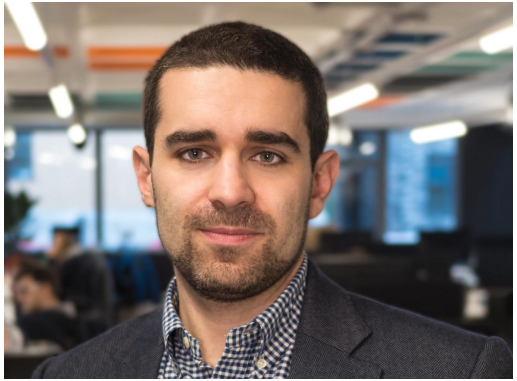
CONTINO

GCP Cloud Foundations

#whoami



Federico Fregosi
Current: Principal Consultant - Technical

Past:

federico.fregosi@contino.io

https://www.linkedin.com/in/federico-fregosi/

About Contino

Contino is a leading transformation consultancy that helps large, heavily-regulated enterprises to become fast, agile and competitive.

360+
People

The deepest pool of DevOps, data & cloud transformation talent in the industry

5
Global offices

We can scale rapidly to support diverse client requirements across the globe

300+
Engagements

More DevOps transformation executed than any other professional services firm

150+
Customers

Specializing in helping the world's leading brands accelerate digital transformation

Ministry of Justice · Allianz · vodafone · BARCLAYS · adidas · HSBC · verizon

Agenda

01 | Cloud Foundations

02 | Organization Structure & Resource Deployment

03 | Authentication & Authorization

04 | Networking

05 | Secrets Management

06 | Logging

07 | Operating Model

08 | FinOps - Billing

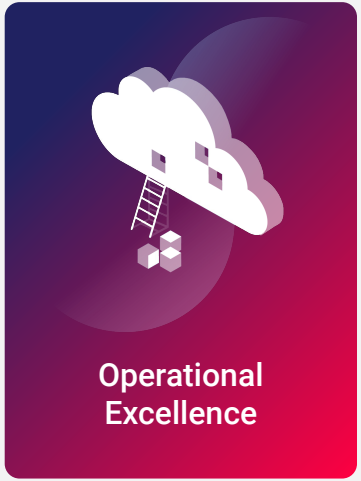
09 | Q&A

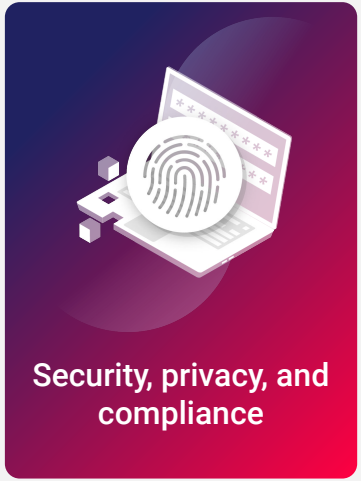
Why Do You Need Cloud Foundations?

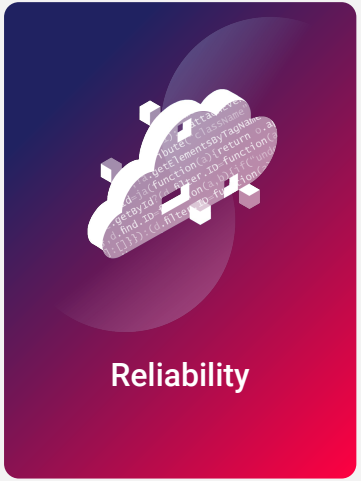
Landing zones enable management of standardised GCP projects, which in turn control your Virtual Private Clouds (VPCs) and consumption of GCP cloud services.

- **Prevents Project Sprawl:** Project provision can be managed as cloud engagement increases
- **Minimises Engineering Overhead**: Eliminating manual changes reduces complexity and enables scalability and consistency
- **Enables Scaling by Design**: Management of services and infrastructure in public cloud is made simple by the use of a well-designed landing zone
- **Accelerates Consumption of Cloud Services**: Allows for GCP projects to be provisioned with a standard set of tooling and services

Core Features







Aligned with "Best practices" and the 5 pillars of "Google Cloud's Architecture Framework" principles

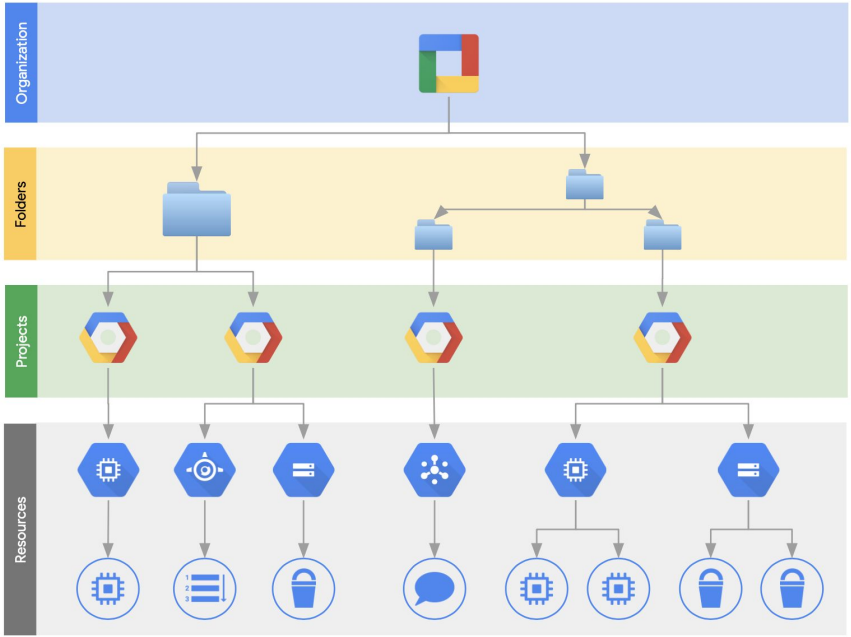
What is a Landing Zone?

GitHub solutions

- https://github.com/terraform-google-modules/terraform-google-project-factory
- https://github.com/terraform-google-modules/terraform-example-foundation
- https://github.com/contino/terraform-gcp-modules
- https://github.com/GoogleCloudPlatform/cloud-foundation-toolkit

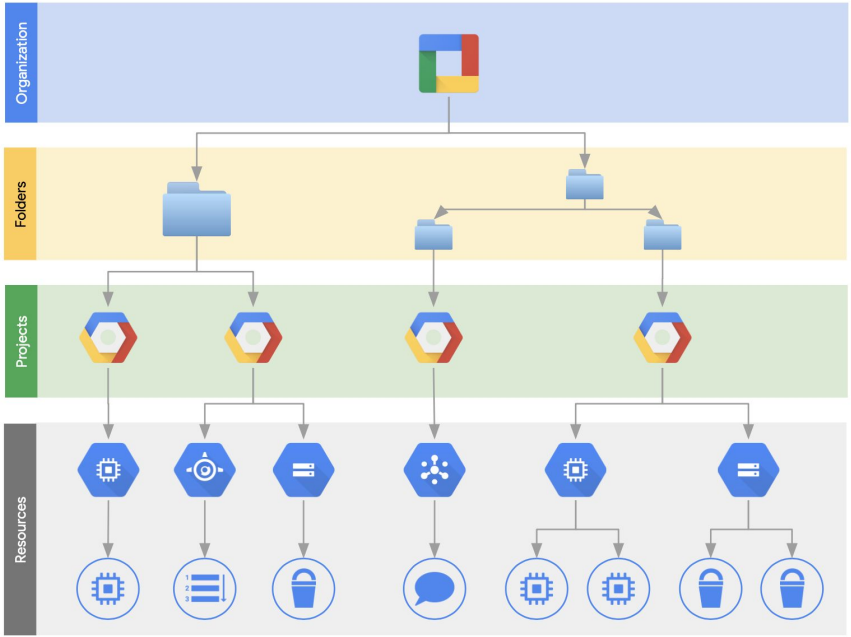
Organization Structure

GCP Resource Management



- [Cloud Resource Manager](#) provides project management & IAM functionality
- The top level component is the GCP organization.
- An organization is tied to a GSuite OR a Cloud Identity account
- Most of the available resources are deployed into a project.
- A project is the main isolation “container” in GCP

GCP Resource Management



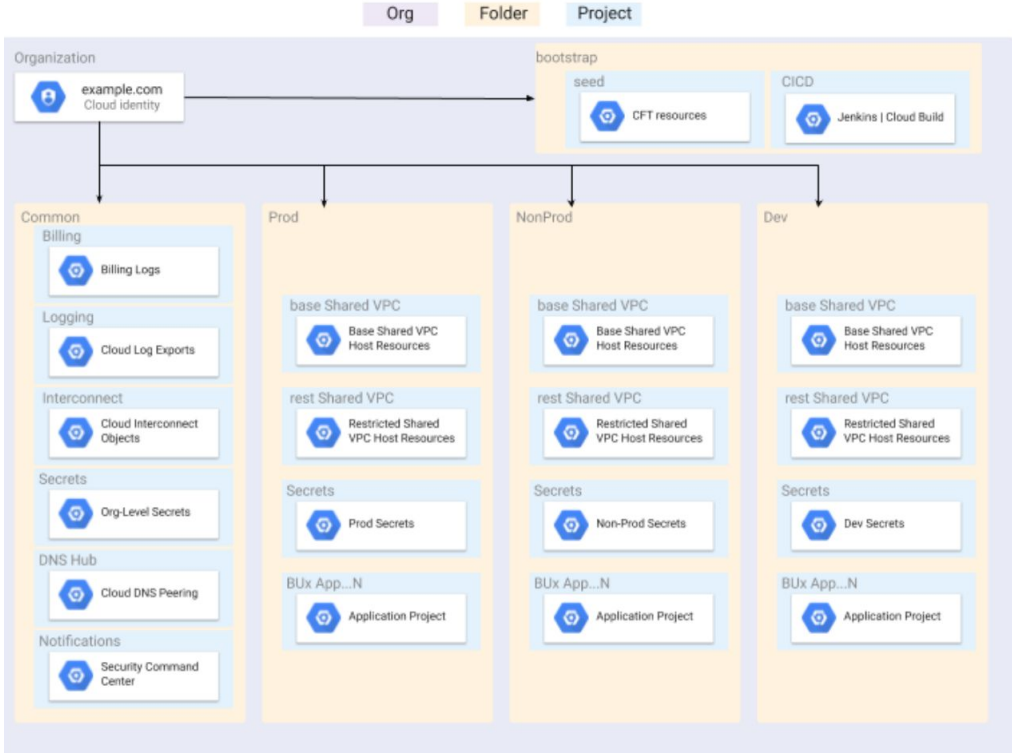
Top-down access inheritance: Additive only

The **effective policy** for a resource is the union of the policy set at that resource and the policy inherited from its parent.

