Google Cloud

Using Recommendations for Infrastructure as Code

Google Cloud Learning Services

GitOps plus FinOps

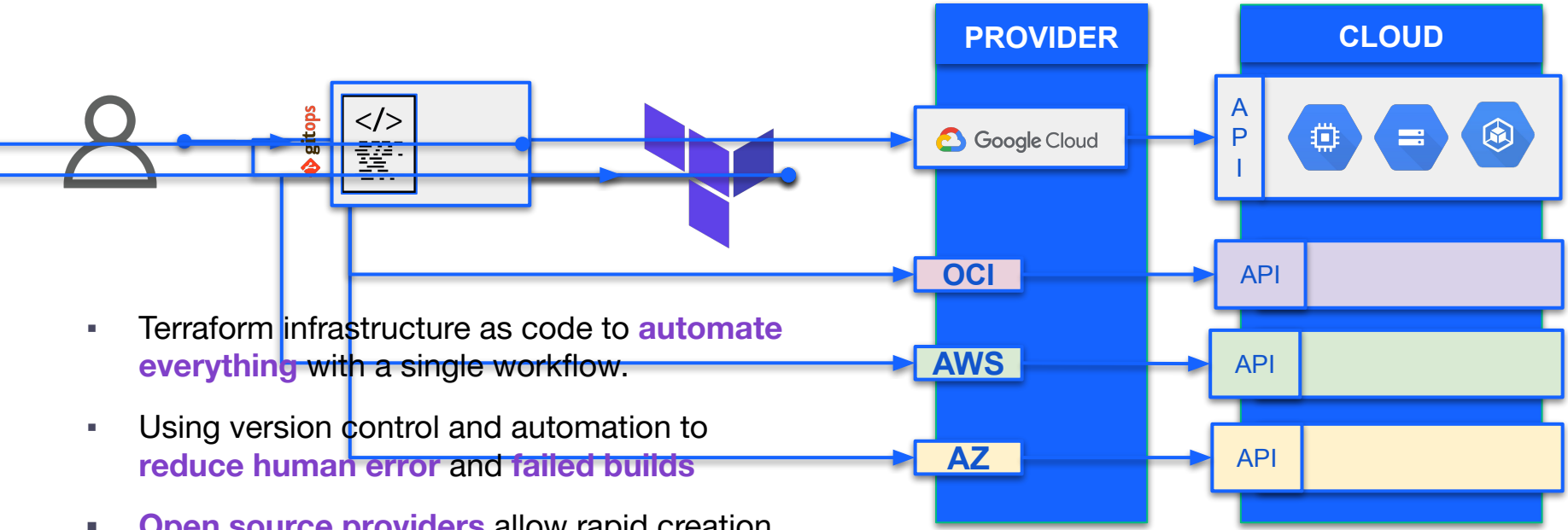
GinOps I made this up

Google Cloud

© 2022 Google LLC. All rights reserved.

Part 2: The Solution

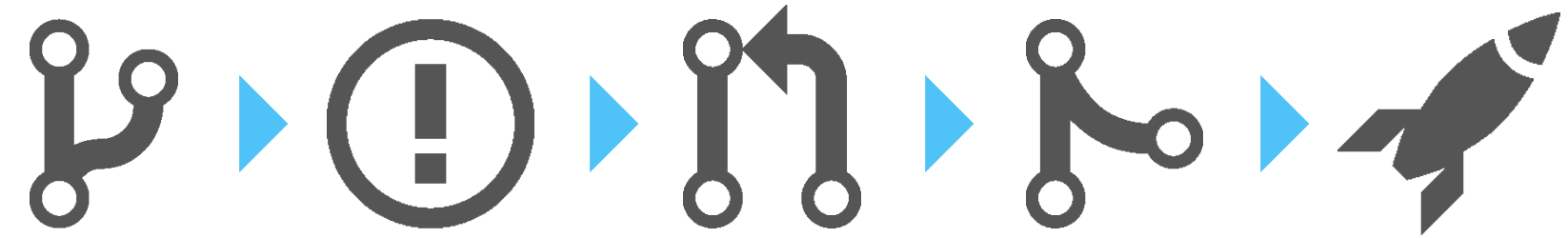
Infrastructure Automation



- Terraform infrastructure as code to **automate everything** with a single workflow.
- Using version control and automation to **reduce human error** and **failed builds**
- **Open source providers** allow rapid creation and support for any infrastructure

Part 2: The Solution

Project as code.

