Operations Suite and Security
in Google Cloud

bangkit

Ground Rules

Observe the following rules to ensure a supportive, inclusive, and engaging classes

Give full attention in class

Mute your microphone when you're not talking

Keep your camera on

Turn on the CC Feature on Meet

Use raise hand or chat to ask questions

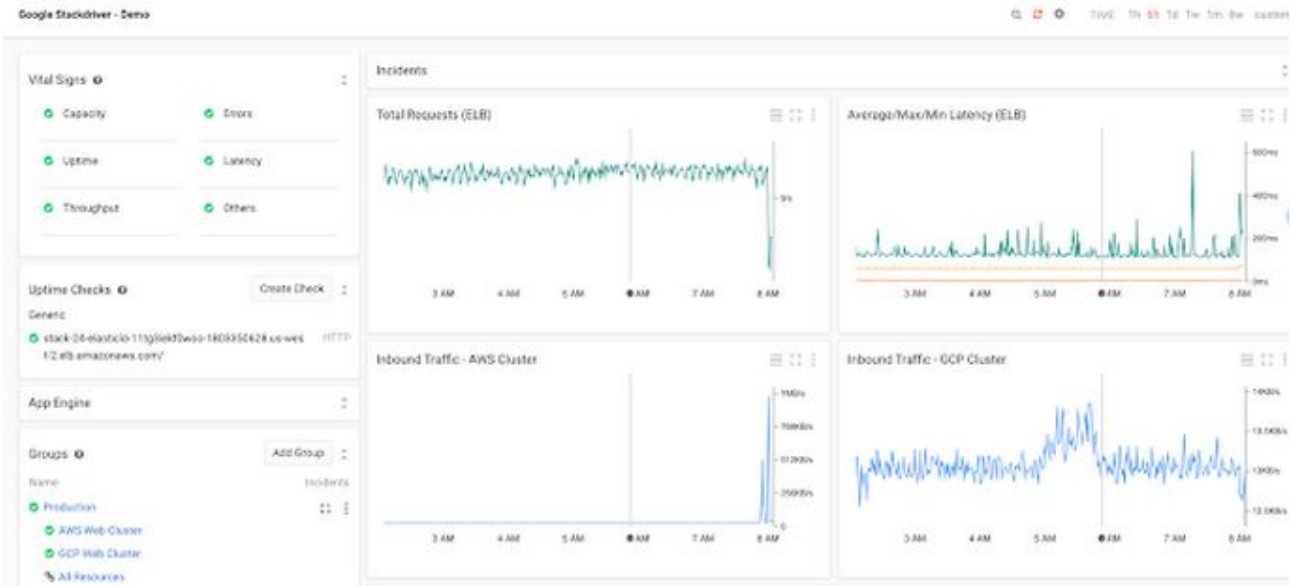
Make this room a safe place to learn and share

bangkit

Google Cloud Operations Suite

Google Cloud Operations Suite (formerly Stackdriver)

Integrated monitoring, logging, and trace managed services for applications and systems running on Google Cloud and beyond.



bangkit

Why use Cloud Operations?

Increase Agility

Realtime observability

Need automation for standardization

Reliability at Scale

The tools should scale with the growth of business

Support DevOps/SRE practices

Breakdown Silos

Quick navigation from metrics and dashboards for troubleshooting

Metrics and logs should drive business insights

Improve Security

Metrics and logs storage is more secure

Can easily be retained for years for compliance purpose

bangkit

Tools Included in the Google Cloud Operations Suite

Monitoring

Platform, system & app metrics
Uptime/Health Checks
Dashboards
Alerts

Logging & Error Reporting

Platform, system & app logs
Log search/view/filter
Logs-based metrics

Error Notification
Error Dashboard

Trace, Debugger, Profiler

Latency reporting

Production debug snapshots
Conditional snapshots
IDE integration

Continuous profiling of CPU & Memory

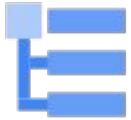
Cloud Monitoring

Gain visibility into the performance, availability, and health of your applications and infrastructure.

bangkit

Cloud Monitoring Features

- Identify trends, prevent issues
- Reduce monitoring overhead
- Improve signal-to-noise
- Fix problems faster
- Throw alert to mail and others



Cloud Logging

Fully managed, real-time log management with storage, search, analysis and alerting at exabyte scale.

bangkit

Cloud Logging Features

- Seamlessly resolve issues
- Scalable and fully managed
- All cloud logs in one place
- Real-time insights

Error Reporting

Identify and understand your application errors.

bangkit

Error Reporting Features

- Quickly understand errors
- Automatic and real-time
- Instant error notification
- Popular languages

Cloud Trace

Find performance bottlenecks in production

bangkit

Cloud Trace Features

- Find performance bottlenecks
- Fast, automatic issue detection
- Broad platform support

Cloud Debugger

Investigate your code's behavior in production.

