DevFest
Bali

2025

From Manual to Automated: Secure and Scalable VM Setup with GCE Metadata

Putu Sintia
Infrastructure Engineer, Zero One Group

Google Developer Groups

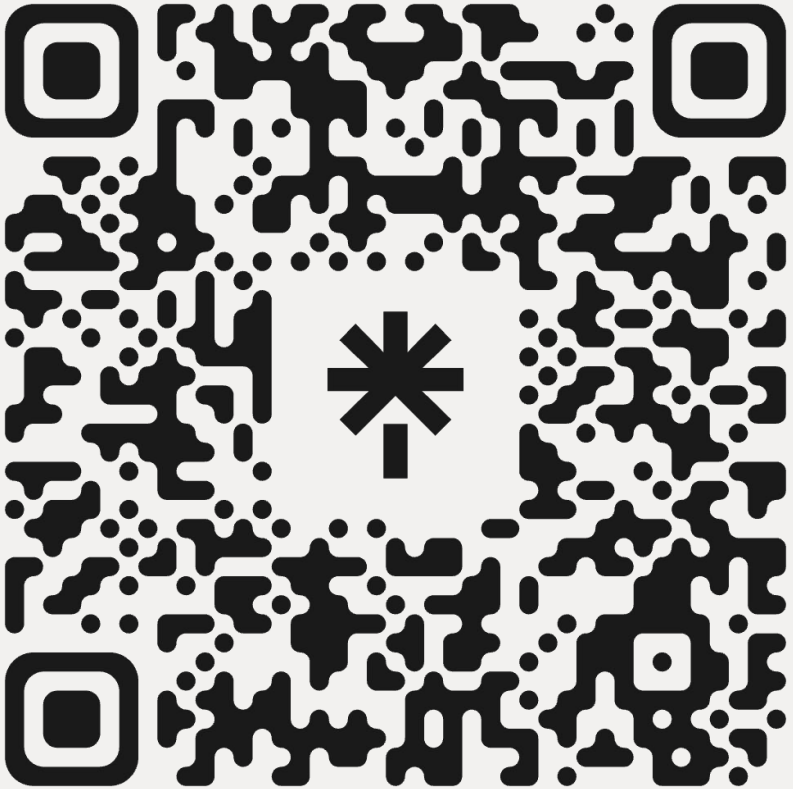
Hi!! I’m Sintia

Balinese IE with 2 years experience in cloud infrastructure, DevOps and observability.

Google Developer Groups

More about me, you can see in my linktree with scan the barcode here or go to the link below

https://linktr.ee/putusintia



Google Developer Groups

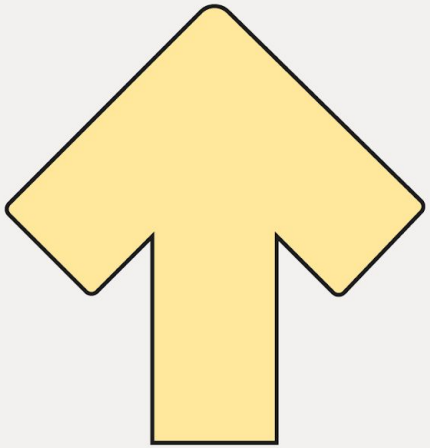
From the tech community to Indonesia—GDG stands with flood victims in Aceh and Sumatera.

https://donasi.gdgmedan.com/

Google Developer Groups

01

Kenapa Bawa Topik Ini?

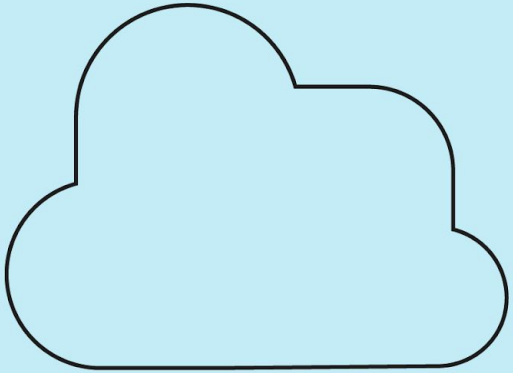


Google Developer Groups

DevFest

Bali

Metadata = Cikal Bakal Automation



Terraform, Ansible, semua IaC tools berinteraksi dengan metadata provider.