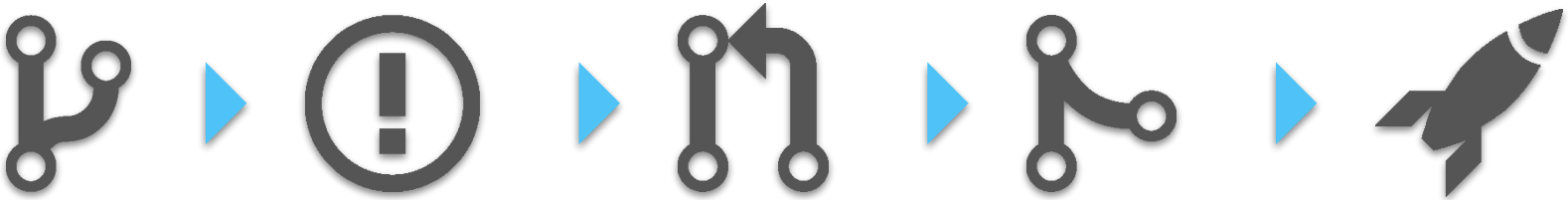


Branch Validate Review Merge Create

Part 2: The Solution

Automation Pipelines

- **Collaborate** in source control
- Ensure **consistency**
- Reduce **manual** effort and **errors**
- Enforce **policies** proactively



Developer submits **Pull Request**

CI runs **Validation**

Admin reviews for **Policy Compliance**

Admin merges the **New Config**

CD updates **Deployed Infrastructure**

GitHub

Terraform ENTERPRISE

GitOps

Recommendations

Recommender

Retrieve recommendations for Google Cloud resources, helping you improve your security, and save costs.

Console gcloud API

1. In the Google Cloud Console, go to the **VM instances** page.

   Go to the VM instances page

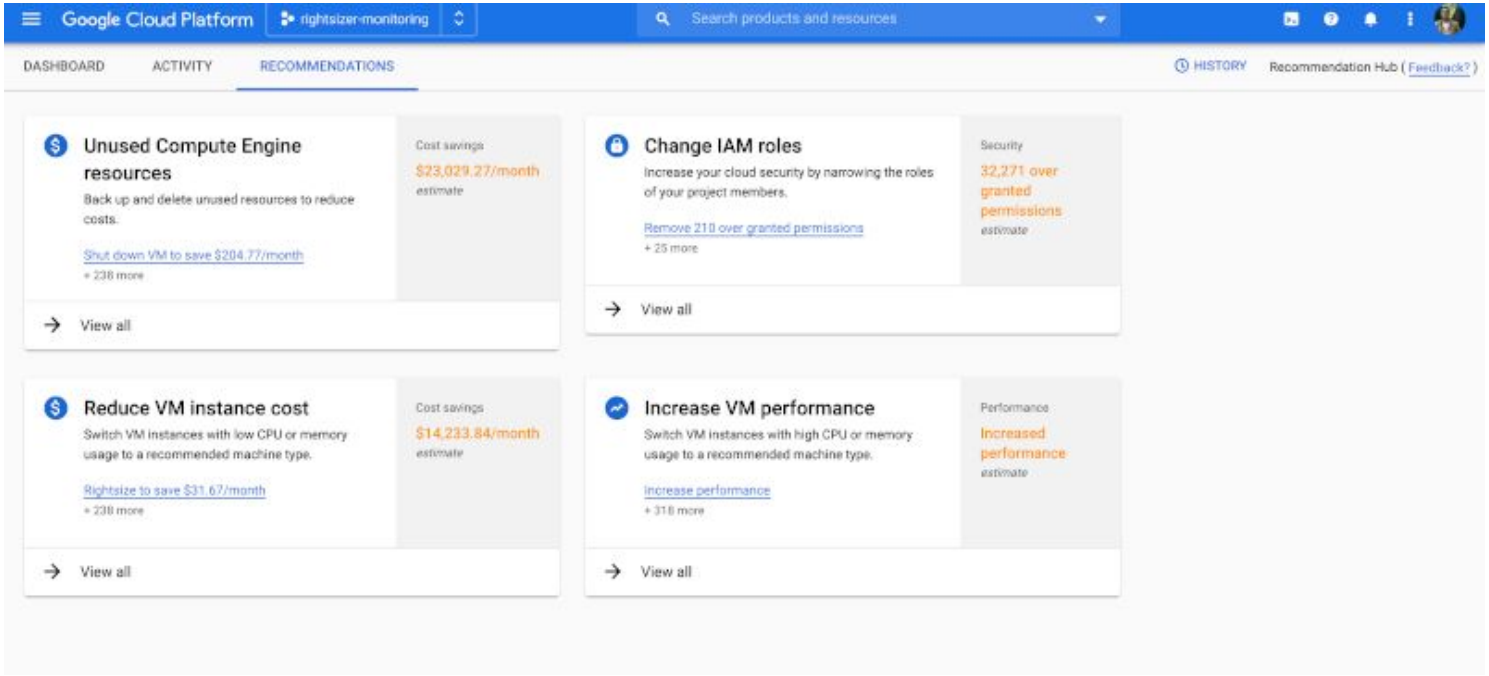
2. Look at the **Recommendation** column to review recommendations for individual instances. You can also sort the column by amount of estimated savings. If there are no recommendations next to your instances, Compute Engine doesn't have any recommendations to make.

