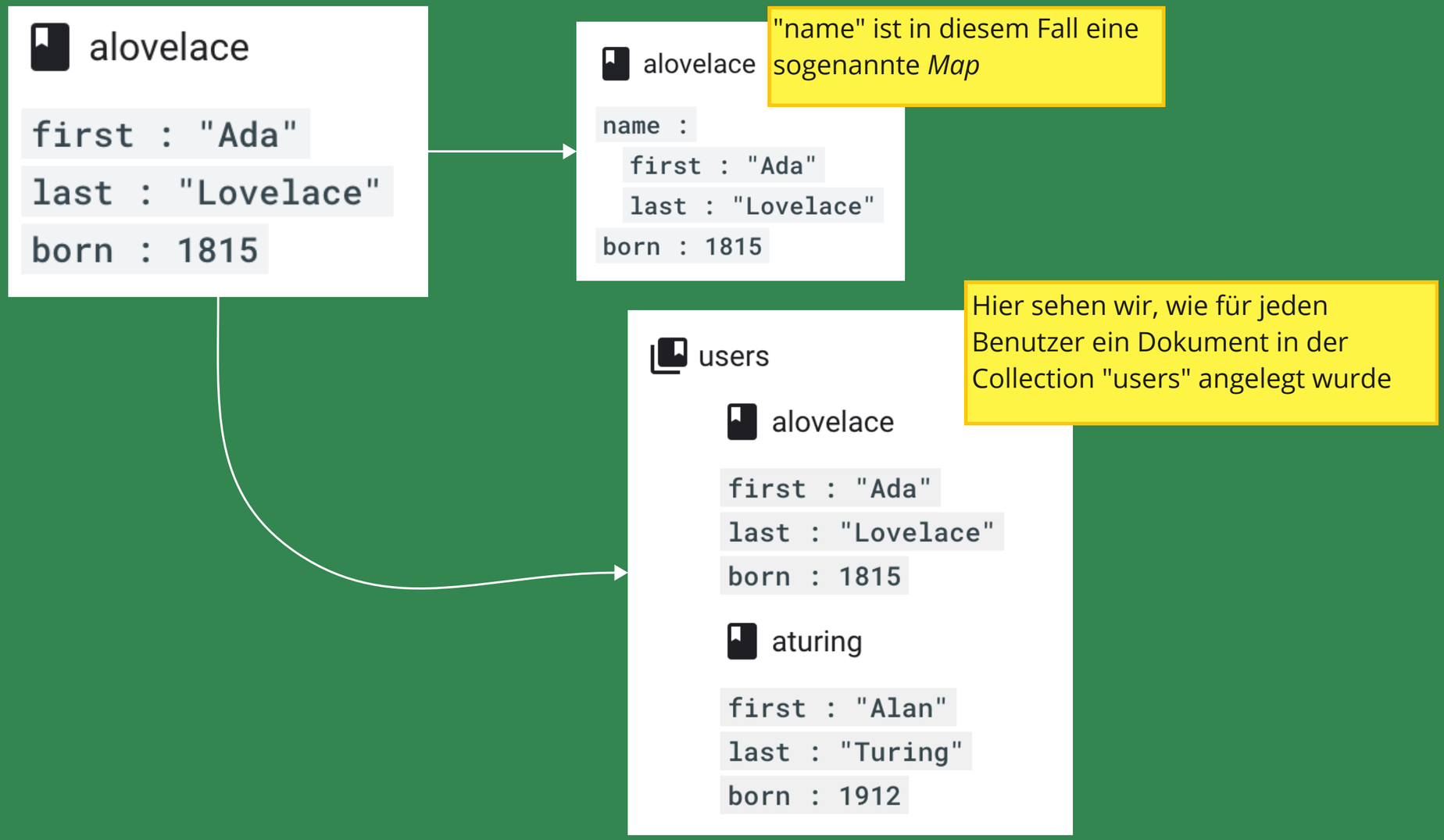
Cloud Firestore

- Firestore ist eine dokumentenorientierte NoSQL-Datenbank
- Voll verwaltet und serverless: Keine Basiskosten
- Integration in Firebase als Anwendungsframework
- SDKs für alle verbreitete Sprachen
- Support für verteilten Datenbanken z.B. für Offlinefähigkeit von Apps

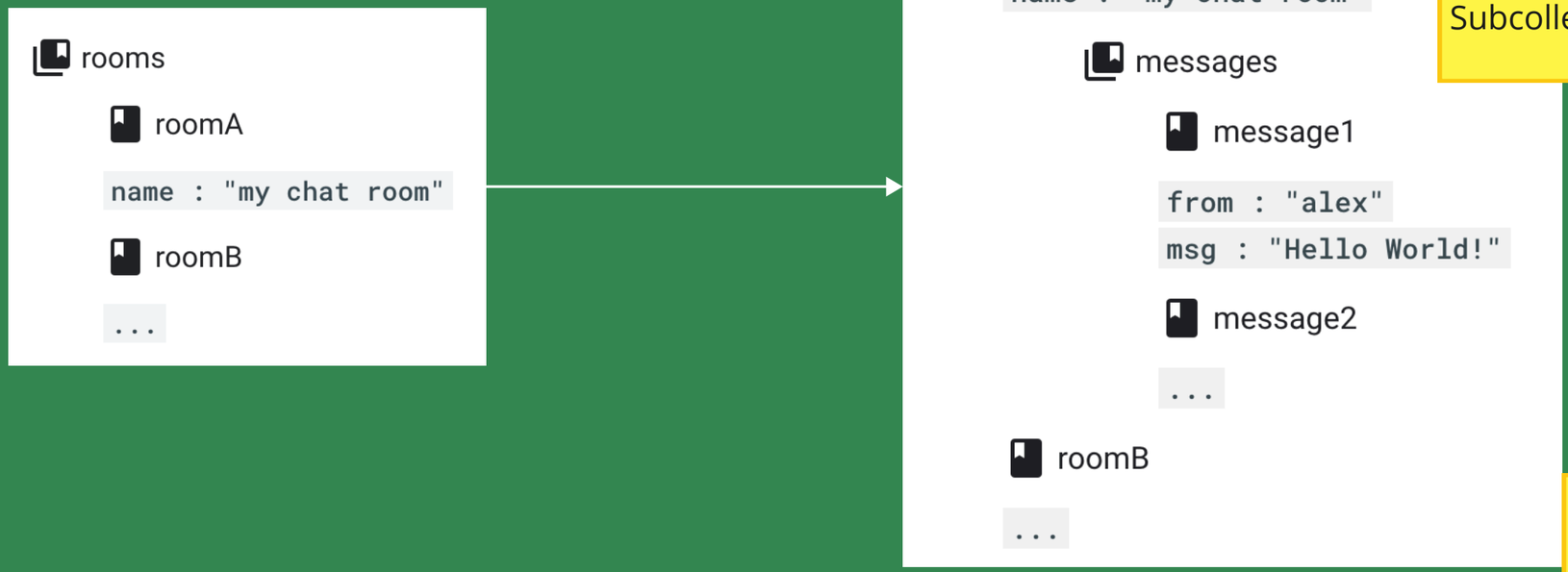
Cloud Firestore
Datenmodell

- Alle Dokumente werden in Sammlungen ("Collections") gespeichert
- Ein Dokument ist eine Reihe von Schlüssel-Wert-Paaren
- Diese Paare können auch hierarchisch sein
- Jedes Dokument hat eine ID
- Dokumente einer Sammlung können unterschiedliche Properties haben
- Ein Dokument kann selbst Sammlungen enthalten ("Subcollections")

Cloud Firestore
Datenmodell Beispiel



Cloud Firestore Subcollections



Jeder Raum ist ein Dokument der Collection "rooms" und enthält alle Nachrichten als Dokumente in der Subcollection "messages"

Dieses Konzept funktioniert gut, wenn man in der Anwendung aus einem Dokument heraus auf Detaildaten zugreifen will.
Es ist ineffizient, wenn man global Abfragen auf alle Daten in Subcollections machen will!

Cloud Firestore
Datentypen

- Alle üblichen Datentypen sind unterstützt
    - Array
    - Boolean
    - Byte
    - Date and Time
    - Float
    - Integer
    - Map
    - Null
    - String…