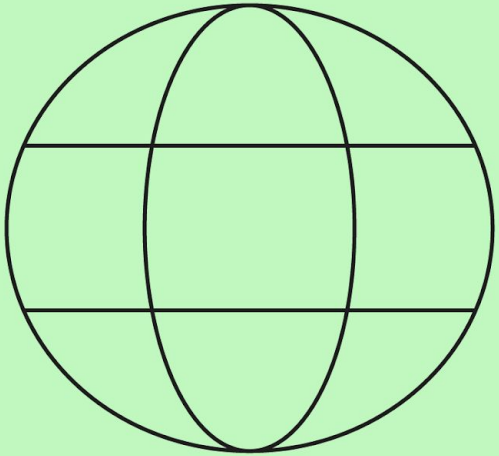
Google Developer Groups

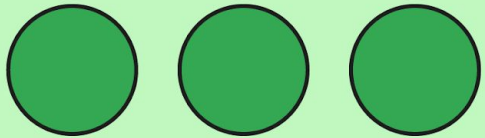
DevFest

Bali

Based Real Case: GPU Setup untuk AI Service

Startup script via metadata bisa mempersingkat flow ini secara signifikan.





Google Developer Groups

DevFest

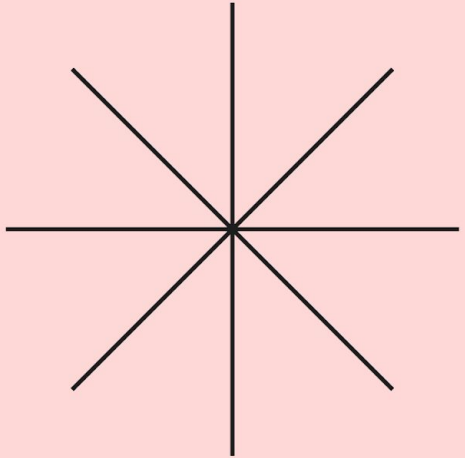
Bali

AI Can't Exist Without Compute

Compute adalah backbone Infra/DevOps

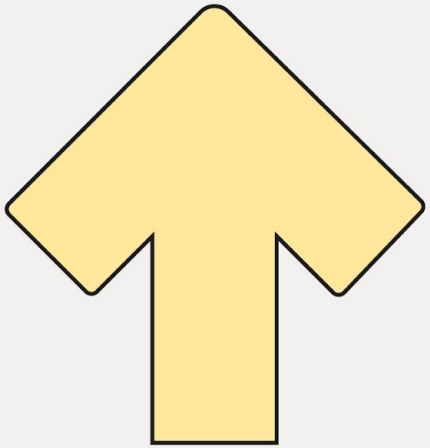
Google Developer Groups

Instead of talking about AI, why not strengthen the compute that powers it?



02

Sebelum Mulai



Fondasi yang perlu dipahami
sebelum masuk ke metadata

Google
Developer
Groups

GCP Basics

SSH Basics

Linux Command Line

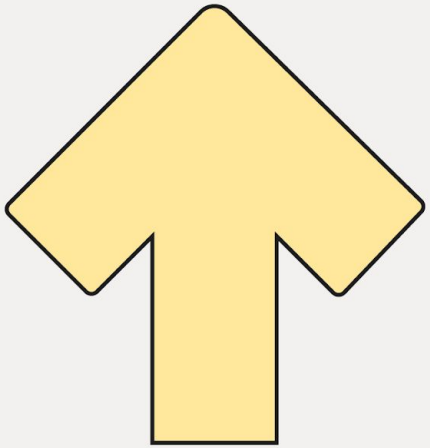
Networking Dasar

Google Developer Groups

03

The Problem

Kekacauan yang
sering terjadi...