Cloud Resource Manager: Organization Hierarchy

The Common folder will include the following baseline projects:

- **Interconnect** - connectivity between an enterprise's on-premises environment and Google Cloud.
- **DNS Hub -** central point of communication between an enterprise's on-premises DNS system and Cloud DNS.
- **Notifications -** managing Security Command Center alerting.
- **Logging -** destination for log sink and detective controls.
- **Secrets -** organization-level secrets.



Organisation Policies

The **Organization Policy Service** constrains the allowed resource configurations. Policies can be applied to the **Organisation**, **Folders**, and **Projects**.

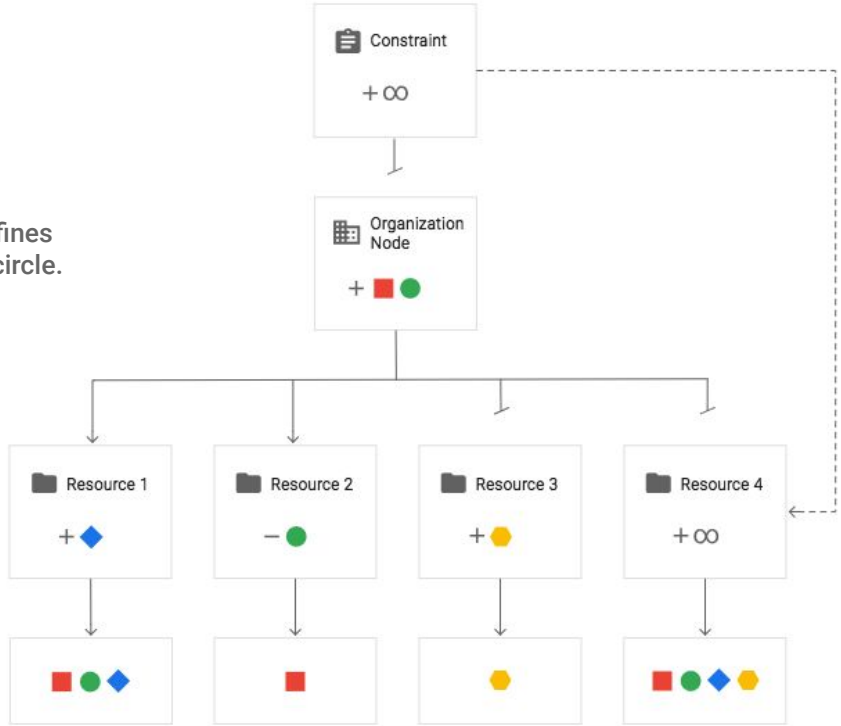
*Requires IAM role: Organization policy / organization policy administrator

Organization Policy Hierarchy Evaluation

In this example, the **Organization Node** defines a policy that allows red square and green circle.

Resource 1 defines a custom policy that sets inheritFromParent to TRUE and allows blue diamond. The effective policy evaluates to allow red square, green circle, and blue diamond.

Resource 2 defines a custom policy that sets inheritFromParent to TRUE and denies green circle. Deny takes precedence. The effective policy evaluates to allow only red square.



Resource 3 defines a custom policy that sets inheritFromParent to FALSE and allows yellow hexagon. The effective policy evaluates to only allow yellow hexagon.

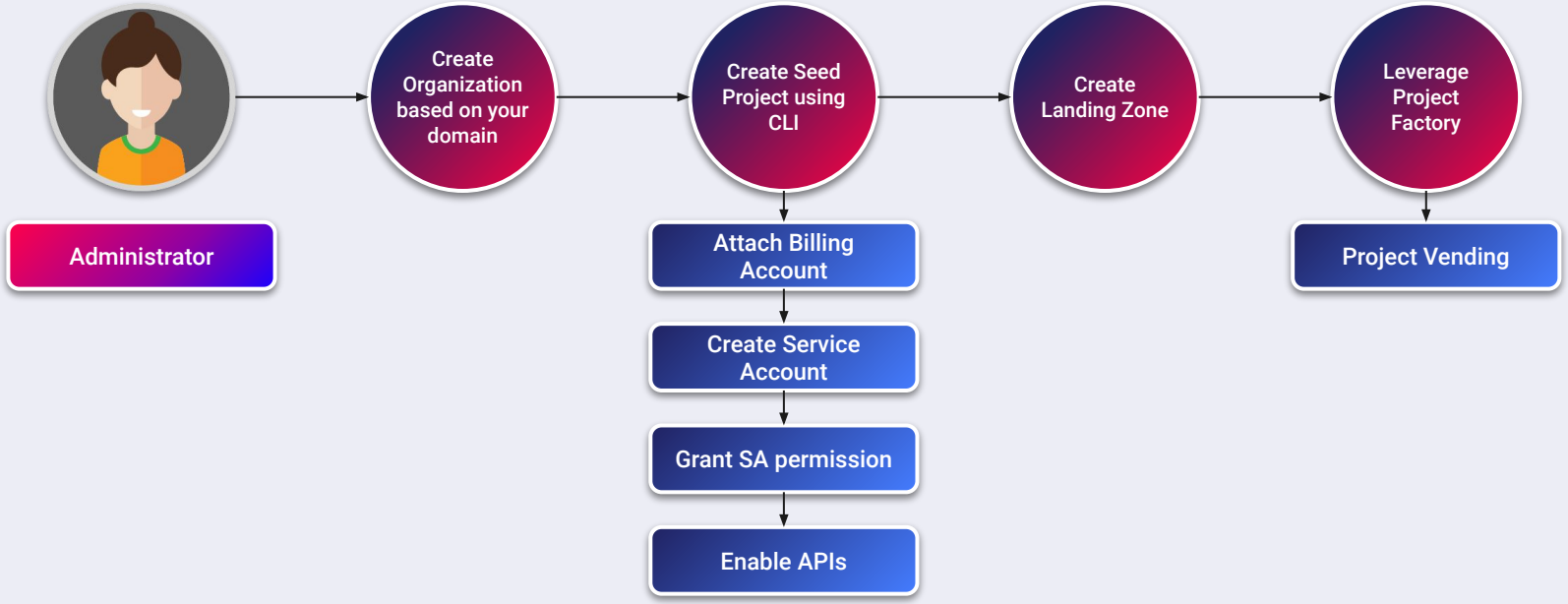
Resource 4 defines a custom policy that sets inheritFromParent to FALSE and includes the restoreDefaultvalue. The default constraint behavior is used, so the effective policy evaluates to allow all.

Note: The exceptions are always set by org-level Organization Policy roles, and not by project-level roles.

Resource Deployment

Cloud Fundations Creation

The seed project contains the Terraform state of the foundation infrastructure, a highly privileged service account that's able to create new infrastructure, and the encryption configuration to protect that state.



Project Factory

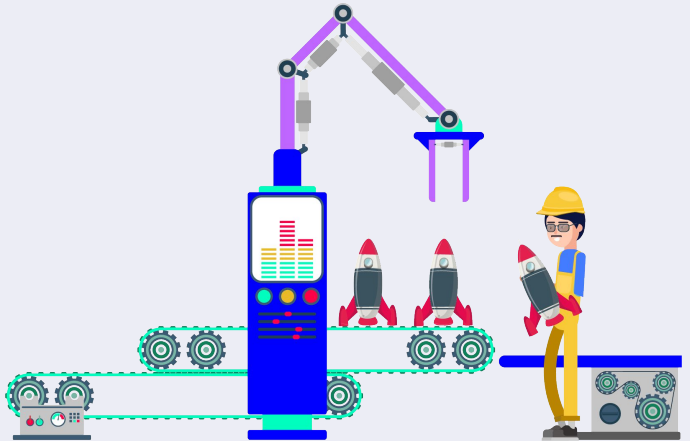
Project creation is a repetitive task.

Projects should be configured to consistently meet the organization needs:

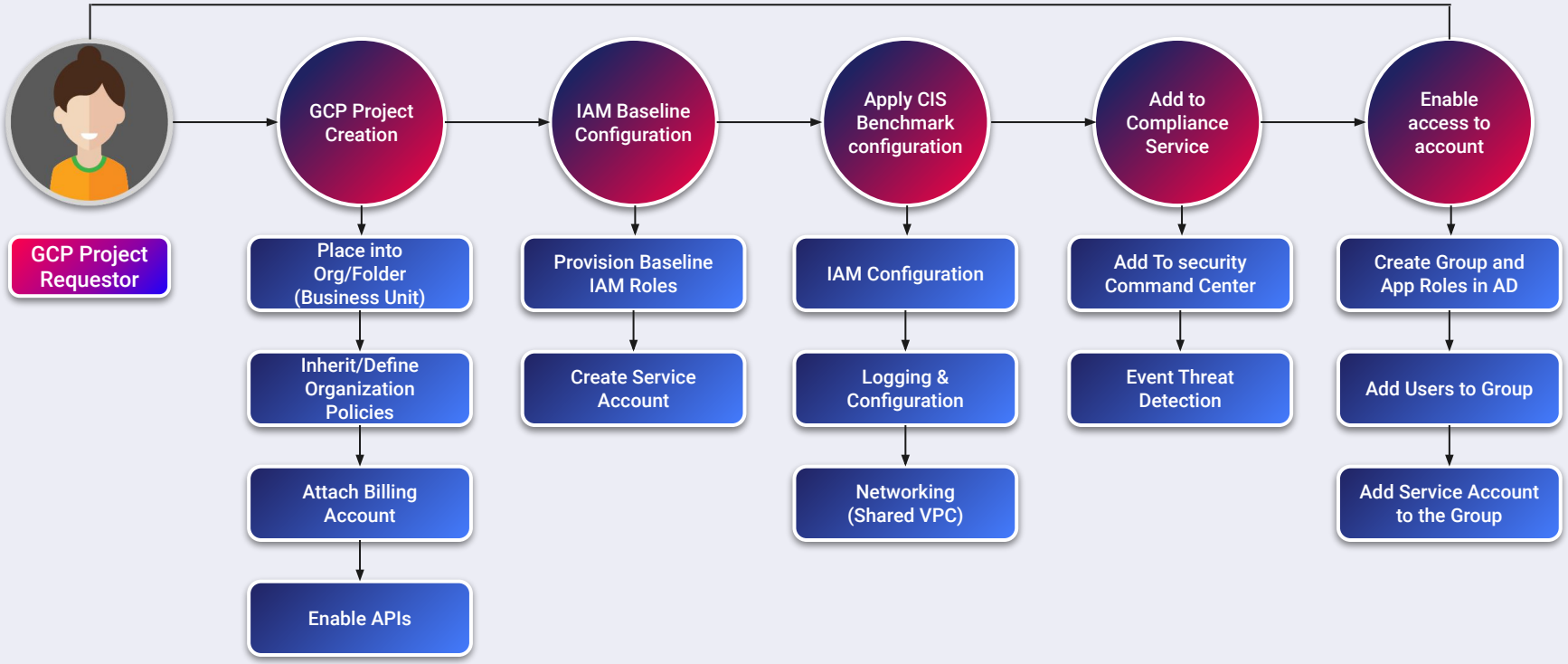
- Project ID/name naming convention
- Billing account linking
- Networking configuration
- Enabled APIs/services
- Compute Engine access configuration
- Exporting logs and usage reports
- Project removal line
- And more