https://console.firebase.google.com/

Create a project

Let's start with a name for your project

Project name

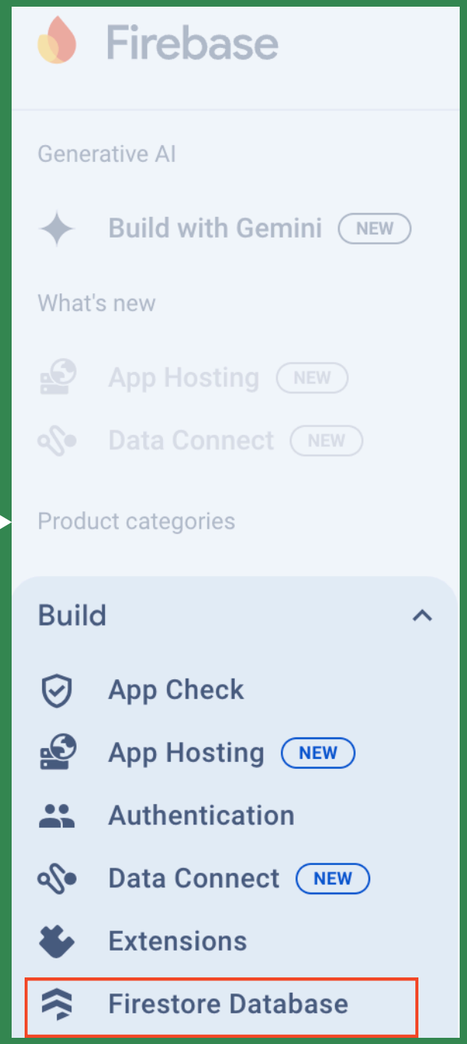
gfu-s3493-apr-2024

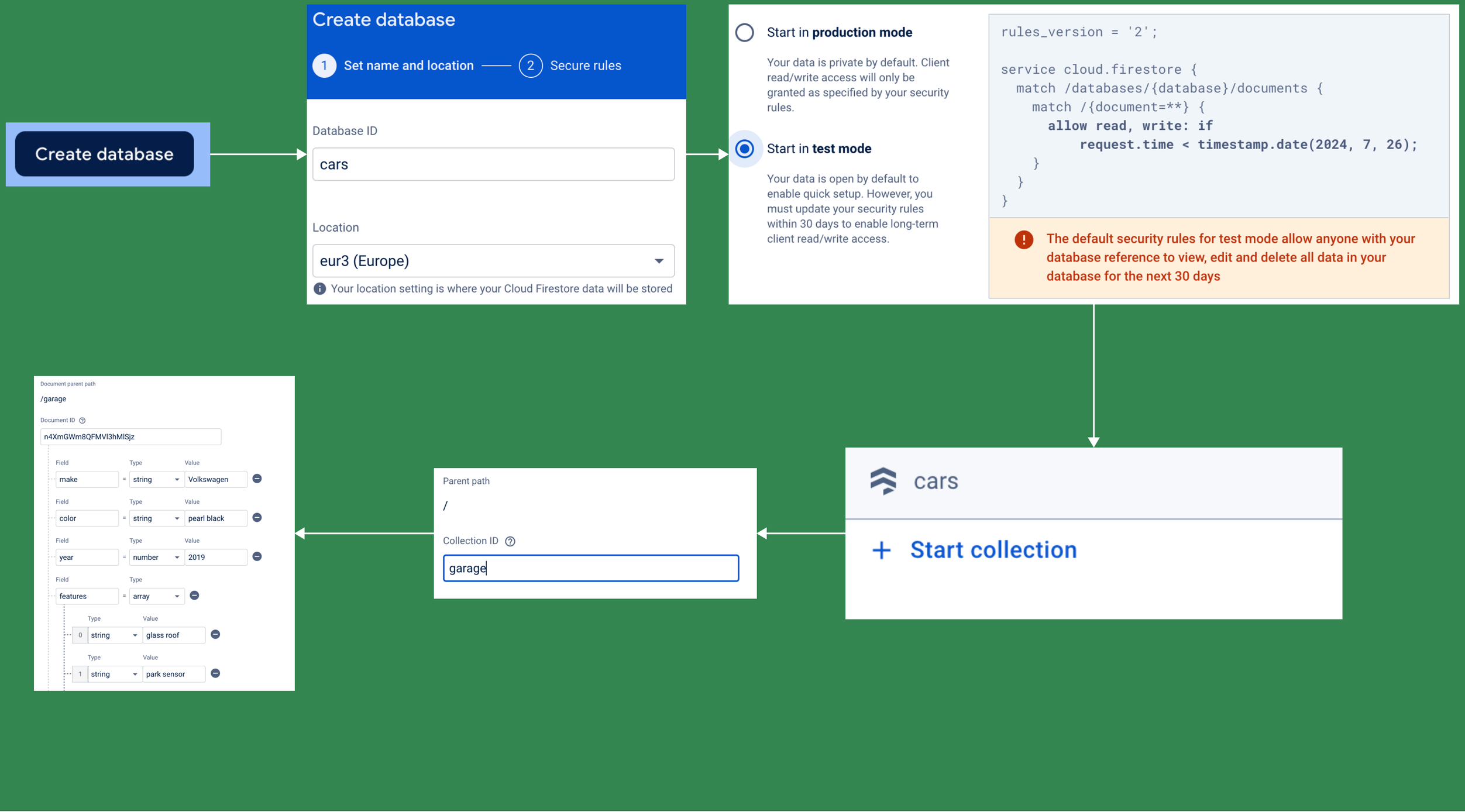
gfu-s3493-apr-2024 | it-erben.com

Continue

Wenn wir hier ein bestehendes GCP-Projekt wählen, wird es direkt mit dem Firebase-Projekt verknüpft.

Falls wir nach Google Analytics gefragt werden, lassen wir es inaktiv.



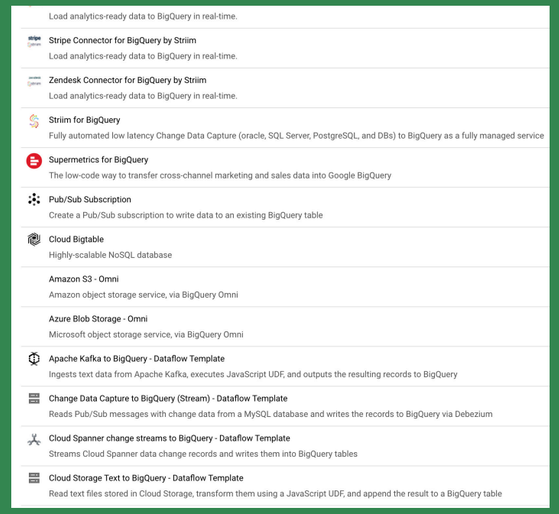

Create database
Create database
1 Set name and location
2 Secure rules
Database ID
cars
Location
eur3 (Europe)
Your location setting is where your Cloud Firestore data will be stored
Start in production mode
Your data is private by default. Client read/write access will only be granted as specified by your security rules.
Start in test mode
Your data is open by default to enable quick setup. However, you must update your security rules within 30 days to enable long-term client read/write access.
rules_version = '2';
service cloud.firestore {
match /databases/{database}/documents {
match /{document=**} {
allow read, write: if
request.time < timestamp.date(2024, 7, 26);
}
}
}
The default security rules for test mode allow anyone with your database reference to view, edit and delete all data in your database for the next 30 days
cars
+ Start collection
Parent path
/
Collection ID
garage
Document parent path
/garage
Document ID
n4XmGWm8QFMVl3hMlSjz
Field
Type
Value
make
string
Volkswagen
color
string
pearl black
year
number
2019
features
array
0
string
glass roof
1
string
park sensor

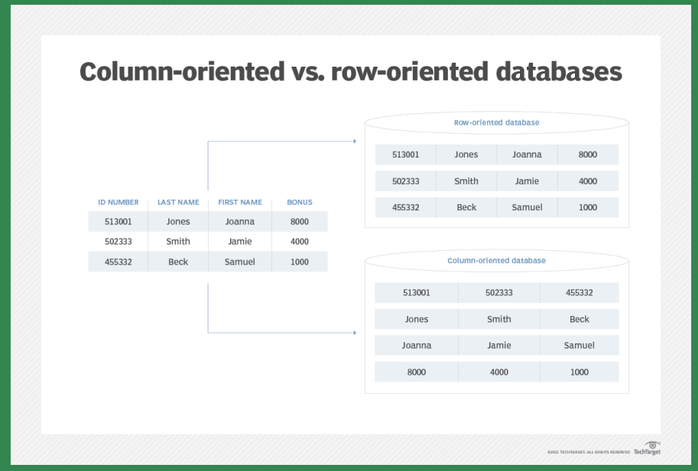
Aufgabe: Google Cloud Firestore

BigQuery

Google BigQuery

- Serverless Data Warehouse
- Relationales Datenmodell
- Viele Import-Formate
    - CSV, JSON, Parquet, ORC
- … und viele Quellen