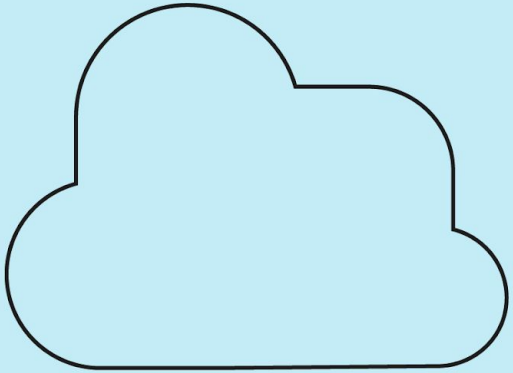


Google
Developer
Groups

DevFest

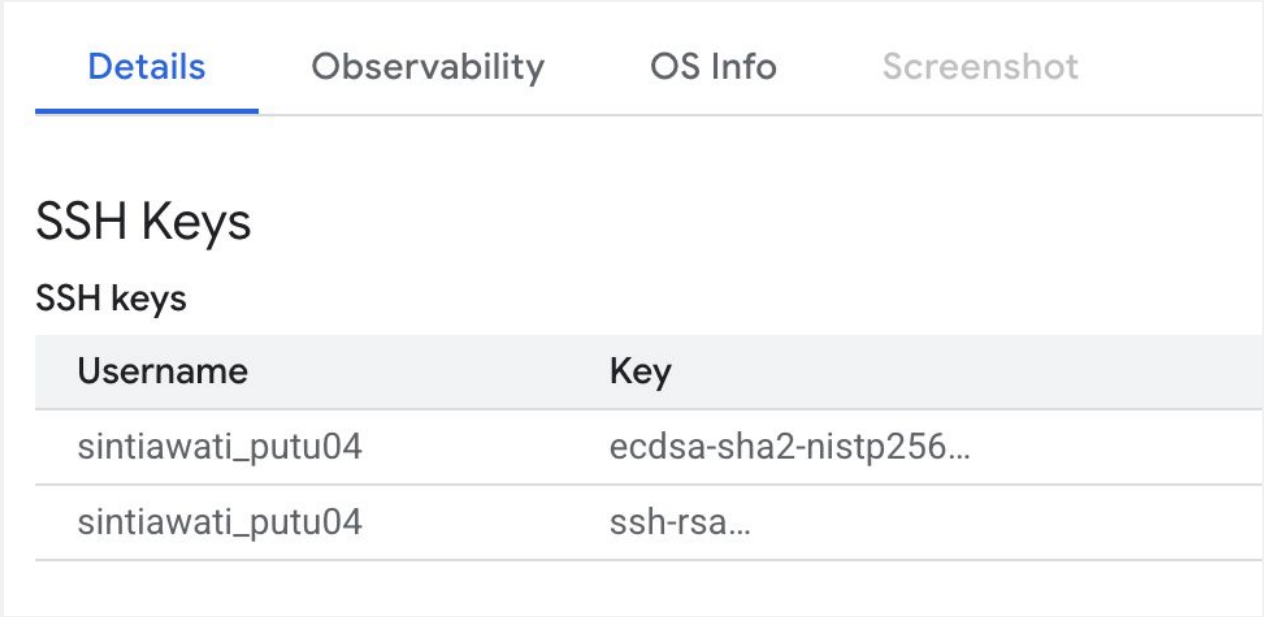
Bali

SSH Key Chaos



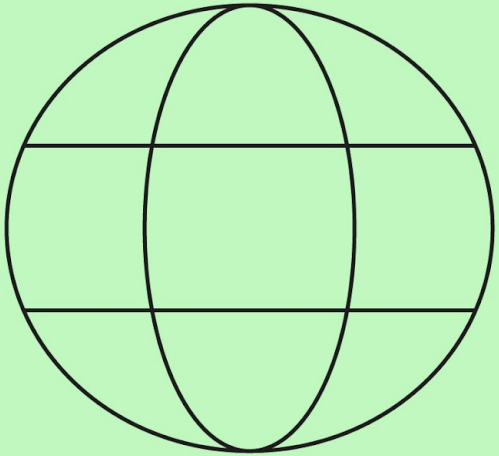
Setiap SSH via Console → key baru dibuat otomatis. **Hasilnya? Puluhan key yang tidak terkelola.**

Google Developer Groups


Details
Observability
OS Info
Screenshot
SSH Keys
SSH keys
Username
Key
sintiawati_putu04
ecdsa-sha2-nistp256...
sintiawati_putu04
ssh-rsa...