Recommendation
Save $16 / mo
Save $500 / mo

Google Cloud

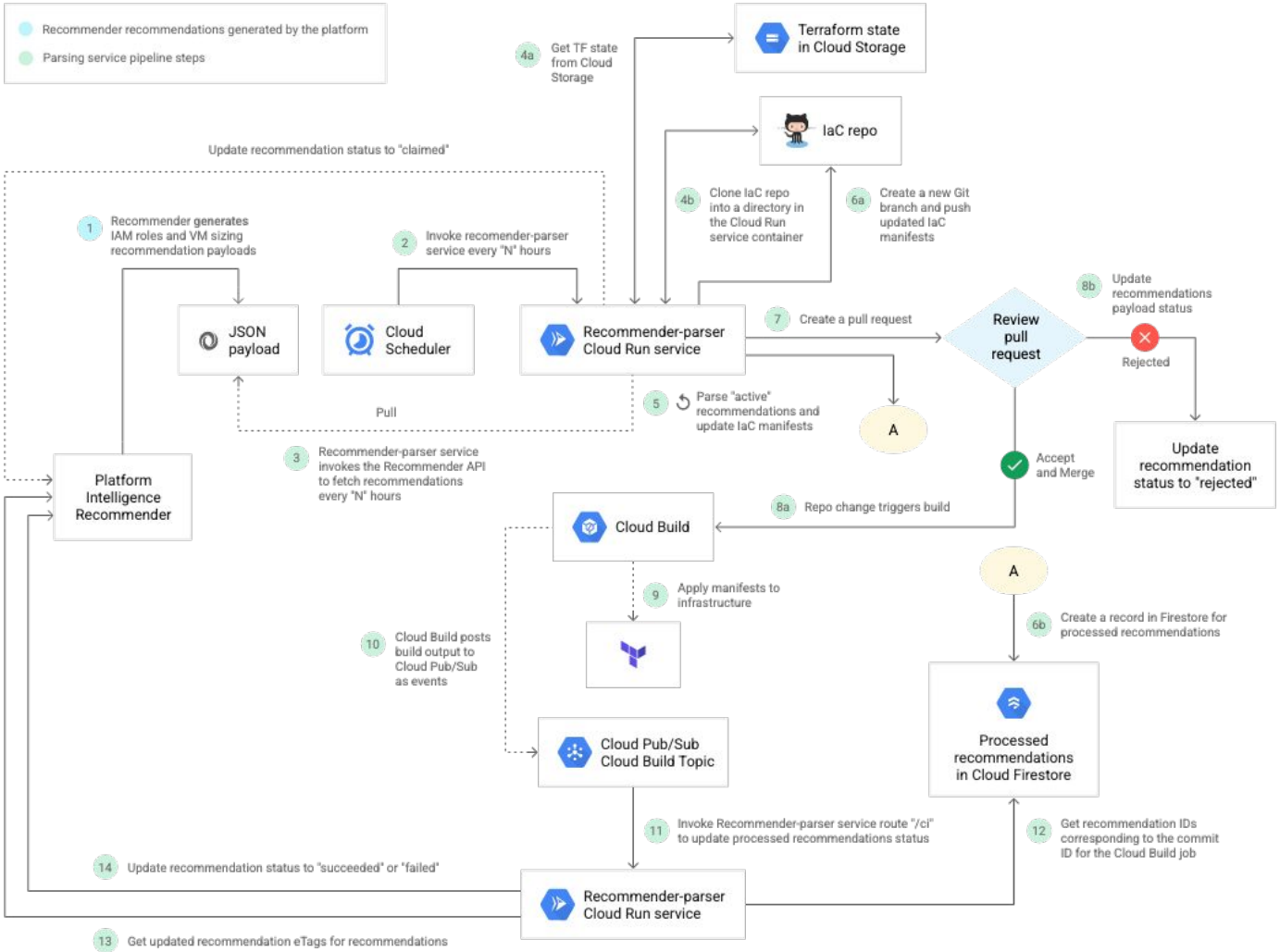
© 2022 Google LLC. All rights reserved.