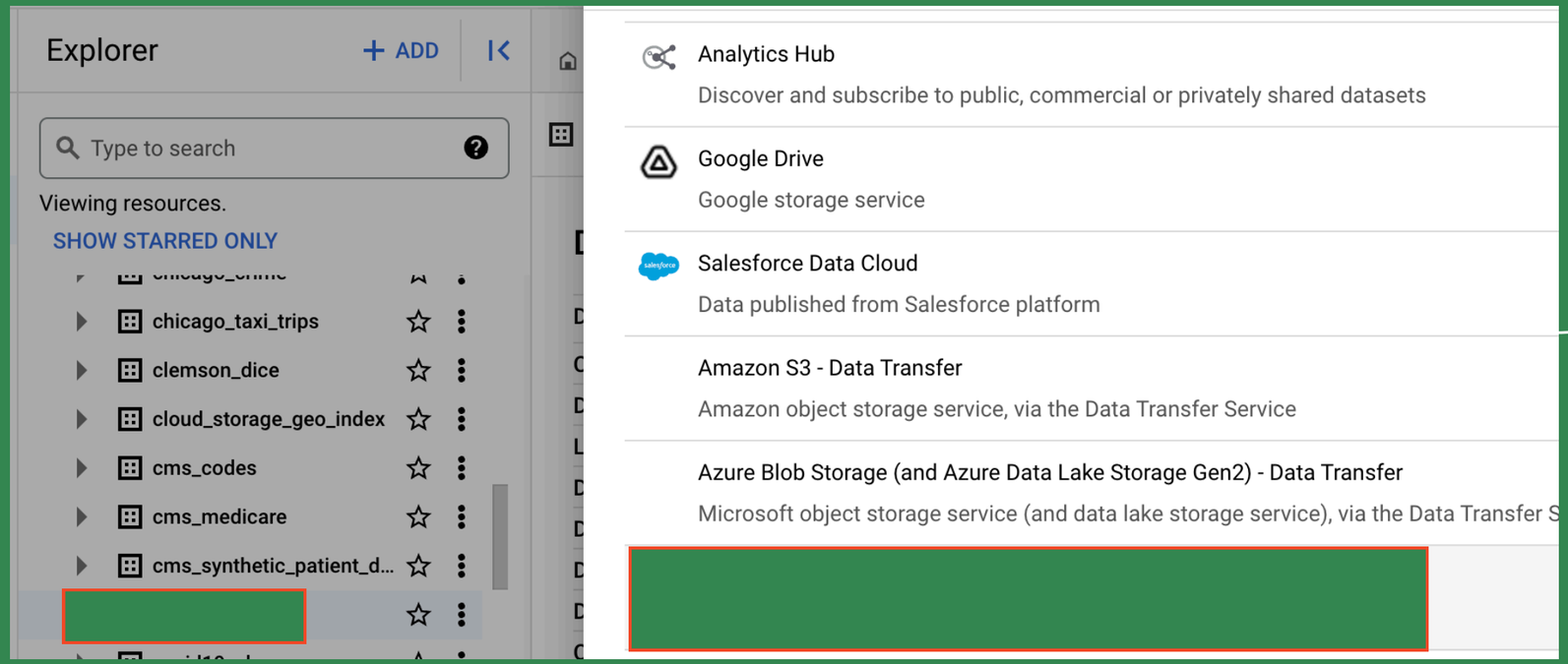


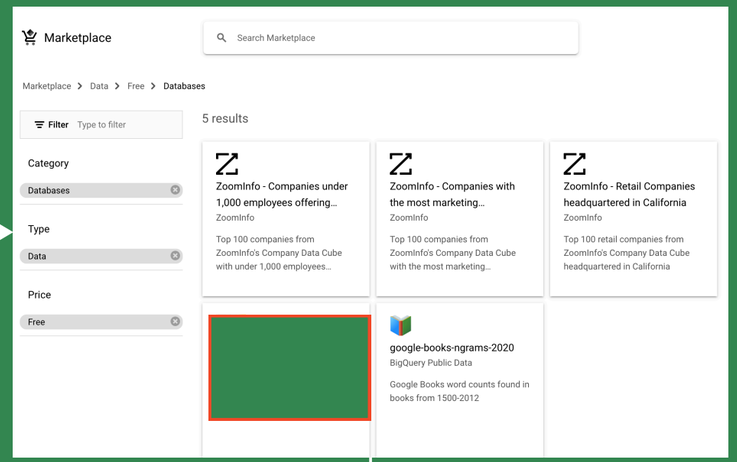
Google BigQuery

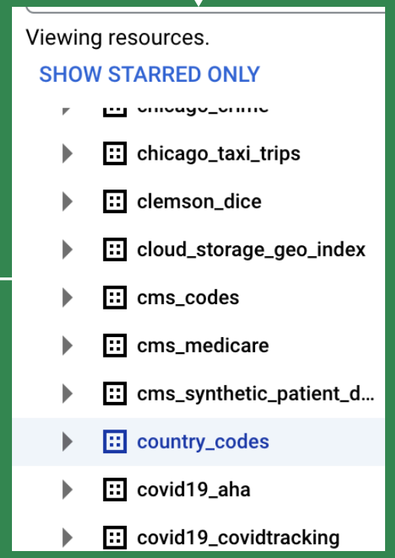
- Automatische Expiration von Datensätzen möglich
- Export in verschiedene Ziele
    - Cloud Storage
    - Cloud SQL
    - Google Drive
- Skaliert bis in den Exabyte-Bereich

Google BigQuery

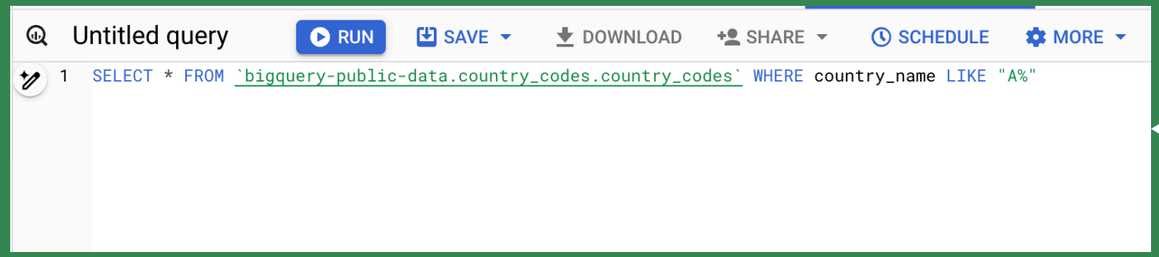
- Verschiedene Zugriffswege
    - Konsole
    - bq CLI (*nicht* gcloud)
    - Rest API
    - SDKs
- BigQuery kann bei falscher Verwendung *sehr* teuer werden
- Insbesondere bei Queries sollte man *immer* vor Absenden die Kostenschätzung betrachten


Explorer
+ ADD
Type to search
Viewing resources.
SHOW STARRED ONLY
chicago_taxi_trips
clemson_dice
cloud_storage_geo_index
cms_codes
cms_medicare
cms_synthetic_patient_d...
Analytics Hub
Discover and subscribe to public, commercial or privately shared datasets
Google Drive
Google storage service
Salesforce Data Cloud
Data published from Salesforce platform
Amazon S3 - Data Transfer
Amazon object storage service, via the Data Transfer Service
Azure Blob Storage (and Azure Data Lake Storage Gen2) - Data Transfer
Microsoft object storage service (and data lake storage service), via the Data Transfer S


Marketplace
Search Marketplace
Marketplace > Data > Free > Databases
Filter Type to filter
5 results
Category
Databases
Type
Data
Price
Free
ZoomInfo - Companies under 1,000 employees offering...
ZoomInfo
Top 100 companies from ZoomInfo's Company Data Cube with under 1,000 employees...
ZoomInfo - Companies with the most marketing...
ZoomInfo
Top 100 companies from ZoomInfo's Company Data Cube with the most marketing...
ZoomInfo - Retail Companies headquartered in California
ZoomInfo
Top 100 retail companies from ZoomInfo's Company Data Cube headquartered in California
google-books-ngrams-2020
BigQuery Public Data
Google Books word counts found in books from 1500-2012


Viewing resources.
SHOW STARRED ONLY
chicago_taxi_trips
clemson_dice
cloud_storage_geo_index
cms_codes
cms_medicare
cms_synthetic_patient_d...
country_codes
covid19_aha
covid19_covidtracking


country_codes
country_codes
covid19_aha
covid19_covidtracking
covid19_ecdc
covid19_ecdc_eu
Open
Query
Query in

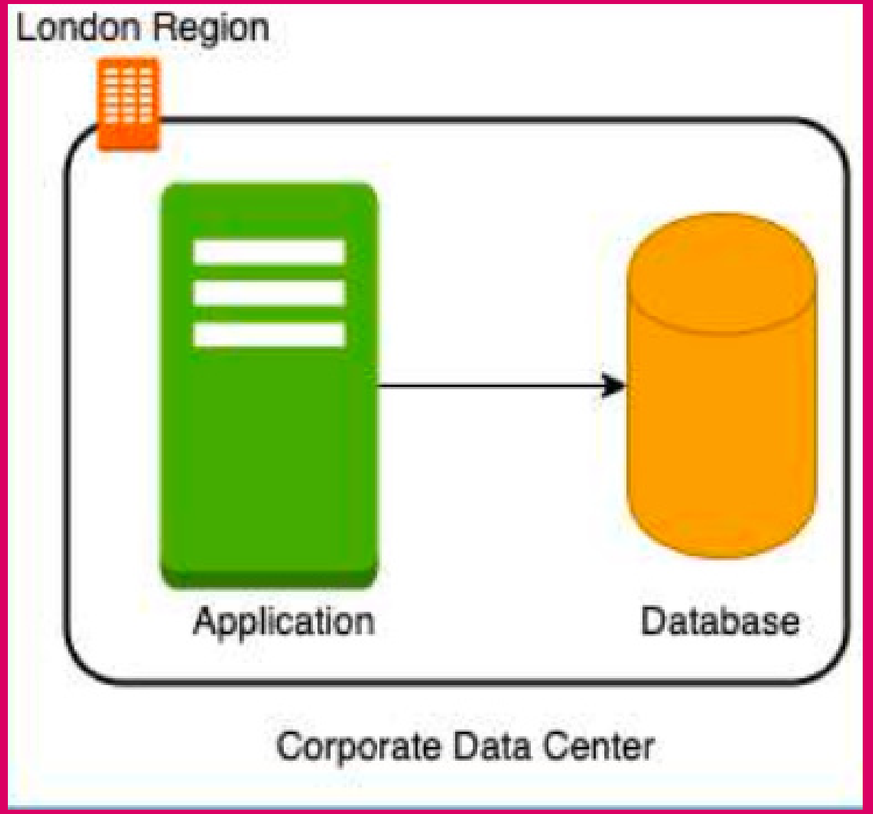

Untitled query
RUN
SAVE
DOWNLOAD
SHARE
SCHEDULE
MORE
1 SELECT * FROM `bigquery-public-data.country_codes.country_codes` WHERE country_name LIKE "A%"

Aufgabe: Google BigQuery

VPC

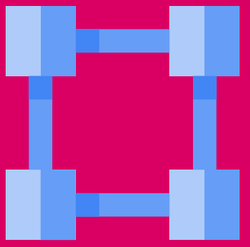
Google Cloud VPC

- Virtuelles Cloud-Netzwerk
- Bietet Isolierung von Netzwerken
- Beispiel-Anwendungsfall: private Kommunikation zwischen Datenbank und Webserver