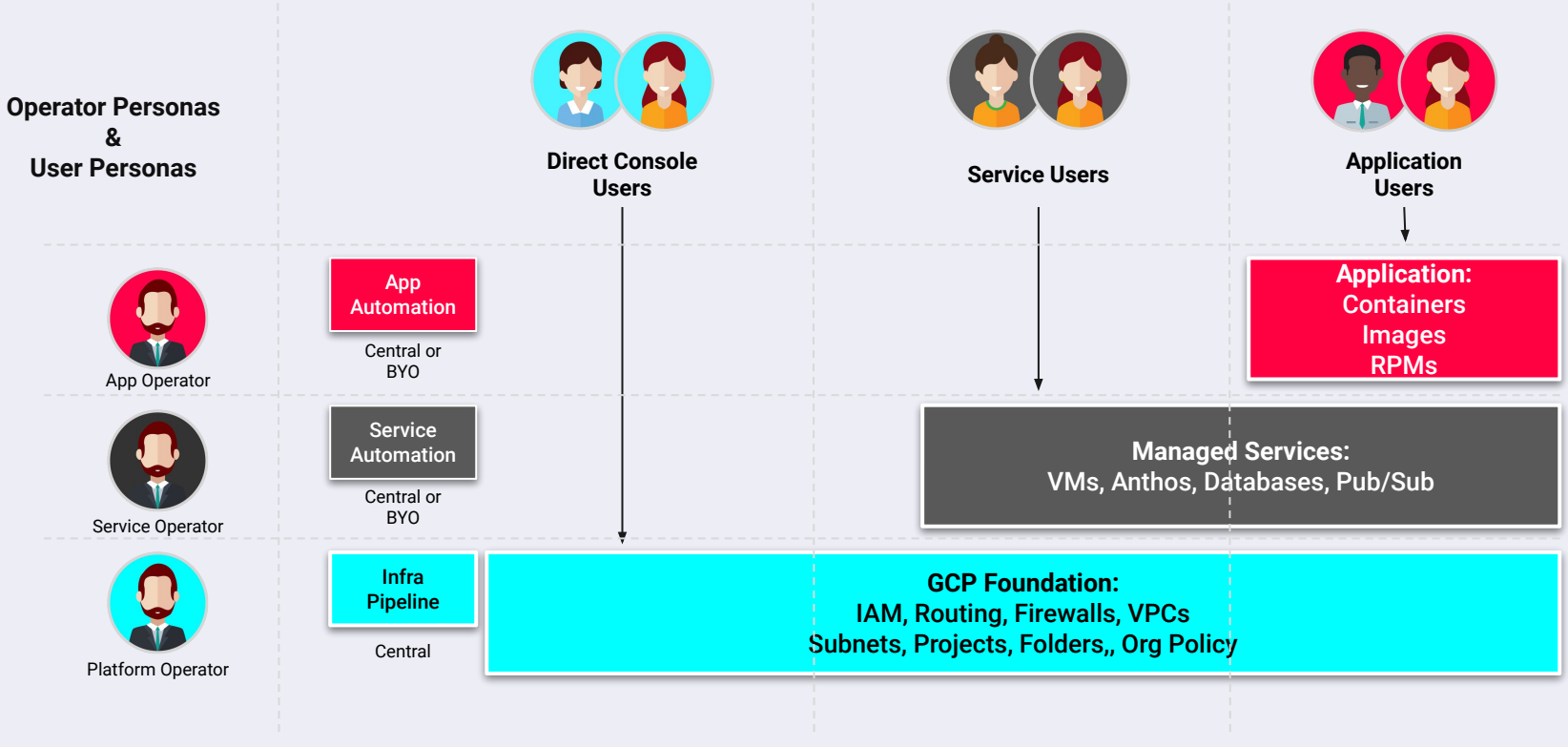
Automatic

Projects are created automatically and consistently based on Infrastructure as Code methodology (Terraform and advanced project vending).

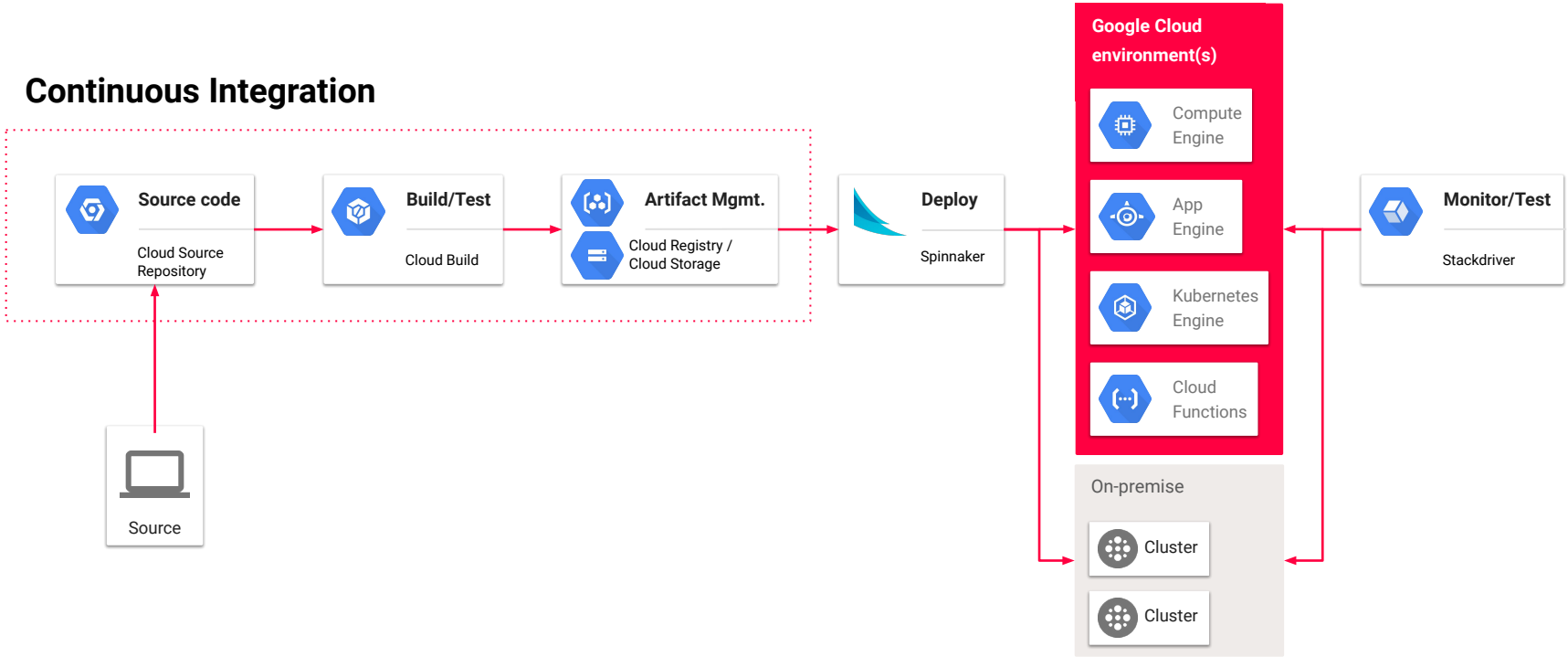


Project Factory - Vending Process




Operator Personas
&
User Personas
Direct Console Users
Service Users
Application Users
App Operator
App Automation
Central or BYO
Application: Containers Images RPMs
Service Operator
Service Automation
Central or BYO
Managed Services: VMs, Anthos, Databases, Pub/Sub
Platform Operator
Infra Pipeline
Central
GCP Foundation: IAM, Routing, Firewalls, VPCs Subnets, Projects, Folders,, Org Policy

Continuous Integration and Delivery on GCP



Application CI/CD - Supporting Services

Cloud Source Repos

- Private Git repositories **hosted on Google Cloud**
- Easily **perform Git operations** required by your workflow
- **Sync** to existing GitHub or Bitbucket repo

Cloud Build

- **Hosted** build execution on Google Cloud
- **Build** container images or non-container artifacts
- **Trigger** new builds based on changes to CSR or other repo

Container Registry

- **Hosted image repository**
- **Push builds** to Container Registry from Cloud Build
- Analyze images to
- **Discover vulnerabilities**

Spinnaker

- Open source, multi-cloud **application deployment platform**
- **Built-in best practices** for deployment
- **Supports many deployment** best practices

Container Analysis API

- **Store, query, and retrieve critical metadata** about software artifacts
- **Query all metadata** across all of your components in real time

Implementing Changes

The toolkit encourages customers to collaborate on infrastructure through a compliant and secure platform.