Cloud Debugger Features

- Debug in production
- Multiple source options
- Collaborate while debugging
- Use your workflows

Cloud Profiler

Continuous CPU and heap profiling to improve performance and reduce costs.

bangkit

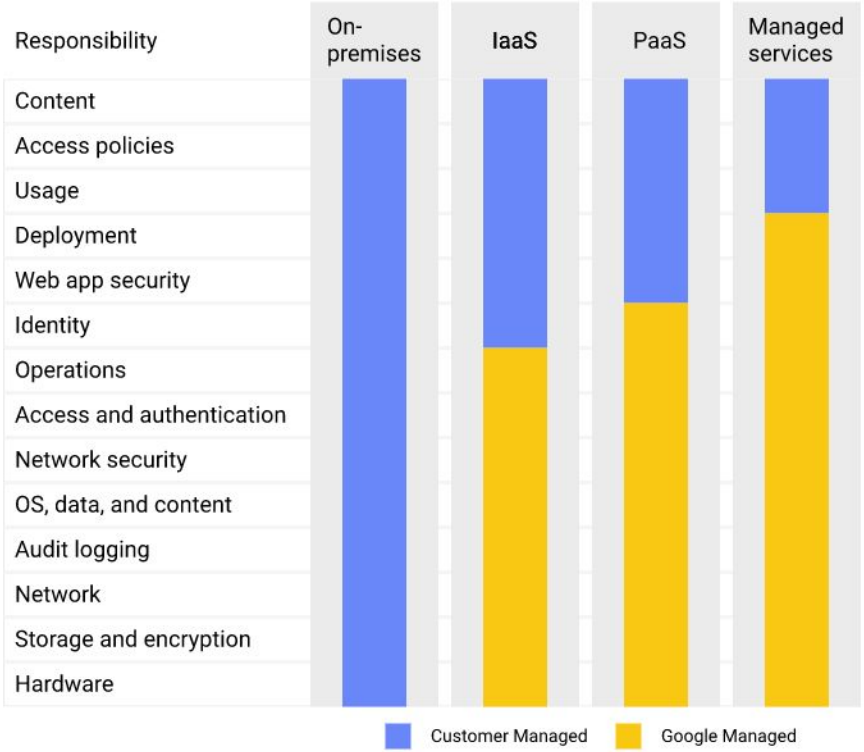
Cloud Profiler Features

- Low-impact production profiling
- Broad platform support

Securing Your Cloud

bangkit

Security is a shared responsibility



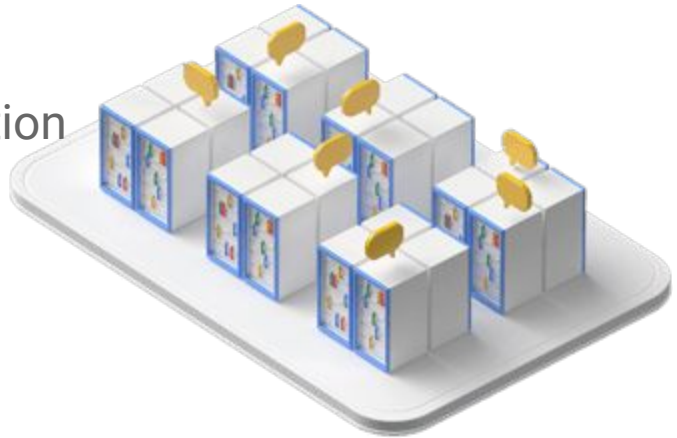
bangkit

Google's Multi-layered Security

- **Hardware Infrastructure**
  - Secure Boot Stack and Machine Identity
  - Hardware Design and Provenance
  - Security of Physical Premises
- Service Deployment
- Storage Services
- User Identity
- Internet Communication
- Operational Security

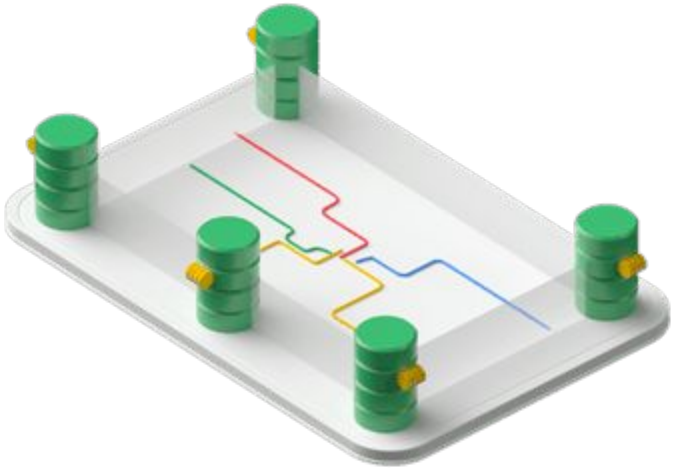
Google's Multi-layered Security

- Hardware Infrastructure
- **Service Deployment**
  - Access Management of End User Data
  - Encryption of Inter-Service Communication
  - Inter-Service Access Management
  - Service Identity, Integrity, and Isolation
- Storage Services
- User Identity
- Internet Communication
- Operational Security