Google Cloud VPC

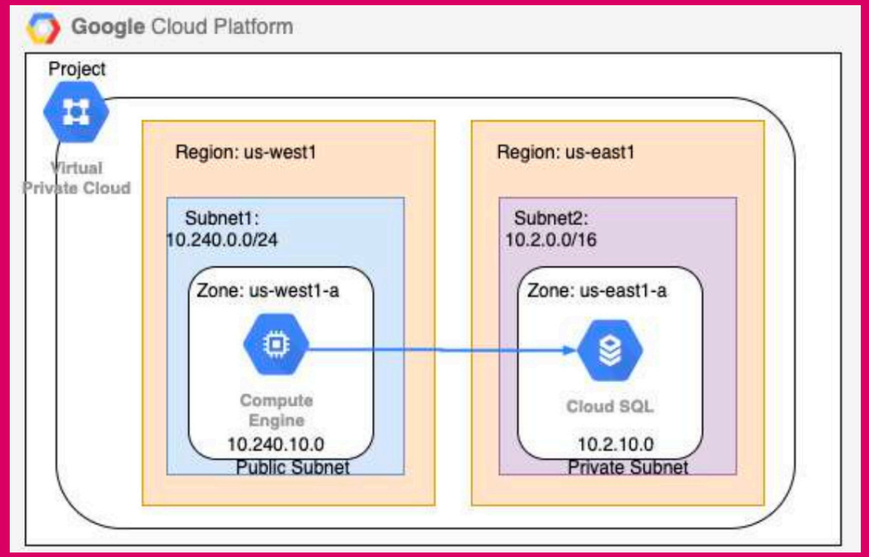
- Jeder ein- und ausgehende Traffic lässt sich kontrollieren
- Best Practice: Alle Server etc. nach Möglichkeit in VPCs anlegen
- VPC ist eine **globale** Ressource. Nicht regional oder zonal.



Virtual Private Cloud

Google Cloud VPC
Subnetze

- VPCs werden in Bereiche unterteilt
- Diese Bereiche werden **Subnetze** genannt
- **Public Subnets** können vom Internet aus erreicht werden
- **Private Subnetze** können nicht erreicht werden

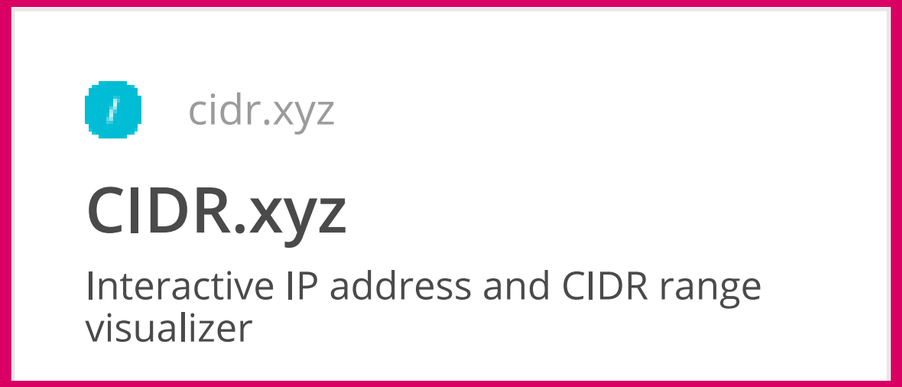


VPCs und Subnetze anlegen

- Standardmäßig hat jedes Projekt eine Default-VPC
- Man kann auch weitere anlegen
    - **Option 1**: Automatischer Modus. Für jede neue VPC werden Subnetze in jeder Region angelegt
    - **Option 2**: Benutzerdefinierter Modus. Keine Subnetze werden automatisch angelegt.
- Weitere Optionen:
    - **Private Google Access:** VMs erhalten privaten Zugriff auf Google APIs ohne über das Internet zu gehen
    - **Flow Logs:** Detaillierte Protokollierung des Netzwerkverkehrs für Debugging und Auditing

CIDR Ranges

- Adressbereiche in Netzwerken werden mit sgg. CIDR-Blöcken definiert
- Ein CIDR-Block besteht aus einer Start-IP (z.b. 10.0.0.0) und eine Range (z.B. /8)
- Die Range bezeichnet die Anzahl an Bits, die im Bereich Fix sind

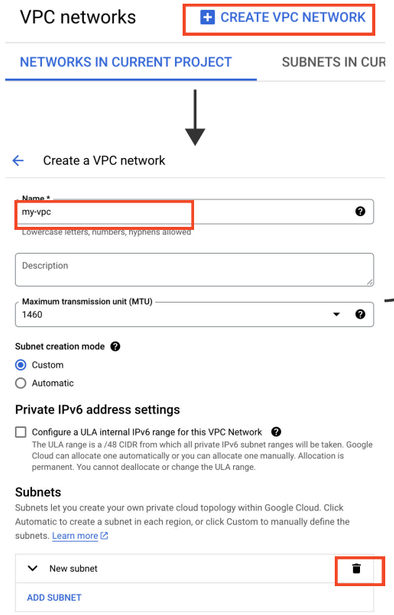


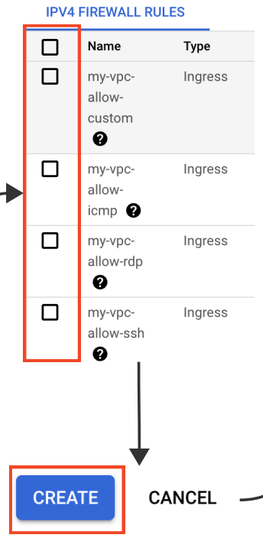
Firewall-Regeln

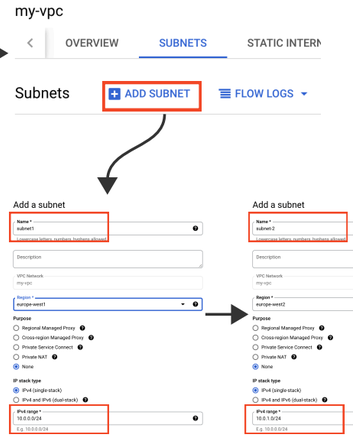
- Firewalls kontrollieren eingehenden und ausgehenden Traffic
- **Stateful**: Wenn eingehend erlaubt, ist auch ausgehend für die Verbindung erlaubt
- Prioritäten: 0 die höchste, 65535 die niedrigste
- Standardregel hat niedrigste Priorität
    - Jeder eingehende Traffic ist verboten
    - Jeder ausgehender Traffic ist erlaubt
- Es gibt vier weitere Standardregeln
    - **default-allow-ssh** (Port 22 ist standardmäßig offen)
    - **default-allow-rdp** (Port 3389 ist offen)
    - **default-allow-internal** (Traffic zwischen Subnetzen ist erlaubt)
    - **default-allow-icmp** (Ping ist möglich)

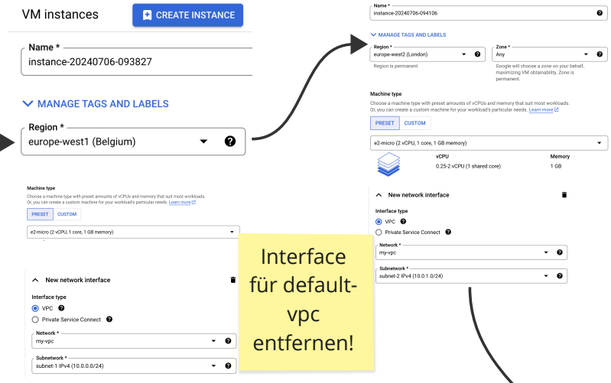
Firewall-Regeln: Egress und Ingress

- **Ingress-Regel**: Eingehender Traffic
    - Ziel: Entweder alle Instanzen, oder nur die mit bestimmten Tag
    - Quelle: Entweder CIDR, alle Instanzen oder nur die mit bestimmten Tag
- **Egress-Regel**: Ausgehender Traffic
    - Quelle: Entweder alle Instanzen, oder nur die mit bestimmten Tag
    - Ziel: CIDR-Range
- Für jede Regel
    - Priorität
    - Action: Deny oder Allow
    - Protocol (TCP/UDP/ICMP)
    - Port
    - Status (Aktiv/inaktiv)

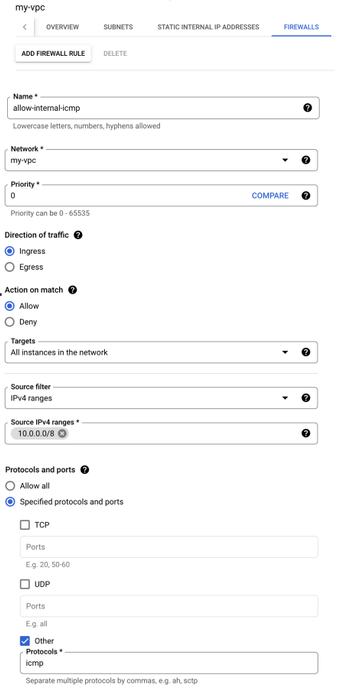


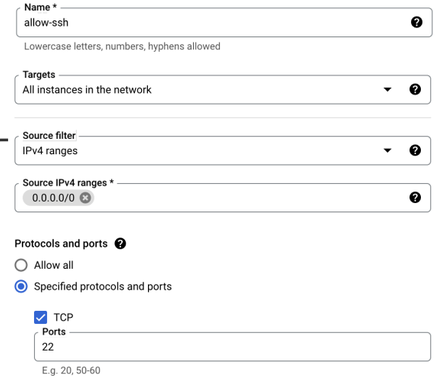


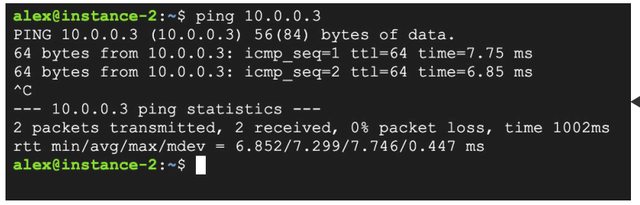




Interface für default-vpc entfernen!