Developer submits **pull request**

CI runs **validation**

Administrator reviews for **policy compliance**

Administrator merges the **new config**

CI/CD updates **deployed infrastructure**

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

Continuous Compliance. It’s always green.

Authentication & Authorization

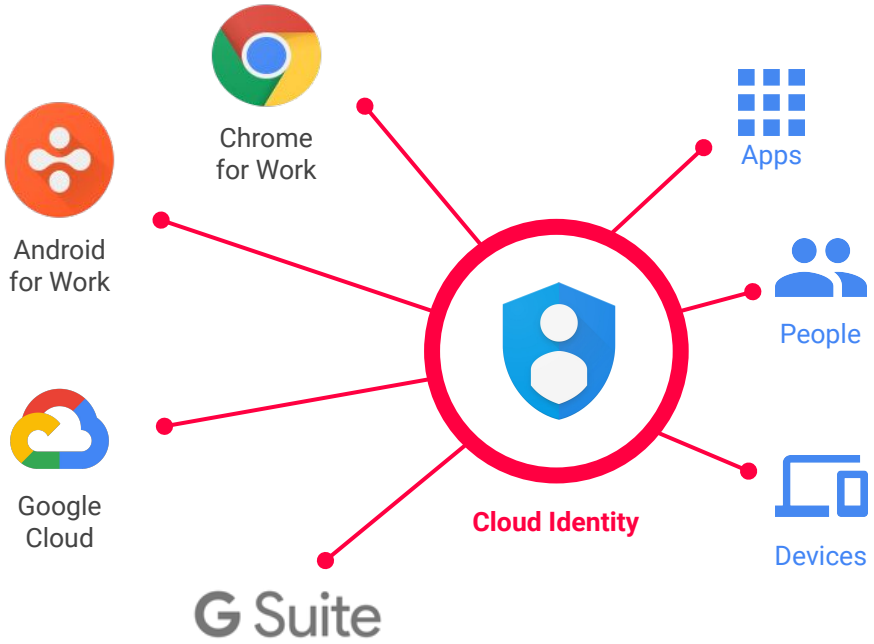
Authentication & Authorization

In order to ensure a consistent and secure manner of accessing the cloud environment and the various resources under the scope of the Landing Zone implementation, the following aspects will be considered and included in the initial landing zone deployment.

Components

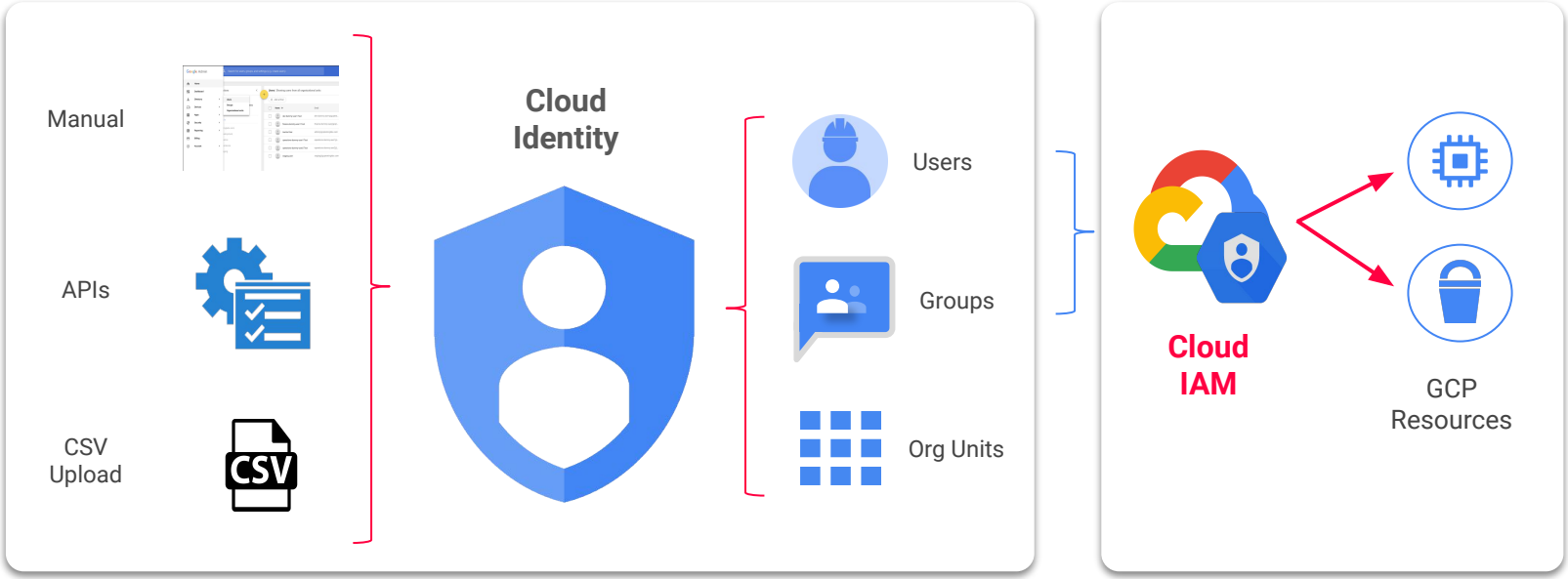
- **Native user and group management:** Cloud identity provides unified identity, access, app, and endpoint management (IAM/EMM) platform.
- **Active Directory integration and Single Sign-on (SSO):** By leveraging Google Directory Sync, we can map Active Directory forests, domains, users, and groups to Cloud Identity entities
- **Roles and permissions:** Standardised IAM roles and permission policies will be created to satisfy the principle of least privilege.

Cloud Identity



- Cloud Identity is an Identity as a Service (IDaaS) solution that **allows you to centrally manage users and groups** who can access Google Cloud and G Suite cloud resources
- It is the same identity service that powers G Suite and can also be used as IdP for 3rd party applications (supports SAML and LDAP applications)

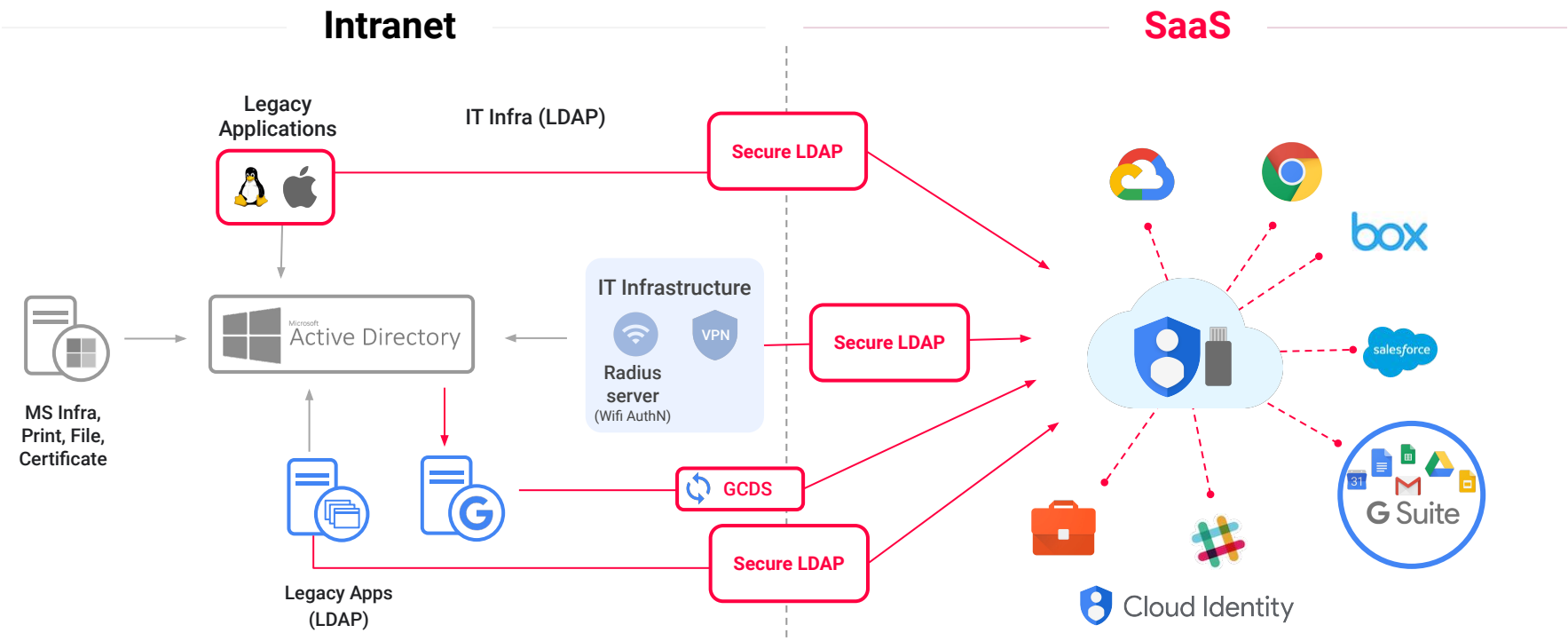
Cloud Identity



Users and groups created in Cloud Identity are the **Google Identities** that *can* be assigned **IAM roles** in the GCP console

The *Cloud Identity roles* only manage aspects of Cloud Identity such as user/group management, *and are different from GCP roles* which manage permissions to cloud resources

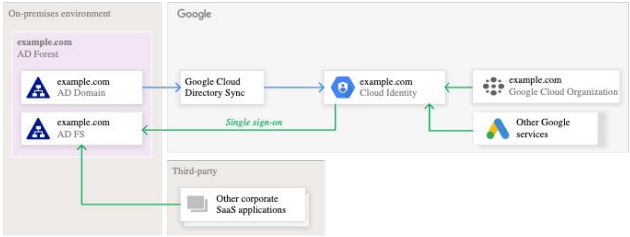
Cloud Identity - Typical Architecture



Active Directory Integration

While Cloud Identity provides the necessary functionality to manage Google identities (users and groups) for use in a GCP environment, this might add unnecessary overhead for customers with existing on-premises AD deployments. The following steps are required for AD integration setup:

- **Provisioning users -** Relevant users and groups are one-way synchronized periodically from Active Directory to Cloud Identity. This process **does not sync passwords** as all authentication will be done through the on-premises Active directory
- **Single Sign-on -** Whenever a user needs to authenticate, Google Cloud delegates the authentication to Active Directory by using the Security Assertion Markup Language (SAML) protocol. This delegation ensures that only Active Directory manages user credentials and that any applicable policies or multi-factor authentication (MFA) mechanisms are being enforced