DevFest

Bali



Manual Setup

Install Docker, setup firewall, configure services.*Semua diulang manual di setiap VM baru.*

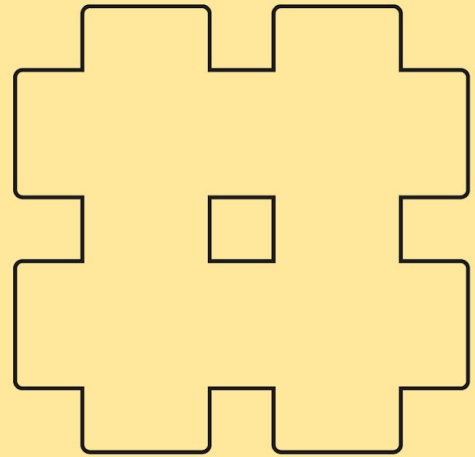
Google Developer Groups

DevFest

Bali

Security Risks

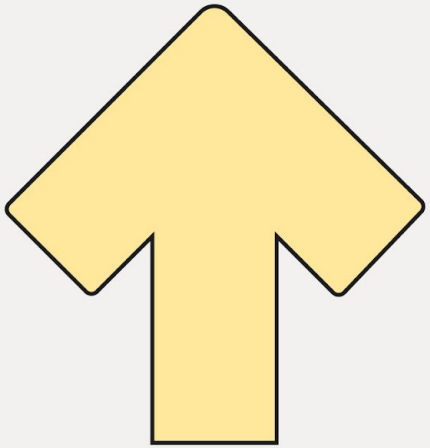
Static credentials, inconsistent configs, dan human error yang mengintai setiap deployment.



Google Developer Groups

04

GCE Metadata Server



Google
Developer
Groups

GCE Metadata Server

Apa itu Metadata Server?

Sebuah internal service yang bisa diakses oleh setiap VM di GCP tanpa perlu authentication eksternal.

http://metadata.google.internal

Apa yang bisa dilakukan?

- Kelola SSH keys secara terpusat
- Jalankan startup scripts otomatis
- Akses service account tokens
- Ambil instance metadata (zone, project, dll)

Key Insight: Semua konfigurasi VM bisa di-manage dari SATU tempat — Metadata!

Metadata Hierarchy

Project Metadata

Berlaku untuk SEMUA VM dalam project

```
/project/project-id
/project/attributes/*
```

Predefined + Custom keys

Zonal Metadata

Per zona, untuk fault isolation

```
/zones/[ZONE]/
attributes/*
```

Custom keys only

Instance Metadata

Spesifik untuk satu VM

```
/instance/name
/instance/attributes/*
```

Predefined + Custom keys

Predefined Keys

Dibuat oleh GCE otomatis: instance-id, machine-type, zone, project-id, dll.

Custom Keys

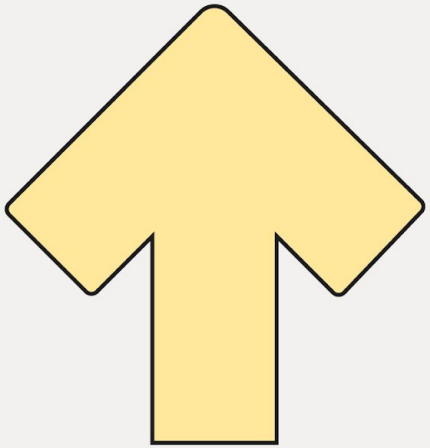
Dibuat user: startup-script, ssh-keys, environment variables, app config, dll.

Google Developer Groups

05

Building for Scalability

Otomatisasi VM bootstrapping dengan
startup-script metadata



Google
Developer
Groups

SSH KEY MANAGEMENT

Satu Key, Semua VM

❌ **SEBELUM (Console SSH)**

- Key dibuat otomatis setiap login
- Key tersebar di ~/.ssh/
- Tidak ada kontrol siapa yang akses
- Sulit di-audit dan di-revoke

✅ **SESUDAH (Metadata SSH)**

- Satu key untuk semua VM (project-wide)
- Centralized di GCP Console/API
- Mudah di-audit dan di-revoke
- Bisa per-instance jika perlu

Cara Setup SSH Key di Metadata

```
# 1. Generate key (sekali saja)
ssh-keygen -t ed25519 -C "user@company"

# 2. Format untuk metadata
username:ssh-ed25519 AAAA... user@company

# 3. Add ke project metadata
gcloud compute project-info \
add-metadata --metadata-from-file \
ssh-keys=./ssh-keys.txt
```

Otomatisasi dari Boot Pertama

Apa itu Startup Script?