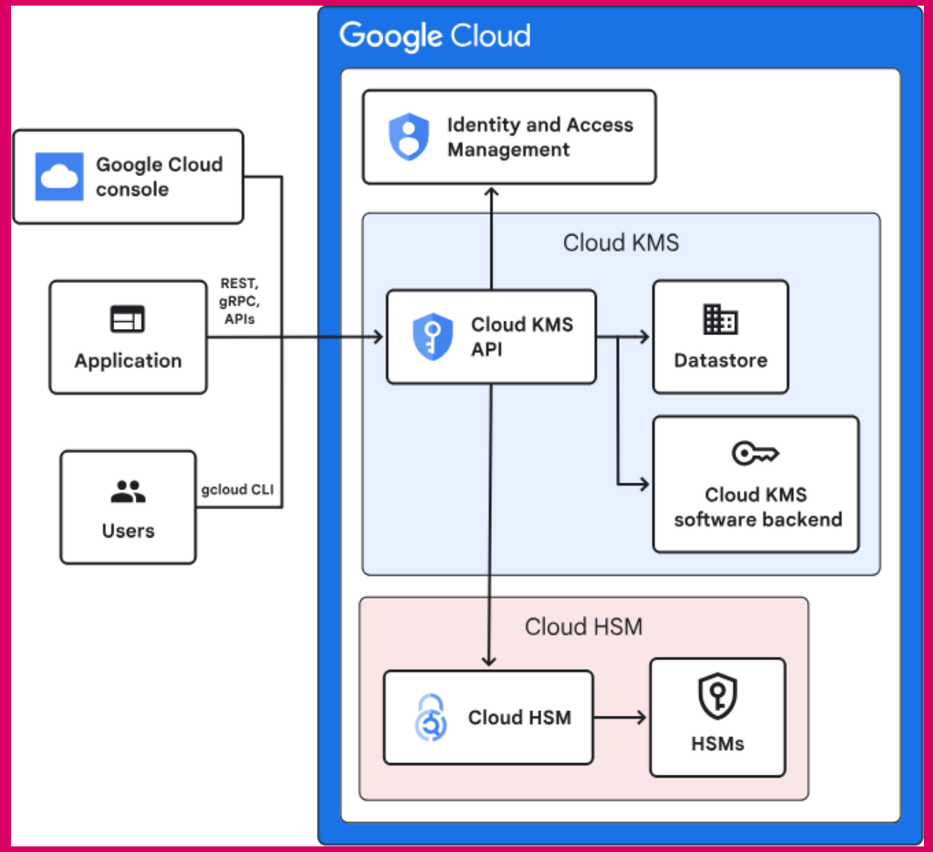
KMS

Google KMS

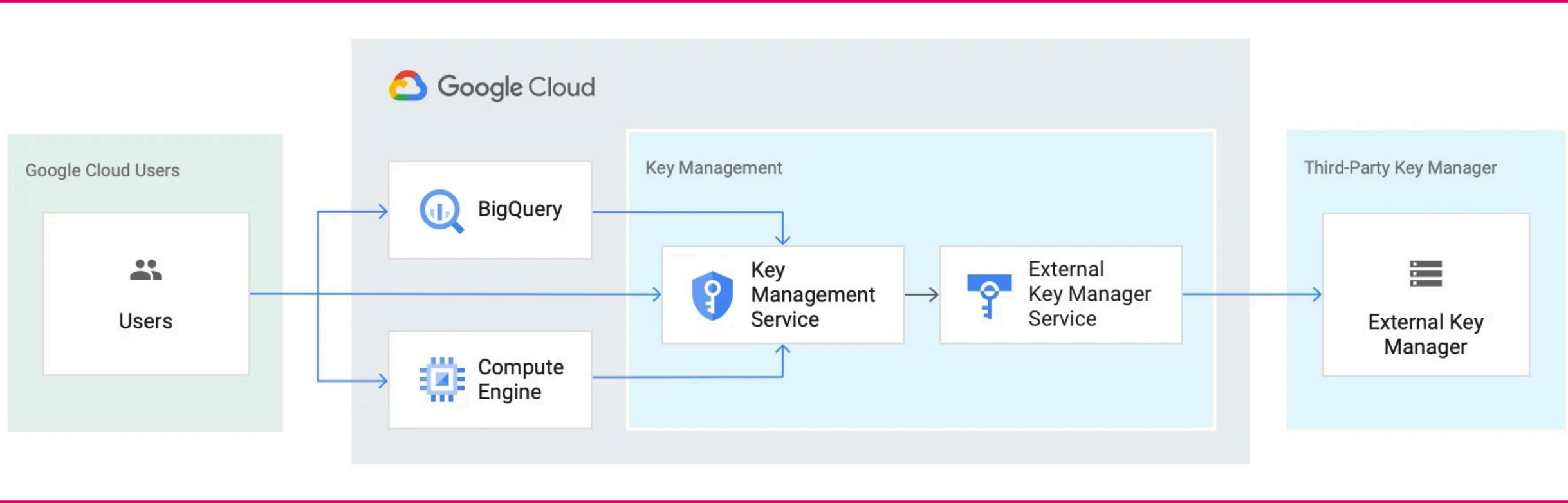
- Verwalteter Dienst zur Erstellung, Nutzung und Kontrolle kryptografischer Schlüssel
- Unterstützt **symmetrische**, **asymmetrische** und **HSM-gesicherte** Schlüssel
- Vollständig integriert mit GCP-Diensten (z. B. GCS, BigQuery, GKE, Pub/Sub)
- Nutzung über REST API, gcloud, oder direkt über GCP Console

Cloud HSM

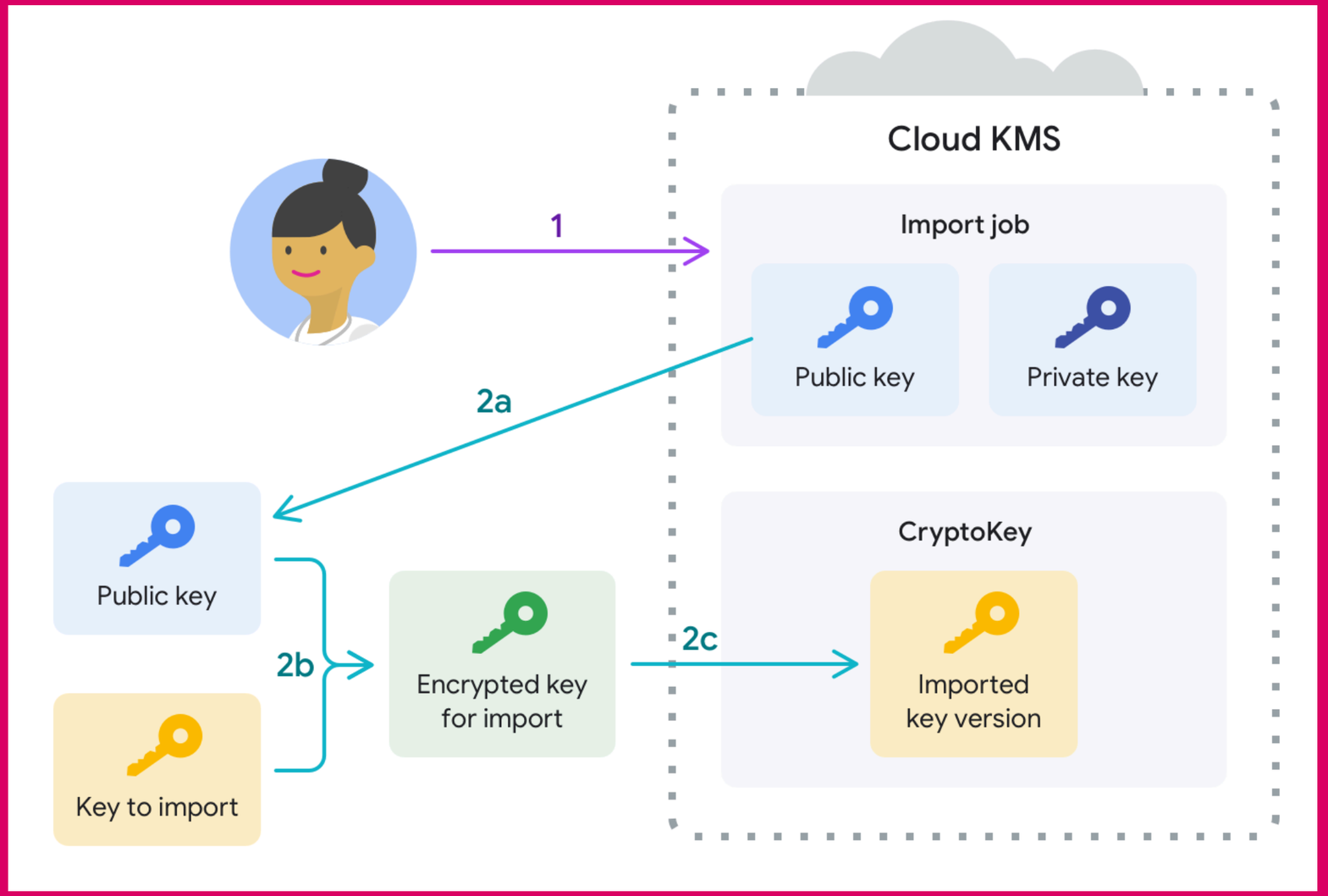
- Hardware Security Module (HSM) als vollständig verwalteter GCP-Dienst
- Bietet FIPS 140-2 Level 3 zertifizierte kryptografische Schlüsselverwaltung
- Native Integration in Cloud KMS – gleiche API & IAM-Steuerung
- Schlüsselmaterial wird ausschließlich in HSM-Hardware generiert und gespeichert
- Ideal für besonders sensible Daten & regulierte Branchen (z. B. Finanz, Gesundheitswesen)