Google's Multi-layered Security

- Hardware Infrastructure
- Service Deployment
- **Storage Services**
  - Encryption at rest
  - Deletion of Data
- User Identity
- Internet Communication
- Operational Security

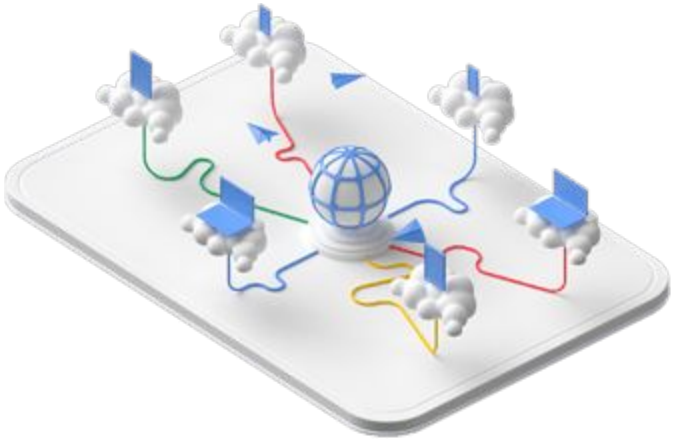


Google's Multi-layered Security

- Hardware Infrastructure
- Service Deployment
- Storage Services
- **User Identity**
  - Authentication
  - Login Abuse Protection
- Internet Communication
- Operational Security

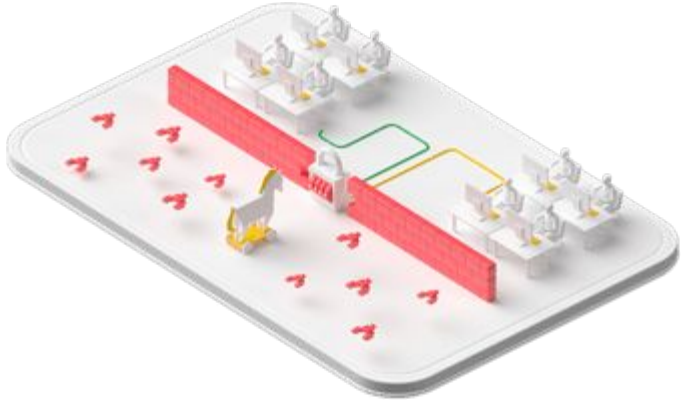
Google's Multi-layered Security

- Hardware Infrastructure
- Service Deployment
- Storage Services
- User Identity
- **Internet Communication**
  - Google Front End
  - DoS Protection
- Operational Security



Google's Multi-layered Security

- Hardware Infrastructure
- Service Deployment
- Storage Services
- User Identity
- Internet Communication
- **Operational Security**
  - Intrusion Detection
  - Reducing Insider Risk
  - Safe Employee Devices & Credentials
  - Safe Software Development



Watch Video: Google Data Center Security

bangkit

Cloud IAM

- It answers “who can do what on which resource”
- To grant people access to your projects, add them as member:
  - Gmail accounts and Google Groups
  - Users and groups in G Suite domain
  - Users and groups in Cloud Identity domain
  - Service accounts

Permissions & Roles

- In order to perform operations on a resource, members need to have permissions.
- Permissions written in the following format: **<service>.<resource>.<verb>**. I.e. **compute.instances.create**.
- Permission is not assigned to identity, but given to roles.
- Roles are simply a list of permissions.

Understanding Roles in GCP

- Basic role
  - I.e., Viewer, Editor, Owner.
- Predefined role
  - InstanceAdmin
    - compute.instances.delete
    - compute.instances.get
    - compute.instances.list
    - compute.instances.start
    - …
  - StorageObjectCreator
    - resourcemanager.projects.get
    - resourcemanager.projects.list
    - storage.objects.create
- Custom role

Service Accounts

A service account is a special kind of account used by an application or a virtual machine (VM) instance, not a person.

For example, a Compute Engine VM may run as a service account, and that account can be given permissions to access the resources it needs. This way the service account is the identity of the service, and the service account's permissions control which resources the service can access.

Resource Hierarchy

- You can set IAM policies at different levels of the resource hierarchy (Project, Folder, or Org Node).
- Resources can inherit policies from parent.
- A less restrictive parent policy overrides a more restrictive resource policy.

Sharing Session

Quiz

Discussion

Thank You

bangkit