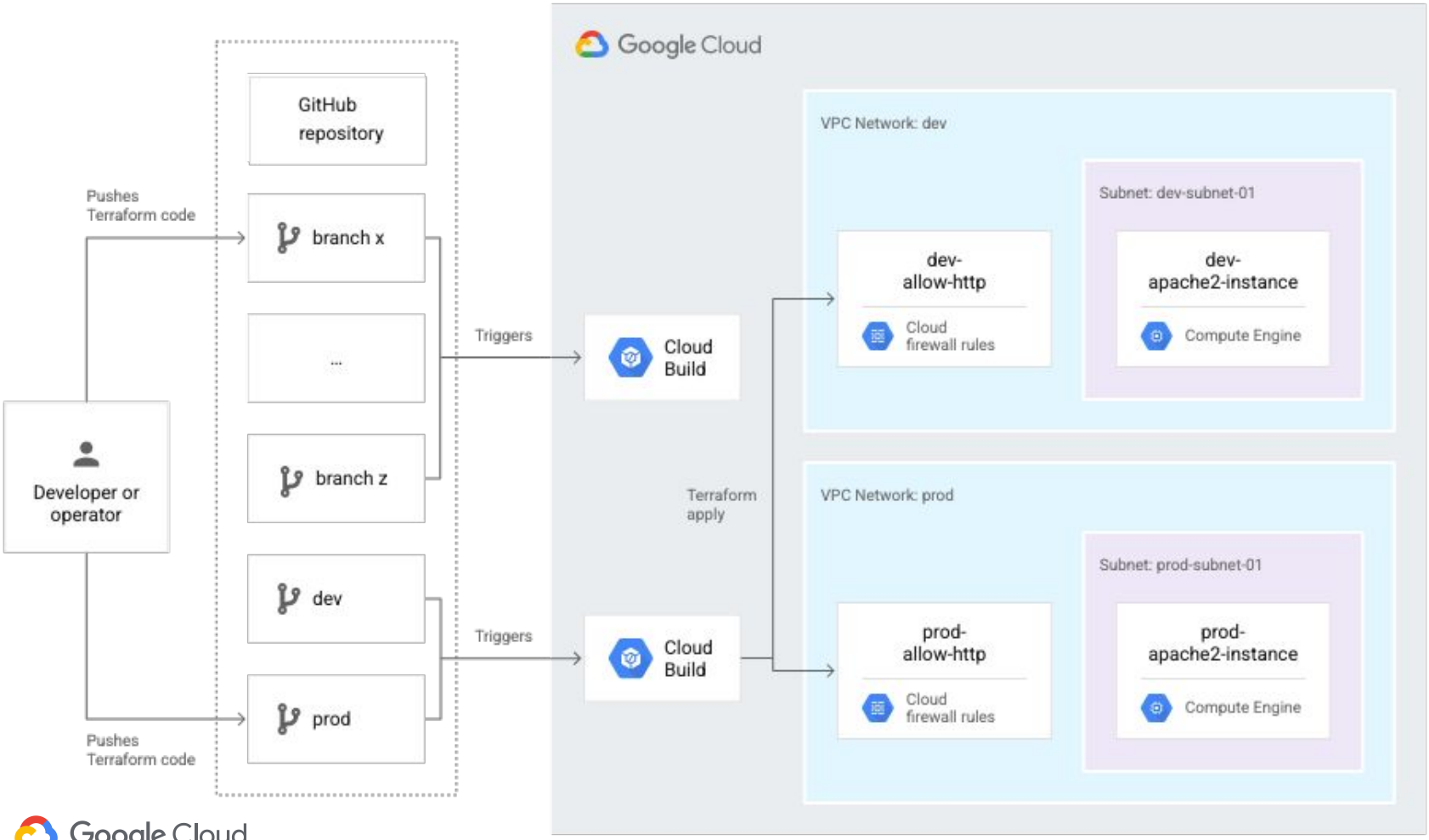
Recommendations Hub



Google Cloud

© 2022 Google LLC. All rights reserved.


Recommender recommendations generated by the platform
Parsing service pipeline steps
4a Get TF state from Cloud Storage
Terraform state in Cloud Storage
IaC repo
Update recommendation status to "claimed"
4b Clone IaC repo into a directory in the Cloud Run service container
6a Create a new Git branch and push updated IaC manifests
1 Recommender generates IAM roles and VM sizing recommendation payloads
2 Invoke recomender-parser service every "N" hours
JSON payload
Cloud Scheduler
Recommender-parser Cloud Run service
7 Create a pull request
Review pull request
8b Update recommendations payload status
Rejected
Pull
5 Parse "active" recommendations and update IaC manifests
A
Accept and Merge
Update recommendation status to "rejected"
3 Recommender-parser service invokes the Recommender API to fetch recommendations every "N" hours
Platform Intelligence Recommender
8a Repo change triggers build
Cloud Build
A
9 Apply manifests to infrastructure
6b Create a record in Firestore for processed recommendations
10 Cloud Build posts build output to Cloud Pub/Sub as events
Cloud Pub/Sub Cloud Build Topic
Processed recommendations in Cloud Firestore
11 Invoke Recommender-parser service route "/ci" to update processed recommendations status
12 Get recommendation IDs corresponding to the commit ID for the Cloud Build job
14 Update recommendation status to "succeeded" or "failed"
Recommender-parser Cloud Run service
13 Get updated recommendation eTags for recommendations



Google Cloud

© 2022 Google LLC. All rights reserved.

Cloud Scheduler

Purpose: Cloud Scheduler triggers the Recommender Parser service.

Google Cloud

© 2022 Google LLC. All rights reserved.

Cloud Run