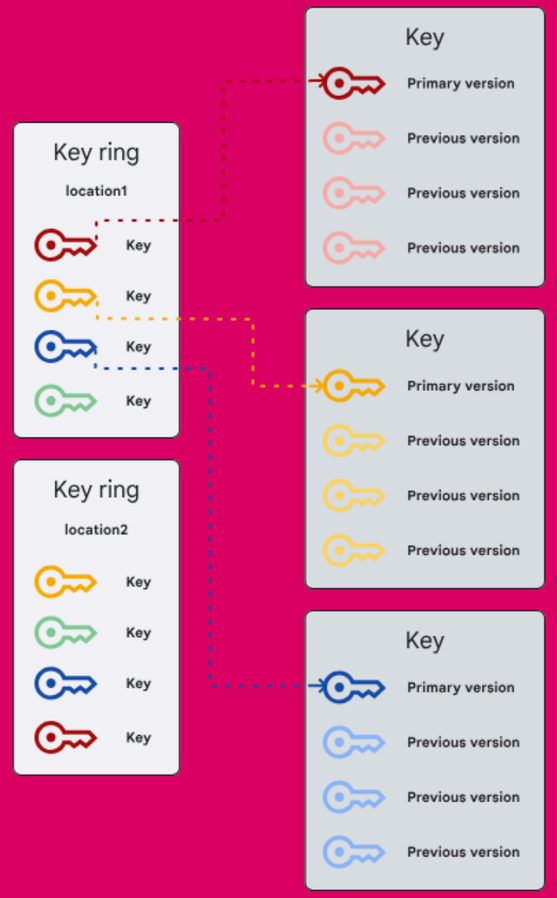
External Keys



Schlüsselimport



Schlüsselbünde



Location

- KMS-Schlüssel sind **regionsgebunden**: Jeder Key wird in einer **festen Location** erstellt
- Zwei Typen:
    - **Regional** (z. B. europe-west1, us-central1): Schlüssel verbleiben in einer spezifischen Region
    - **Global**: Nur für Schlüssel, die mit globalen GCP-Diensten wie dem globalen Load Balancer genutzt werden
- Wichtig für Compliance, Latenz und Datenresidenz
- Ein Key ist nicht verschiebbar zwischen Regionen – Architektur muss Standortwahl berücksichtigen
- Beispiel:
    - --location=us-central1 → physisch in Iowa
    - --location=global → weltweit verfügbar, aber intern regional verteilt

External Keys

- **External Keys**: Verschlüsselungsschlüssel, die **außerhalb von Google Cloud** gespeichert und verwaltet werden
- Ermöglicht die Nutzung von Drittanbieter-HSMs oder KMS-Systemen (z. B. Thales, Fortanix, AWS CloudHSM)
- Funktioniert über **Cloud External Key Manager (EKM)** – vermittelt zwischen GCP-Dienst und externem Key
- **GCP sieht das Schlüsselmaterial nie** – ideal für hohe Compliance-Anforderungen (z. B. Banken, Regierung)
- Nutzbar mit GCP-Diensten wie BigQuery, Cloud Storage, Compute Engine (über CMEK)

Schlüsselimport

- Ermöglicht das **Einspielen eigener Schlüsselmaterialien** in Cloud KMS
- Schlüssel werden **außerhalb von GCP generiert**, z. B. in einem lokalen HSM oder auf sicherem Gerät
- Import erfolgt über ein **zweistufiges Verfahren** mit temporärem Import-Job und RSA-Verschlüsselung
- Unterstützt **Compliance-Anforderungen**, bei denen Schlüsselgenerierung außerhalb von Google vorgeschrieben ist

```
export KMS_KEYRING=demo-keyring
export KMS_KEY=demo-key
export KMS_LOCATION=global

gcloud kms keyrings create $KMS_KEYRING \
  --location=$KMS_LOCATION

gcloud kms keys create $KMS_KEY \
  --location=$KMS_LOCATION \
  --keyring=$KMS_KEYRING \
  --purpose=encryption

echo "Geheime Nachricht von der Demo" > plaintext.txt

gcloud kms encrypt \
  --location=$KMS_LOCATION \
  --keyring=$KMS_KEYRING \
  --key=$KMS_KEY \
  --plaintext-file=plaintext.txt \
  --ciphertext-file=ciphertext.bin

gcloud kms decrypt \
  --location=$KMS_LOCATION \
  --keyring=$KMS_KEYRING \
  --key=$KMS_KEY \
  --ciphertext-file=ciphertext.bin \
  --plaintext-file=decrypted.txt

cat decrypted.txt
```

Cloud Loadbalancing

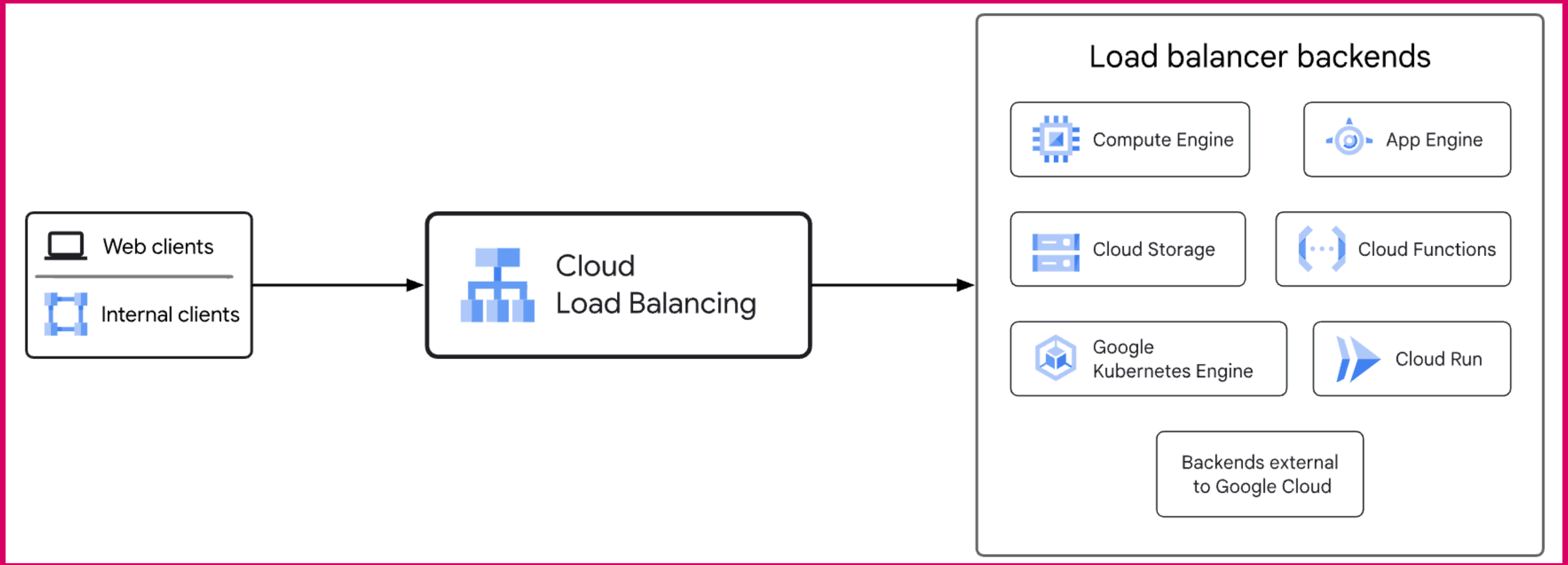
Cloud Load Balancer

- Vollständig verwalteter, globaler Load Balancer auf Layer 4 (TCP/UDP) & Layer 7 (HTTP/HTTPS)
- Automatische Skalierung und integriertes Health Checking
- Native Integration mit GCP-Diensten (z. B. GCE, GKE, Cloud Run)
- Kein Pre-Warming erforderlich – skaliert sofort mit Traffic

Load Balancer Typen

- **HTTP(S) Load Balancer**: global, Layer 7 – ideal für Websites & APIs
- **Network Load Balancer**: regional, Layer 4 – hohe Performance bei niedrigem Overhead
- **Internal Load Balancer**: privat, innerhalb eines VPC – z. B. für Mikroservices
- Kombinierbar mit Cloud Armor (WAF) & Cloud CDN für Sicherheit und Performance