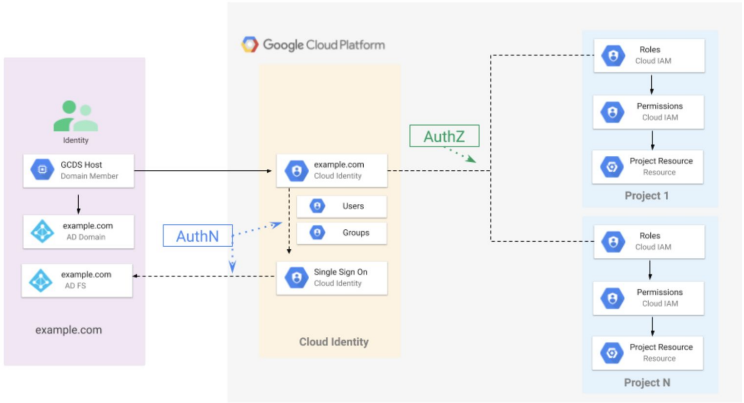


Cloud Directory Sync Implementation

1. Google Cloud Directory Sync (GCDS) is deployed on an on-premises domain joined VM, either Linux or Windows.

2. Leveraging cron, GCDS is triggered automatically at regular intervals to sync identities between Active Directory and Cloud Identity

3. In order to filter which users or groups are synced with Cloud Identity, an attribute is added to the users in AD and Directory Sync filters are implemented to filter based on the provided attribute.



Authorization with IAM

Roles are a collection of **permissions** that may be assigned to **users**, **groups** and **service accounts**.
Permissions grant the ability to execute specific API calls, for example: compute.instances.create

Primitive Roles

Legacy Google Cloud roles that grant broader set of permissions
(Owner, Editor, Viewer).

Predefined Roles

More granular roles than primitive, based on job function.

Custom Roles

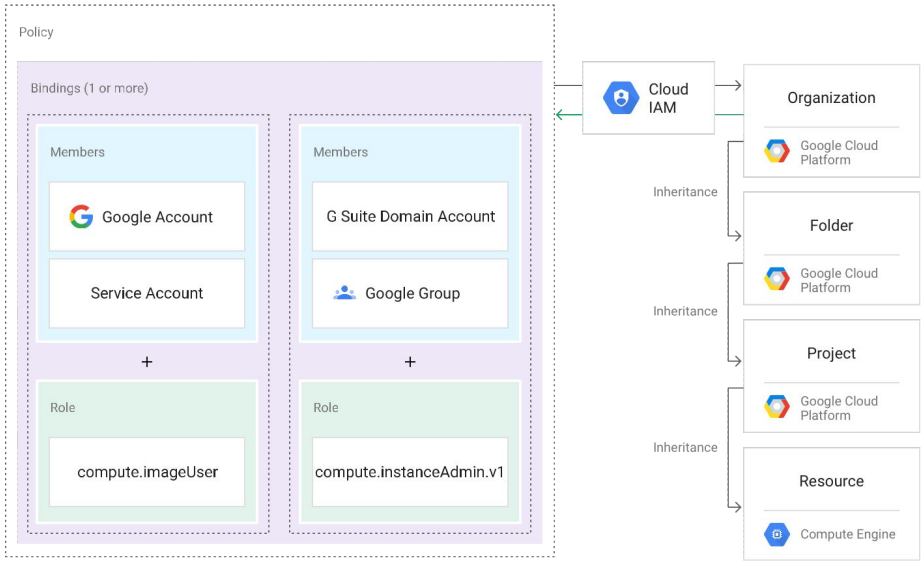
Ability to create roles with a specific permission set.

Authorization with IAM

Give access to a subset of resources within a project

Condition access based on context-aware access levels

Grant time limited IAM policies



Best Practices

Controversial Approaches

- Disabling APIs by default
- Deleting Default Service Accounts
- G-Suite Super Admin Role management
- Controlling Scopes
- Using Service Accounts outside original project

Follow Industry Standards

- CIS Benchmarks
- NIST Cybersecurity Framework

Networking

Networking Considerations

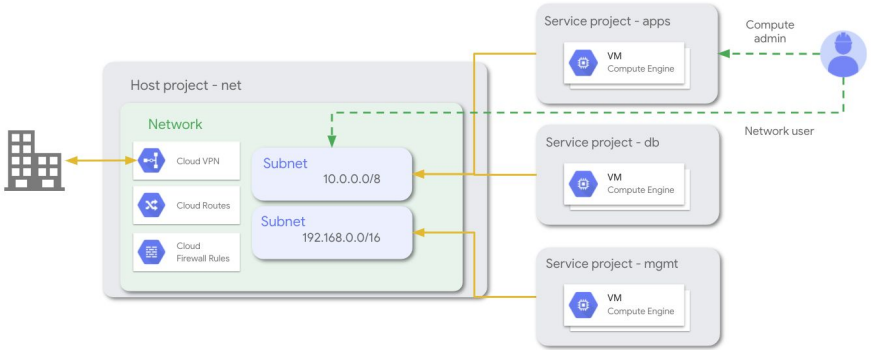
Components

Shared VPC - Introduction

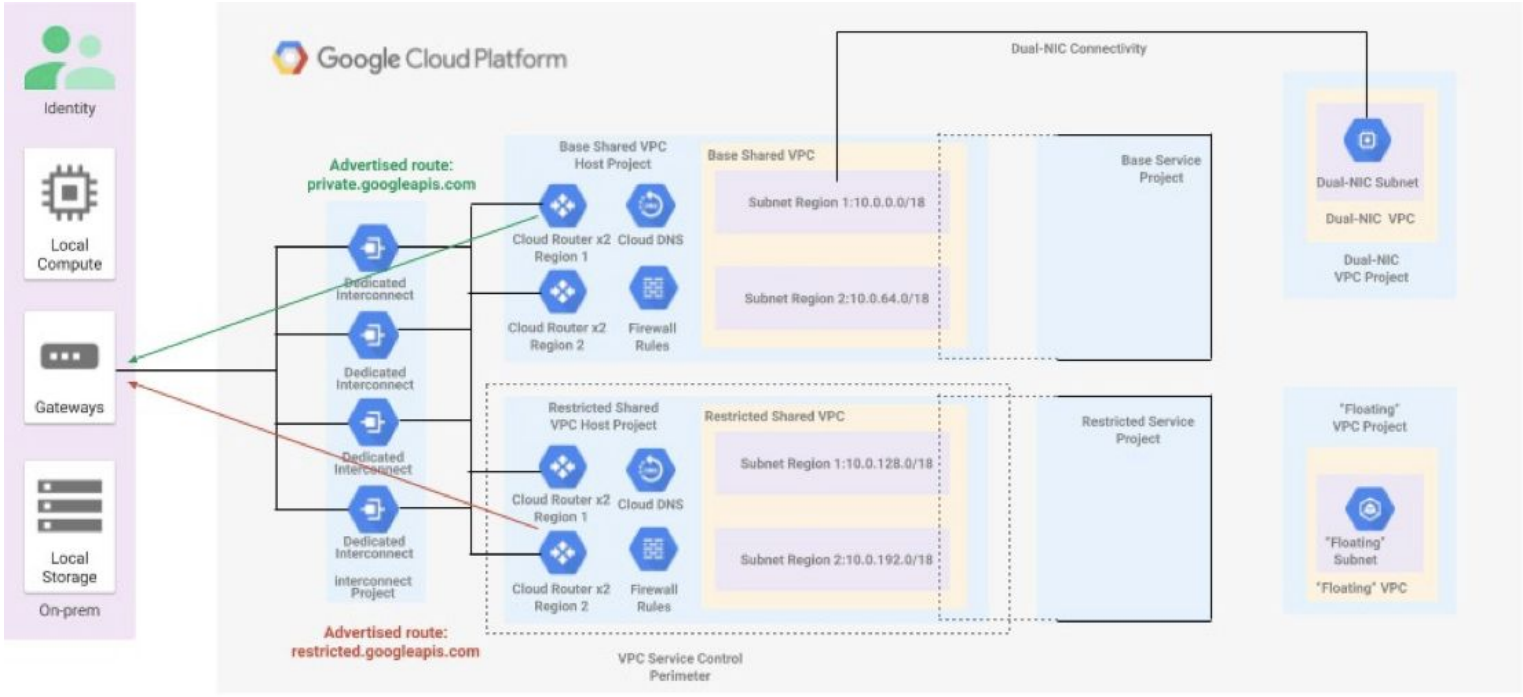
Shared VPC allows an organization to connect resources from multiple projects to a common Virtual Private Cloud (VPC) network, so that they can communicate with each other securely and efficiently using internal IPs from that network.

Definition:

- **Host Project:** contains one or more Shared VPC networks. A Shared VPC Admin must first enable a project as a host project. After that, a Shared VPC Admin can attach one or more service projects to it.
- **Service Project:** A service project is any project that has been attached to a host project by a Shared VPC Admin. This attachment allows it to participate in Shared VPC. It's a common practice to have multiple service projects operated and administered by different departments or teams in your organization.