Script yang dijalankan otomatis saat VM boot.

Perfect untuk initial setup!

Use Cases:

- Install packages (Docker)
- Configure firewall rules
- Pull dan run containers
- Setup monitoring agents

startup-script.sh

```
#!/bin/bash
apt-get update -y
# Install Docker
curl -fsSL https://get.docker.com | sh
systemctl enable docker
systemctl start docker
# Run application
docker run -d -p 80:80 nginx
echo "Done!" | logger
```

Google Developer Groups

Debugging Startup Scripts

Ketika script tidak jalan sesuai harapan...

1. Via journalctl (SSH)
Paling detail, bisa lihat output dan error.

2. Via Serial Port (Console)
Berguna kalau SSH belum bisa.

3. Via Cloud Logging
Centralized, query across VMs.

Debugging Commands

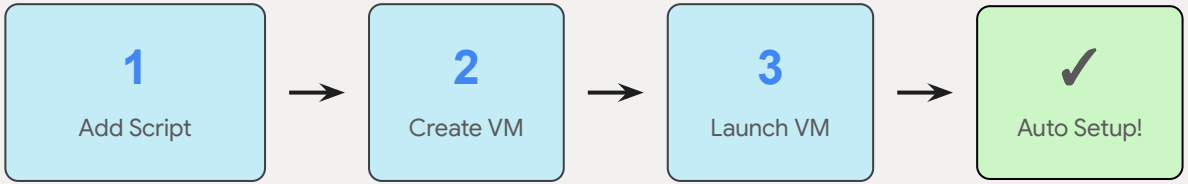
```
# Method 1: journalctl
sudo journalctl -u google-startup-scripts.service

# Filter by tag
sudo journalctl -t startup-script

# Method 2: Serial port
gcloud compute instances get-serial-port-output VM

# Method 3: Cloud Logging
gcloud logging read "resource.type=gce_instance"
```

Google Developer Groups

LIVE DEMO

Instance + Docker

Membuat VM yang otomatis install dan run Docker container saat boot



Access here for see snippets command to use during demo

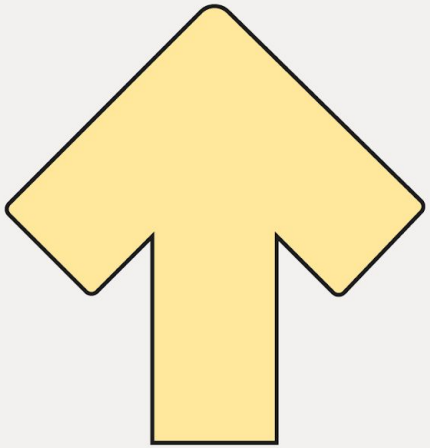
https://s.id/GaBMO

Google Developer Groups

06

Building for Security

Keyless authentication dengan Service Account



Google Developer Groups

SERVICE ACCOUNT

Keyless Authentication

Kenapa Service Account?

- Tidak perlu manage JSON key files
- Automatic token rotation
- Granular IAM permissions
- Audit trail yang jelas

Cara Kerja:

VM mengakses Metadata Server untuk mendapatkan short-lived access token. Token auto-refresh setiap ~1 jam.

Akses GCS dari VM tanpa key file

```
# Get token dari metadata server
curl -H "Metadata-Flavor: Google" \
  "http://metadata.google.internal/
  computeMetadata/v1/instance/
  service-accounts/default/token"

# Atau lebih simple dengan gcloud:
gcloud storage cp file.txt gs://bucket/

# gcloud otomatis pakai attached SA!
# No credentials needed
```

Security Best Practices

Prinsip keamanan untuk GCE Metadata

Least Privilege

Berikan Service Account hanya permission yang dibutuhkan. Hindari Editor/Owner role.

No Static Keys

Jangan download JSON key. Gunakan attached Service Account dan Metadata Server.

Block Project SSH

Set metadata block-project-ssh-keys=TRUE untuk VM sensitif.

Audit Regularly

Review SSH keys dan Service Account permissions secara berkala.

Wait-for-Change Feature

Apa itu?
Request yang menunggu hingga metadata berubah. React terhadap config changes secara real-time.