Cloud Load Balancer

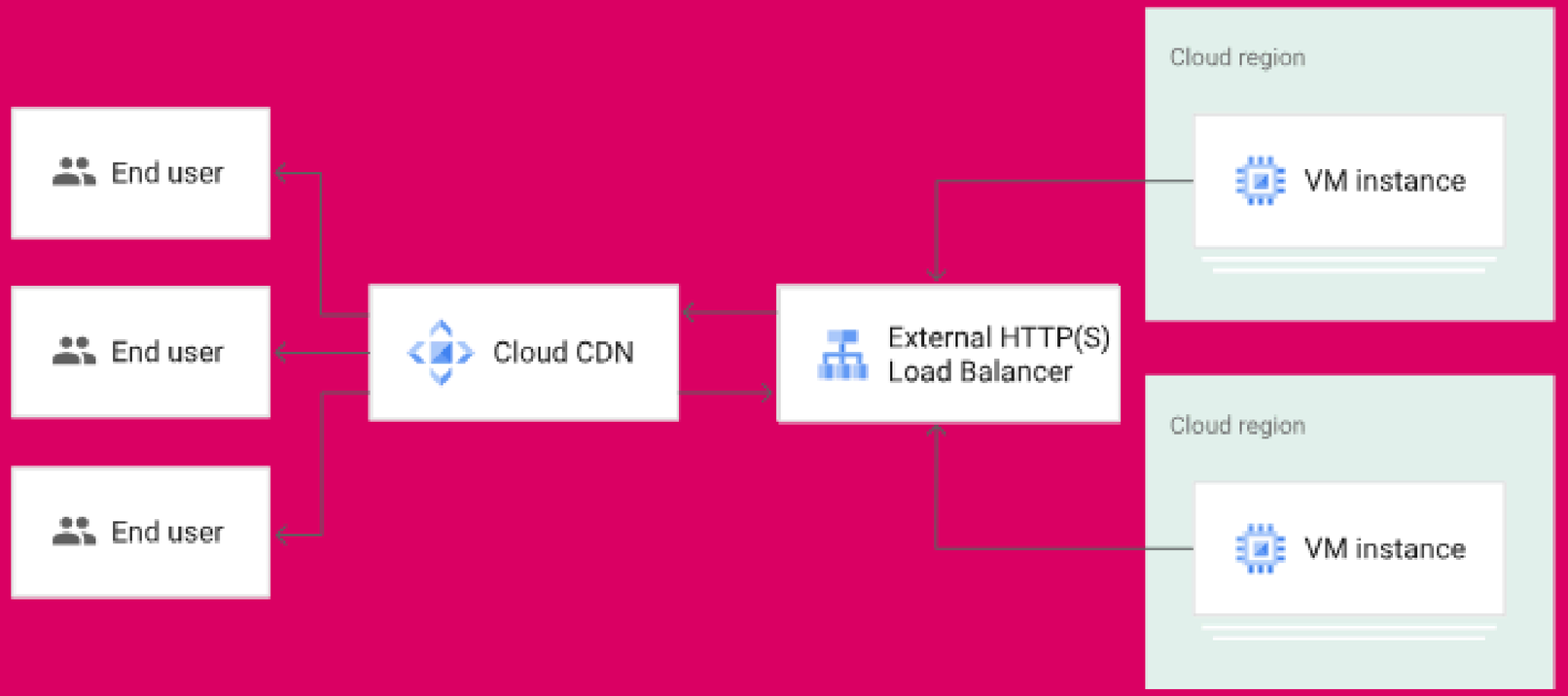


Cloud CDN

Cloud CDN

- Globales Content Delivery Network, direkt integriert mit Cloud Load Balancer
- Reduziert Latenz & Backend-Last durch Caching an Edge-Standorten weltweit
- HTTP/HTTPS-Support mit optimierter TLS-Auslieferung
- Automatisches Caching statischer & dynamischer Inhalte (per Cache-Control)
- Nahtlose Integration mit GCP-Diensten wie GCE, GKE, Cloud Run

Cloud CDN


End user
End user
End user
Cloud CDN
External HTTP(S)
Load Balancer
Cloud region
VM instance
Cloud region
VM instance

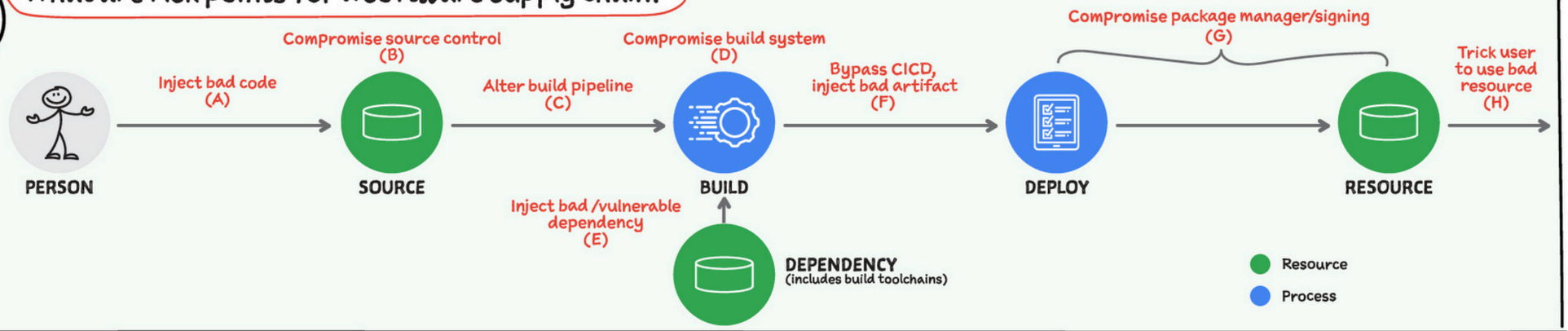
Automation

Secure Software Development Lifecycle

ON GOOGLE CLOUD

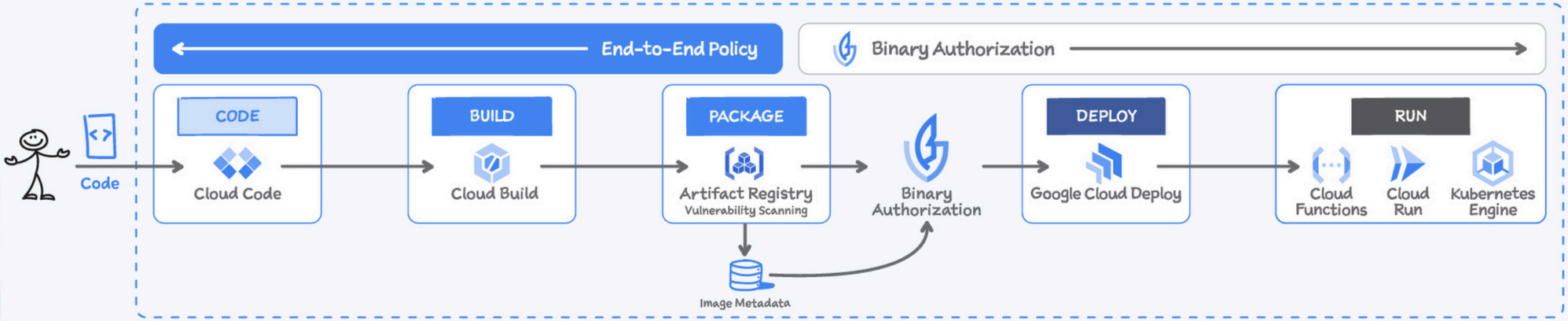
#GCPSketchnote
@PVERGADIA
THECLOUDGIRL.DEV
11.03.2021

What are risk points for a software supply chain?



How to secure software development lifecycle with Google Cloud?

SECURE SOFTWARE DEVELOPMENT LIFECYCLE WITH GOOGLE CLOUD

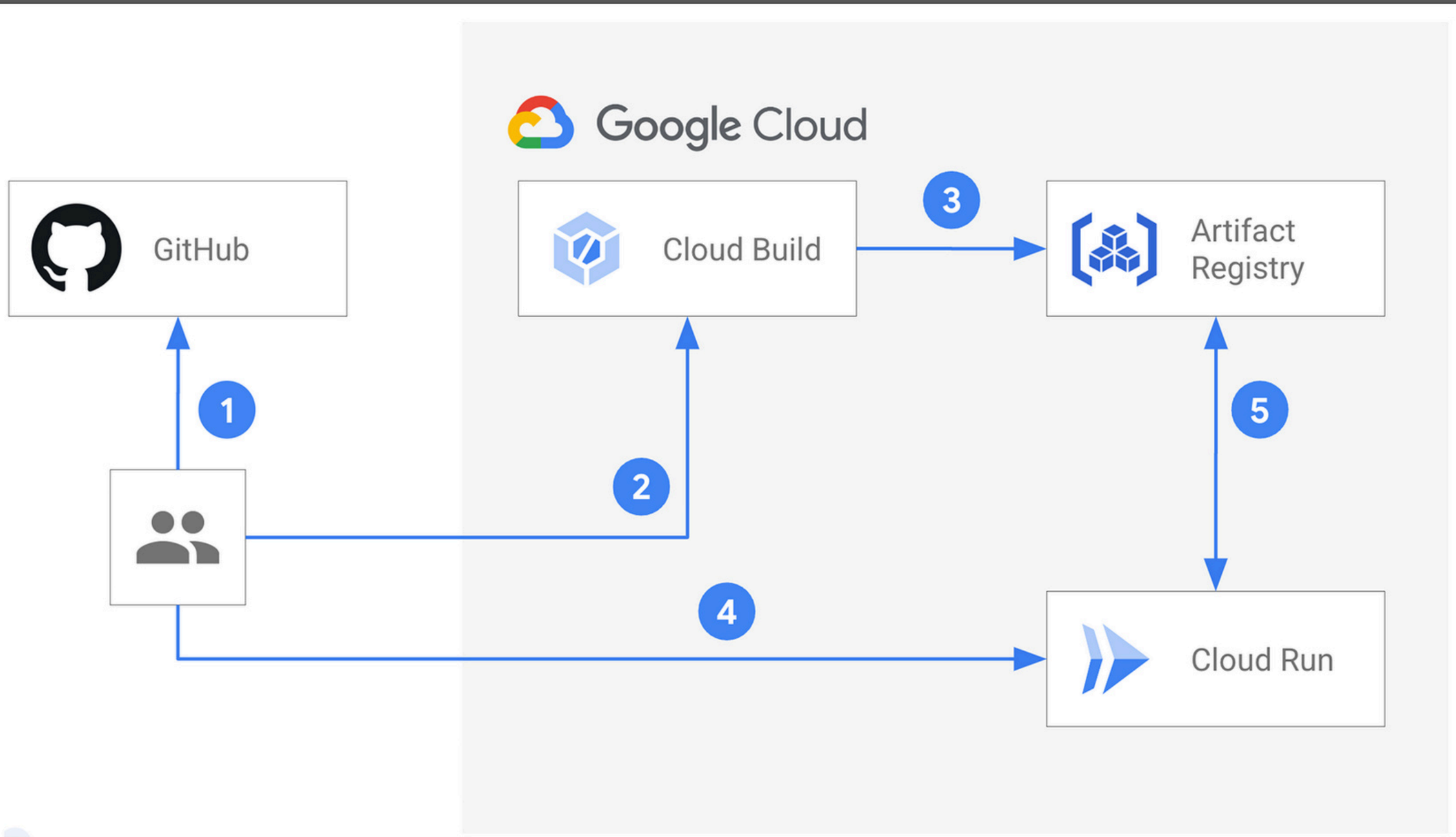


Artifact Registry

- **Nachfolger der Container Registry (GCR)** – universeller & sicherer
- Unterstützt mehrere **Artefakttypen**: Docker, Maven, npm, Python, Go u. a.
- **Regionale Repositories** für bessere Performance und Datenresidenz