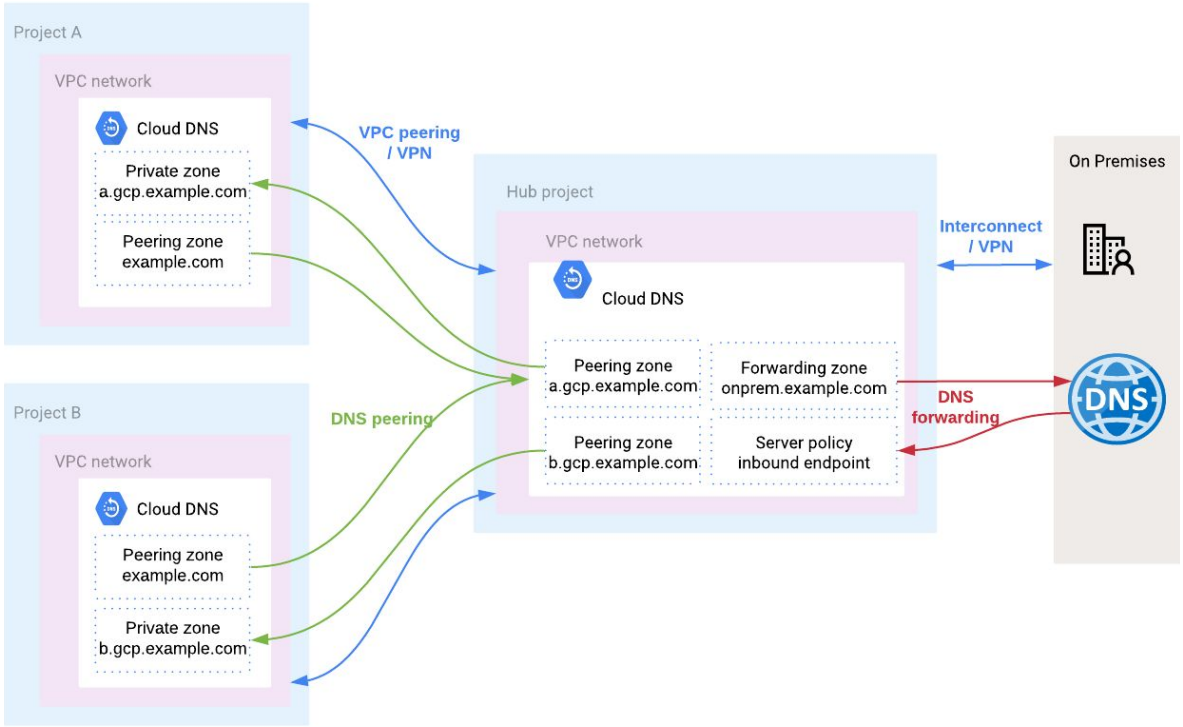


Shared VPC

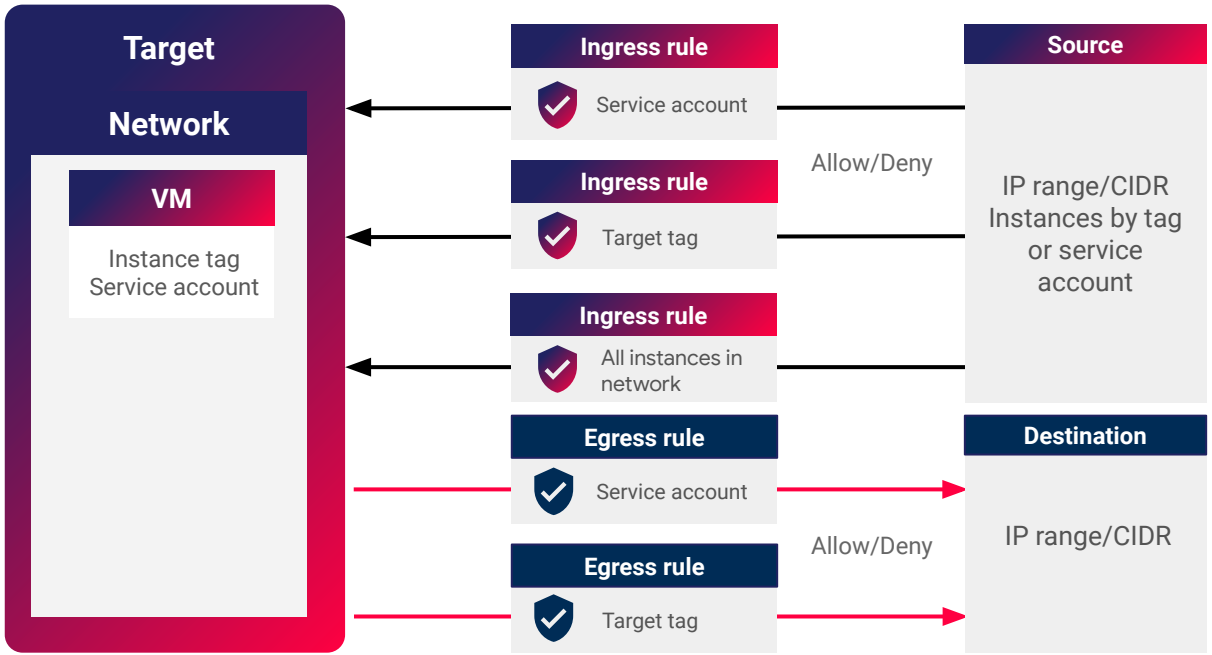


Shared VPC Per Environment:
Prod/Non-prod//Dev

DNS - Hub-and-spoke model



Firewall Rules



VPC Firewall

- **Stateful** with connection tracking
- **Distributed**: enforced on underlying host

Implied Rules

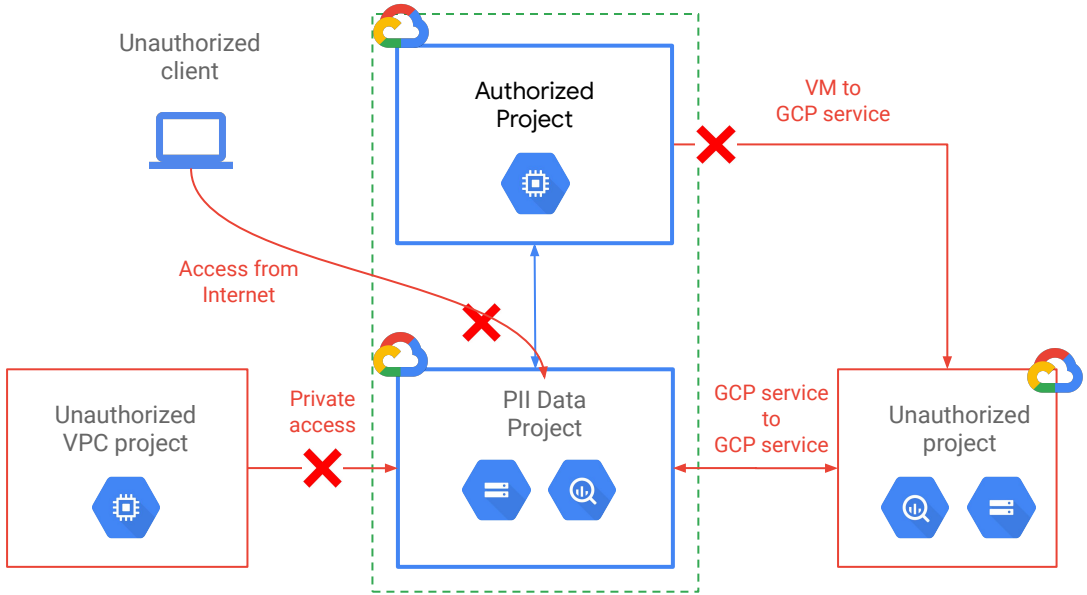
- Ingress deny
- Egress allow

VPC Service Controls

Service Perimeter

Extend perimeter security to managed GCP services

- Control VM-to-service and service-to-service paths.
- Ingress: prevent access from the unauthorized networks.
- Egress: prevent copying of data to unauthorized GCP Projects.
- Project level granularity.



Connectivity Options

Public Internet (IPSEC VPN)

- Fastest way to connect to the cloud or between clouds
- Leverages existing internet network connectivity
- Supports high availability and aggregated bandwidth with **1.5 to 3 Gbps per tunnel**
- Static/dynamic (BGP) based VPC
- Easy HA setup: **99.99% SLA**

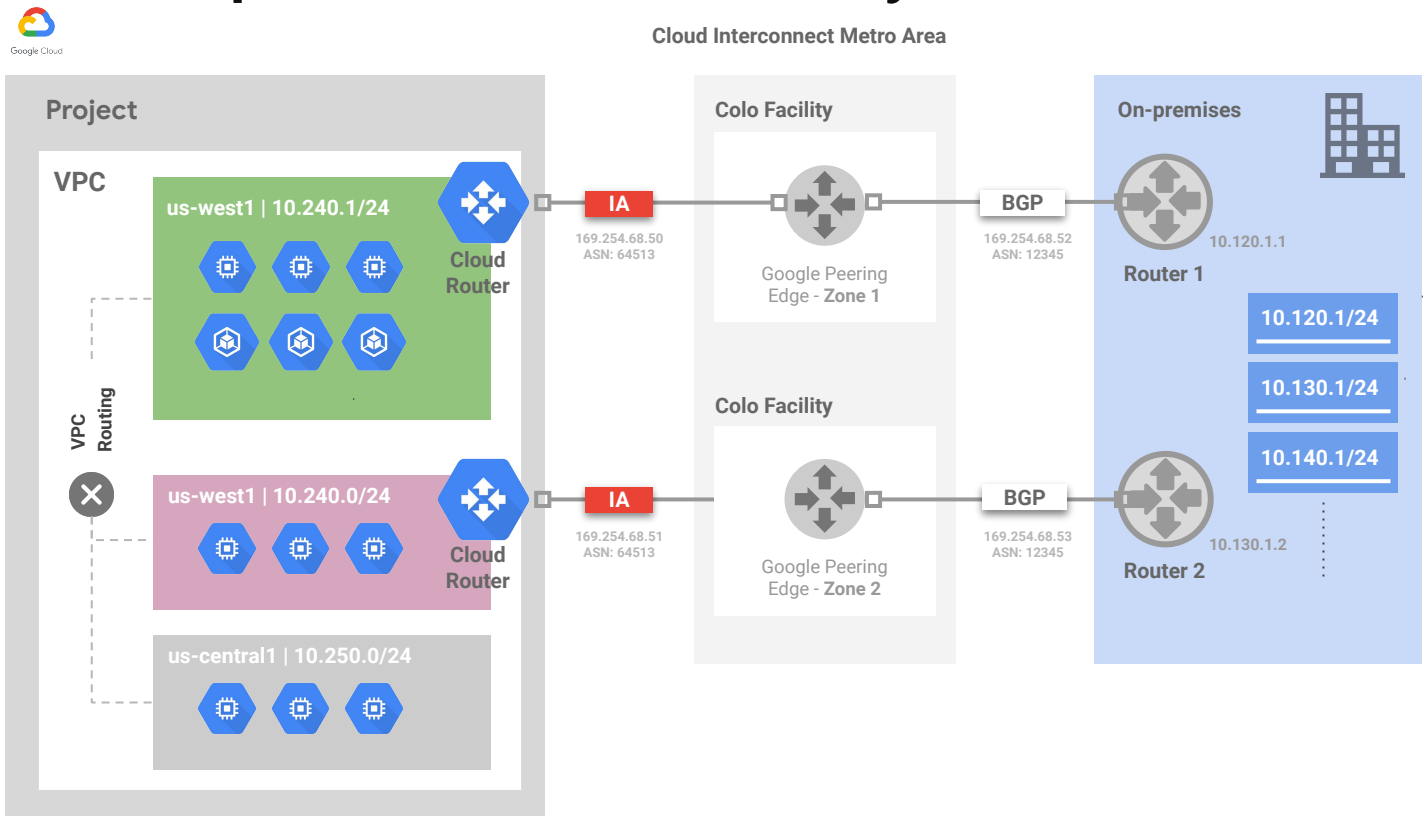
Cloud Interconnect

- Enterprise-grade, private connectivity to GCP
- Provisioned as a dedicated link to a Google PoP or via a partner
- Dedicated Interconnect: Highest bandwidth with **10 Gbps and 100 Gbps links**
- Partner Interconnect offers more flexible subscriptions (**50 Mbps to 10 Gbps**)