Purpose: The recommender-parser service is where all the processing logic resides. It has multiple routes, each of which serve a specific purpose:

- Parsing recommendations for each recommendation type.
- Updating the status of the recommendations being processed

Google Cloud

© 2022 Google LLC. All rights reserved.

Terraform

Purpose: Terraform 0.12 is the infrastructure as code tool.

A Cloud Build builder for Terraform is used to invoke Terraform commands and the Cloud Build service account is used for that purpose.

© 2022 Google LLC. All rights reserved.

Cloud Build

Purpose: Google Cloud Build automates the deployment of infrastructure based on the changes made to the IaC manifests per policy intelligence recommendations.

Google Cloud

© 2022 Google LLC. All rights reserved.

GitHub

Purpose: The IaC repository uses GitHub for source control. The IaC repository in GitHub is integrated with Cloud Build. When commits are made to the master branch, a Cloud Build job is triggered to run a set of preconfigured tasks.

Google Cloud

© 2022 Google LLC. All rights reserved.

Firestore

Firestore is a fully managed, scalable NoSQL document database that is used in this architecture to persist information related to the Recommendation IDs that are parsed by the Recommender Parser service, along with the corresponding details pertinent to Git commits.

Google Cloud

© 2022 Google LLC. All rights reserved.

Pub/Sub

Purpose: Cloud Build publishes messages on a Pub/Sub topic when your build's state changes, such as when your build is created, when your build transitions to a working state, and when your build completes.

The Pub/Sub topic to which Cloud Build publishes messages is called cloud-builds, and it is automatically created for you when you enable the Cloud Build API in your project.

© 2022 Google LLC. All rights reserved.