Artifact Registry

- Fein granulare **IAM-basierte Zugriffssteuerung**, optional mit VPC Service Controls
- Native Integration mit **Cloud Build, GKE, Cloud Run** und CI/CD-Pipelines
- CLI-Zugriff via gcloud und Artifact Registry Docker-Helper


Google Cloud
GitHub
Cloud Build
Artifact Registry
Cloud Run
1
2
3
4
5

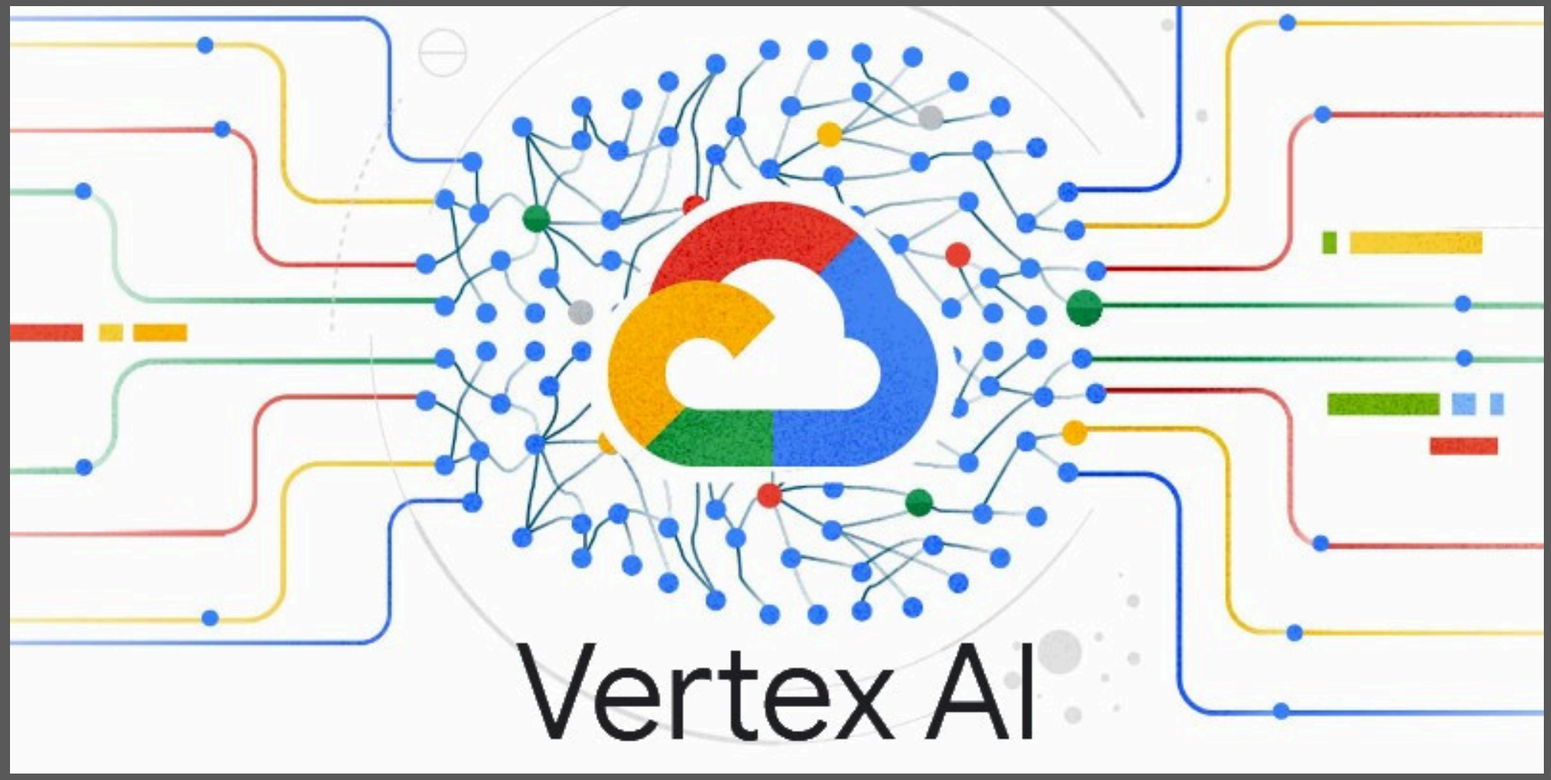
Cloud Build

- Fully managed CI/CD Plattform von Google Cloud
- Unterstützt **Builds aus verschiedenen Quellen**: GitHub, GitLab, Cloud Source Repositories, lokal
- Erzeugt **Docker-Container, JARs, Node-Pakete, uvm.**
- Build-Spezifikation per cloudbuild.yaml oder cloudbuild.json
- Integriert mit GCP-Diensten wie Cloud Run, GKE, Artifact Registry
- Unterstützt parallele Schritte und Caching
- Skalierung erfolgt automatisch (kein eigener Runner nötig)

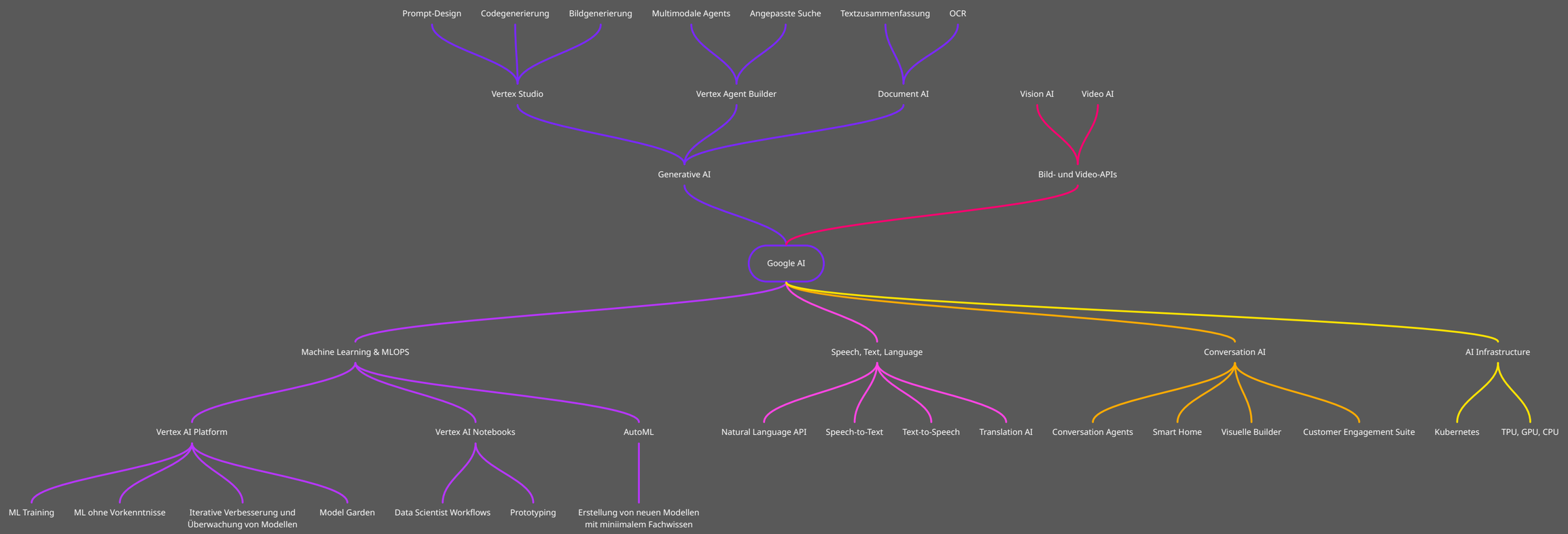
Aufgabe: Google Cloud Build

Vertex AI

AI: Ein Moving Target



vormals AI Platform


Prompt-Design
Codegenerierung
Bildgenerierung
Multimodale Agents
Angepasste Suche
Textzusammenfassung
OCR
Vertex Studio
Vertex Agent Builder
Document AI
Vision AI
Video AI
Generative AI
Bild- und Video-APIs
Google AI
Machine Learning & MLOPS
Speech, Text, Language
Conversation AI
AI Infrastructure
Vertex AI Platform
Vertex AI Notebooks
AutoML
Natural Language API
Speech-to-Text
Text-to-Speech
Translation AI
Conversation Agents
Smart Home
Visuelle Builder
Customer Engagement Suite
Kubernetes
TPU, GPU, CPU
ML Training
ML ohne Vorkenntnisse
Iterative Verbesserung und Überwachung von Modellen
Model Garden
Data Scientist Workflows
Prototyping
Erstellung von neuen Modellen mit miniimalem Fachwissen

Checkout

Das habe ich neu gelernt

Das fand ich besonders interessant oder spannend

Das hätte ich anders erwartet

Sticky stack