Peering

- Access G Suite and Google services, as well as GCP with reduced egress rates
- Utilizes existing BGP route selection and internet routing
- Greater control of peering facilities
- Direct or carrier

On-premises Connectivity



- **Layer 2** connectivity
- Up to **eight 10 Gbps** links, or **two 100 Gbps** links
- Same Interconnect can link to **multiple VPCs** within the same project
- 99.9% or 99.99% SLAs depending on the architecture chosen

Zero Trust Networking

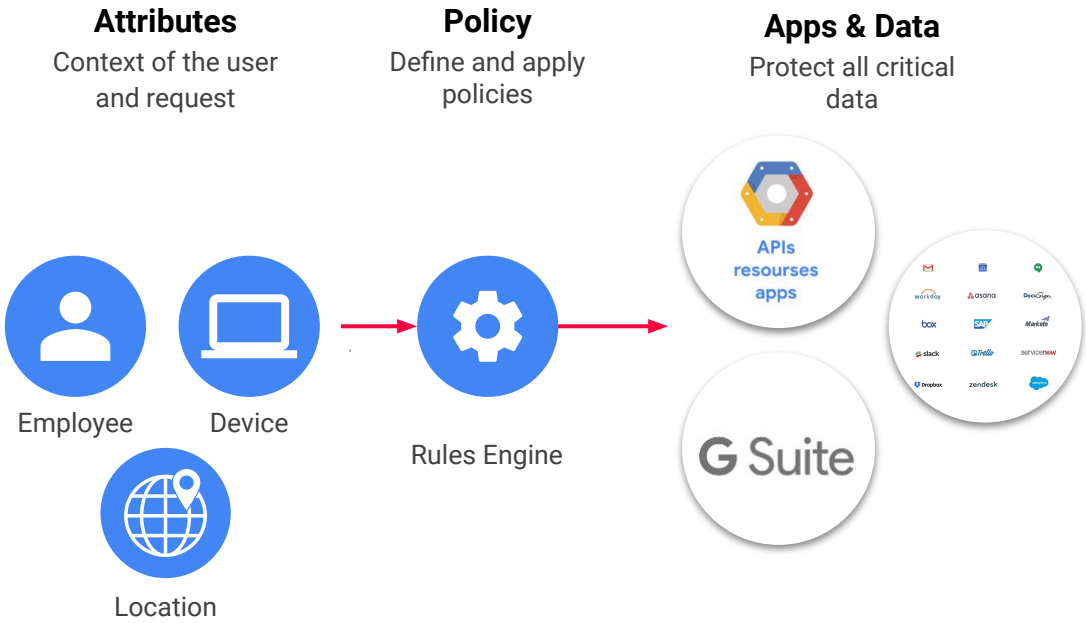
Access Context Manager - Access Levels

Context-Aware Access Suite of Products collects attributes and data

- Endpoint verification collects device identity and security posture
- Cloud Identity provides user information

Access Context Manager Defines Authorization Rules

- Define rules around geography, device status, time of day, etc for granting access



User + Device + Context is the new security perimeter

Identity-aware Proxy

Central enforcement

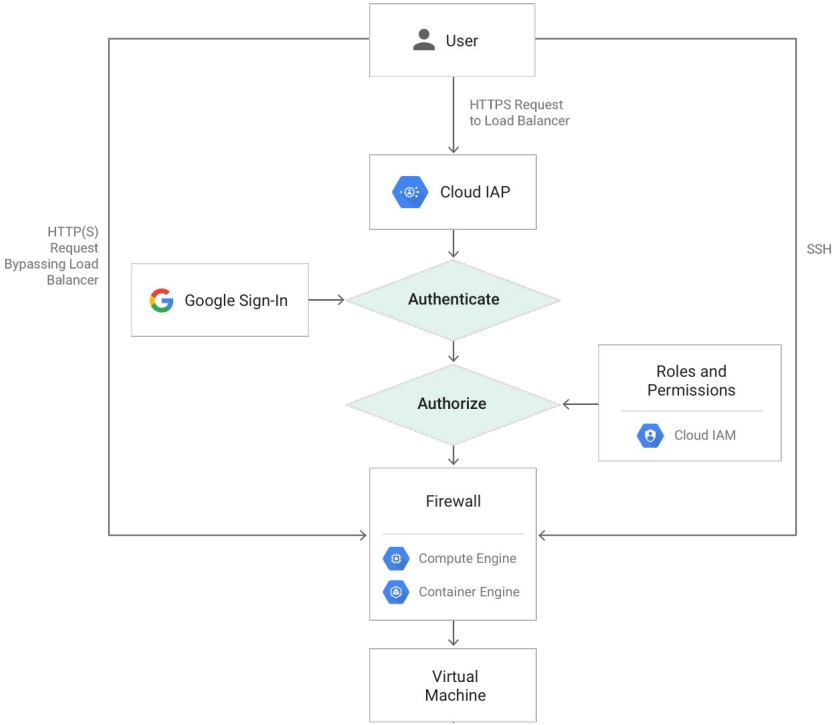
- Single point of control for managing user access
- Security team can define and enforce policy

Access control

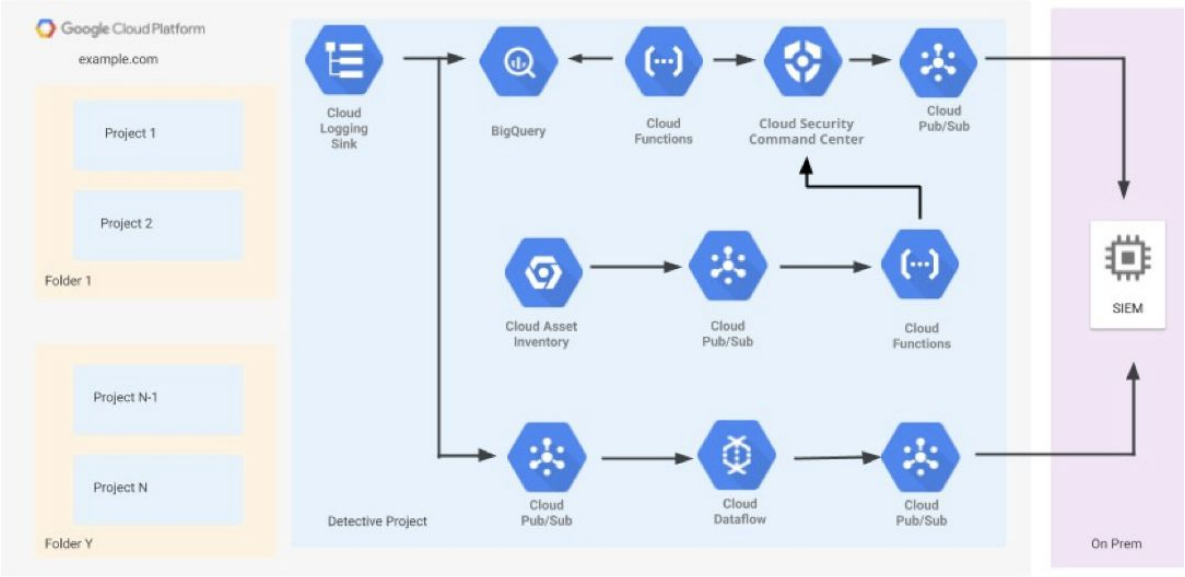
- Control access by user identity
- Apply policy by group membership
- Supports 2FA Security Keys

Deployment

- Little to no change to applications
- No need to implement own authentication for each application
- Integrated with HTTP(s) Load Balancer