Use Cases
Dynamic config reload, feature flags, rolling updates, maintenance notifications.

Basic Wait-for-Change

```
# Request blocks sampai berubah
curl -H "Metadata-Flavor: Google" \
".../attributes/my-config\
?wait_for_change=true"
# Dengan timeout
?wait_for_change=true&timeout_sec=60
```

With ETag (Avoid Race)

```
# 1. Get current ETag
curl -v ... # Response: ETag: abc123
# 2. Wait with last_etag
?wait_for_change=true&
last_etag=abc123
```

Google Developer Groups

Tools & SDK

Library untuk mempermudah akses metadata

Go Go SDK

```
import
"cloud.google.com/go/
compute/metadata"

metadata.ProjectID()
metadata.InstanceName()
```

JS Node.js

```
const
gcpMetadata =
require('gcp-metadata')

gcpMetadata.project('id')
gcpMetadata.instance()
```

Py Python

```
import
google.auth.compute_engine
._metadata as metadata

metadata.get(client, 'path')
```

Environment Variables

GCE_METADATA_HOST

Custom metadata server host (untuk testing/emulator)

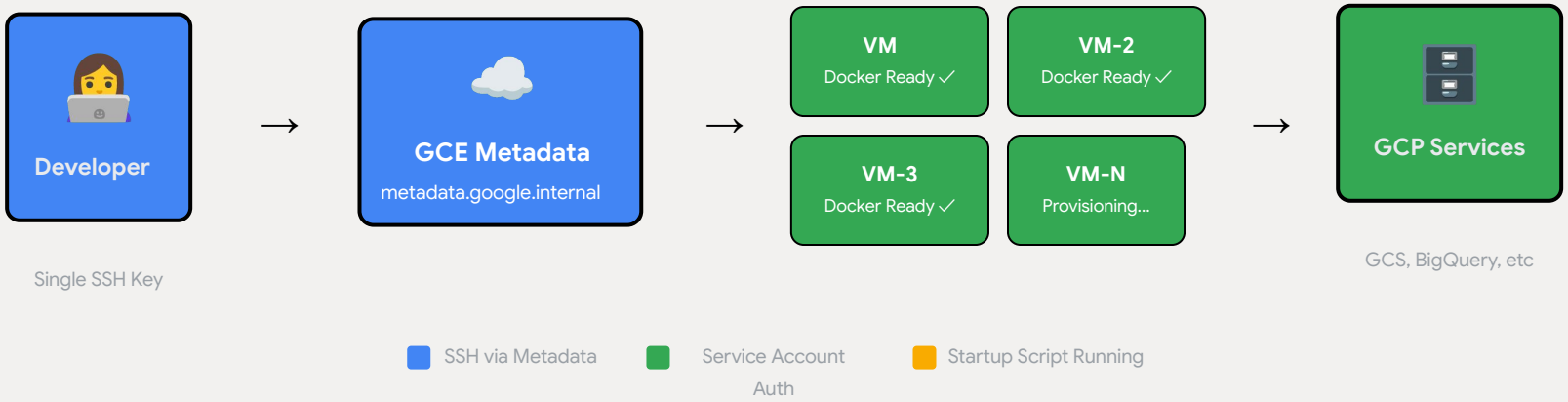
METADATA_SERVER_DETECTION

assume-present, none, bios-only, ping-only

📦 Go: pkg.go.dev/cloud.google.com/go/compute/metadata

📦 Node: github.com/googleapis/gcp-metadata

Putting It All Together



Google Developer Groups

Key Takeaways

1. **GCE Metadata adalah pusat kontrol VM**

   Gunakan untuk SSH keys, startup scripts, dan instance configuration

2. **Startup scripts = Repeatable infrastructure**

   Kombinasikan dengan Instance Template untuk scalability

3. **Service Account = Keyless, secure authentication**

   Tidak perlu manage JSON keys, token auto-refresh

4. **Always apply least privilege principle**

   Audit SSH keys dan SA permissions secara berkala

Google Developer Groups

Thank You!

Questions? Let's discuss!

Putu Sintia
Infrastructure Engineer
Zero One Group

sintiawati.putu04@gmail.com
linkedin.com/in/putusintia

Google Developer Groups