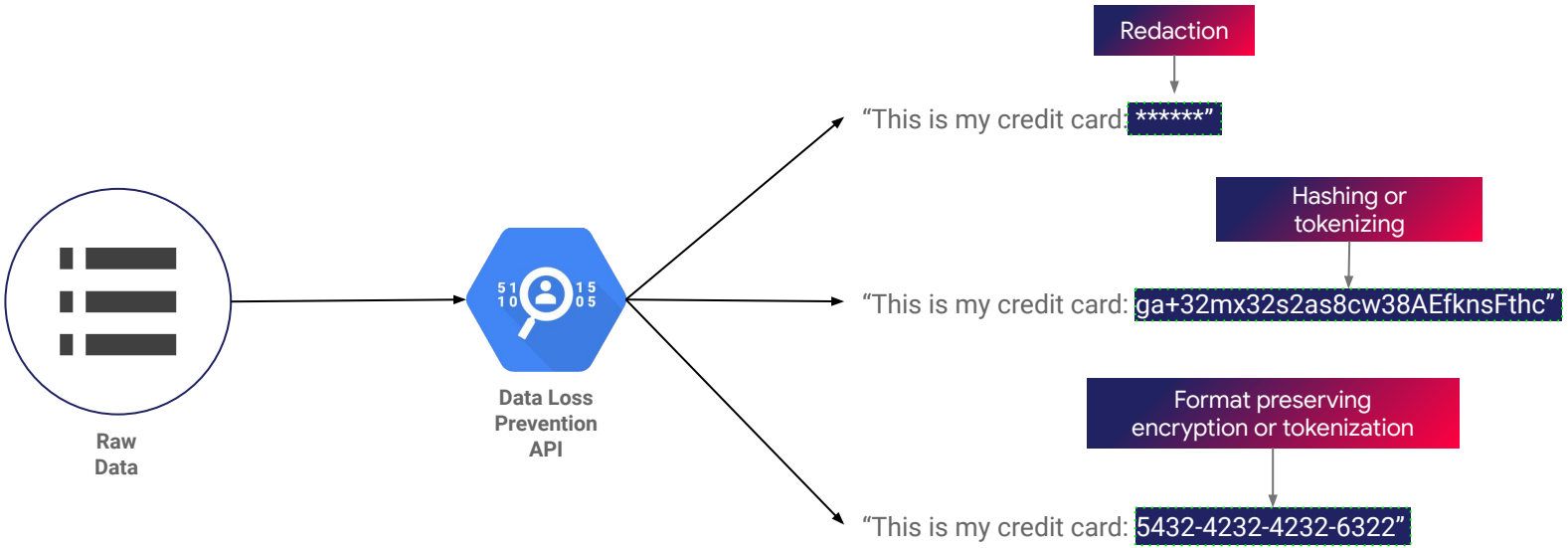


Detective Controls

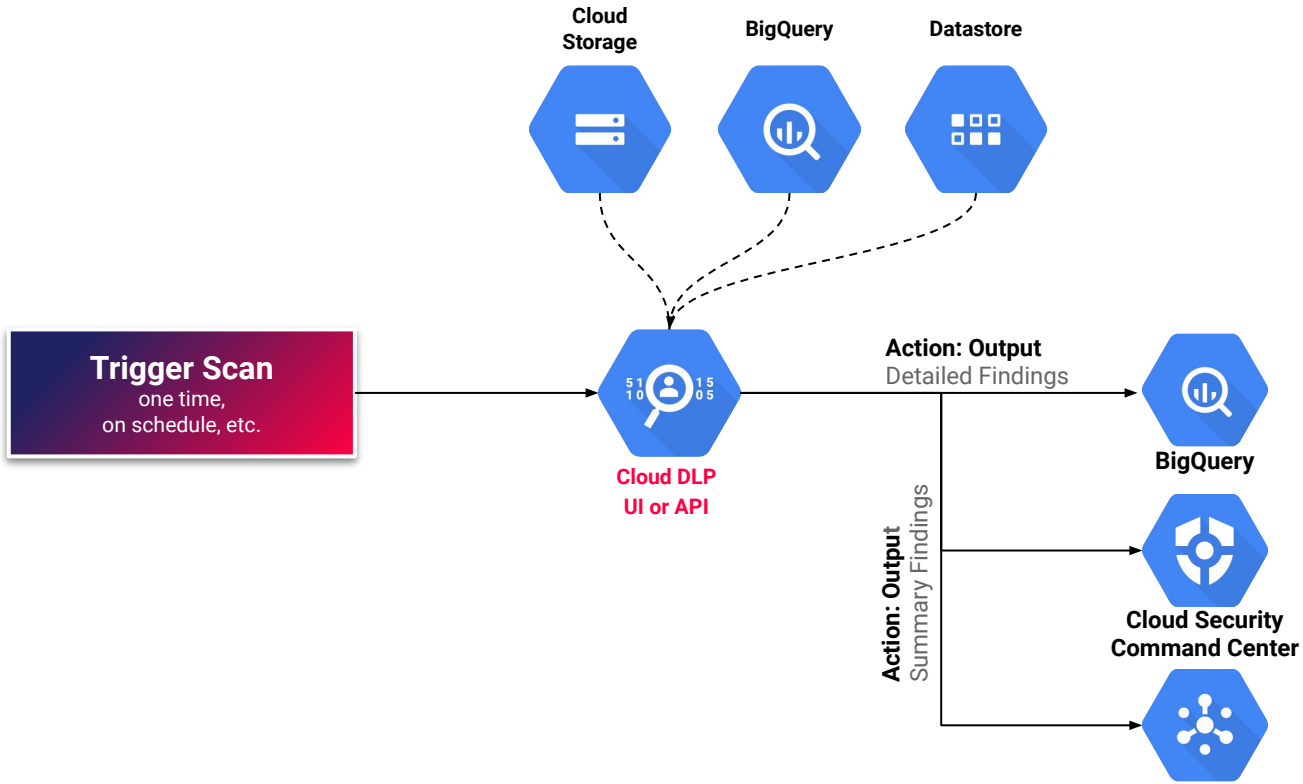


Cloud DLP (Data Loss Prevention)

Cloud Data Loss Prevention provides programmatic access to a powerful detection engine for PII Data

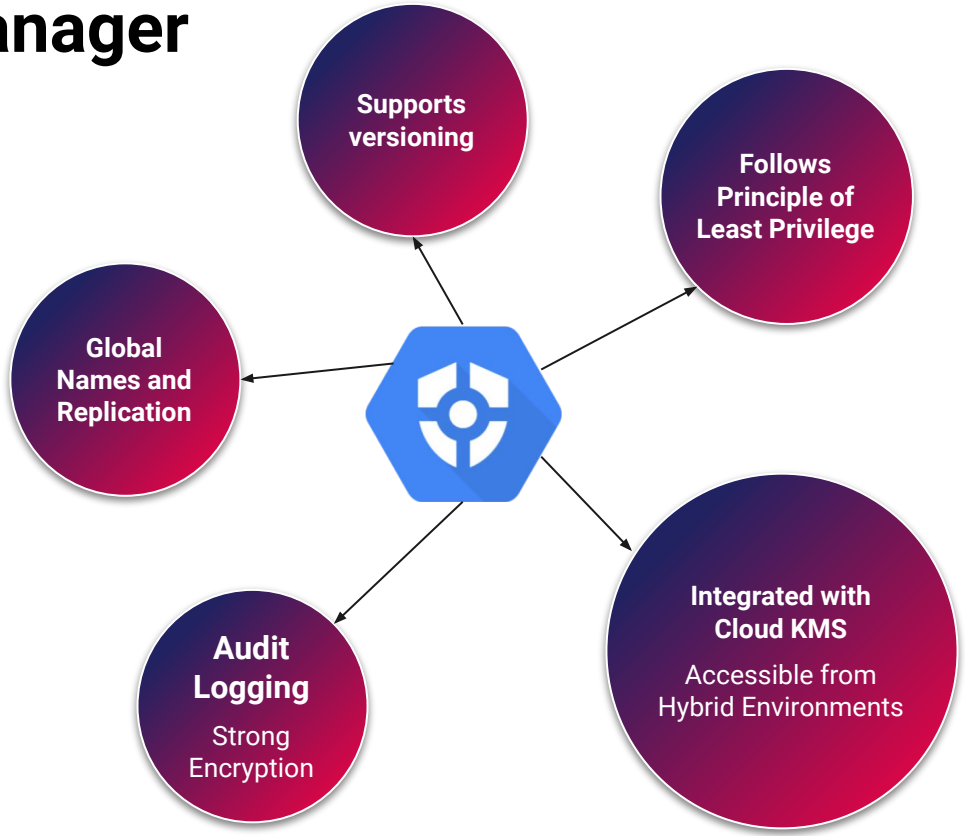


Implementation

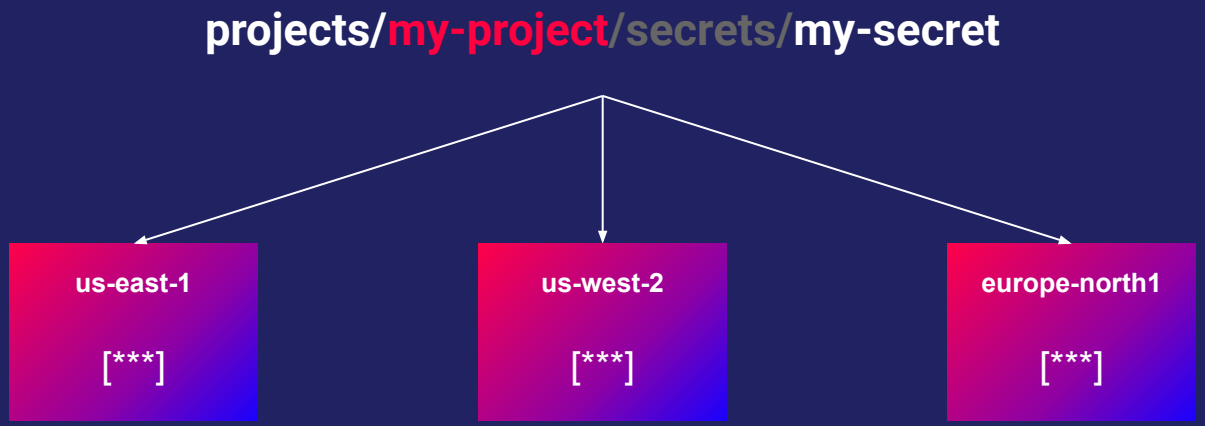


Secrets Management

Secret Manager



Global Names and Regional Data



Key Management Comparison

Role	Default Encryption	CMEK via Cloud KMS	CSEK
Supported Products	All	BigQuery, Compute Engine, Cloud Storage, Dataproc, Dataflow, Kubernetes Engine, Cloud SQL	Compute Engine, Cloud Storage
Key Management Effort	None	Medium	High
Data Encryption Effort	None	Low	Medium (GCE,GCS)
Key rotation effect on encrypted data	Automatic	Re-Encrypt All data	Re-Encrypt All data

Logging

Stackdriver

Monitoring

- Endpoint checks to internet-facing services
- Uptime checks for URLs, groups, or resources
- Plugins for many major stacks (Apache, MySQL, CouchDB etc.)

Logging

- Filter, search, and view
- Define metrics, dashboards, and alerts
- Export to BigQuery, Google Cloud Storage, and Pub/Sub

Performance

- Built on the same systems that power Google's global infrastructure
- Unprecedented scale, performance, and resiliency

Multi-cloud

- Google Cloud Platform, Amazon Web Services, Hybrid configuration
- Combines metrics, logs, and metadata

Log Compliance

Separation of Duties (SoD)

- Use Aggregated Exports to centralise all logs from all projects into a single separate project, with different ownership than the source
- Choose Cloud Storage as the destination

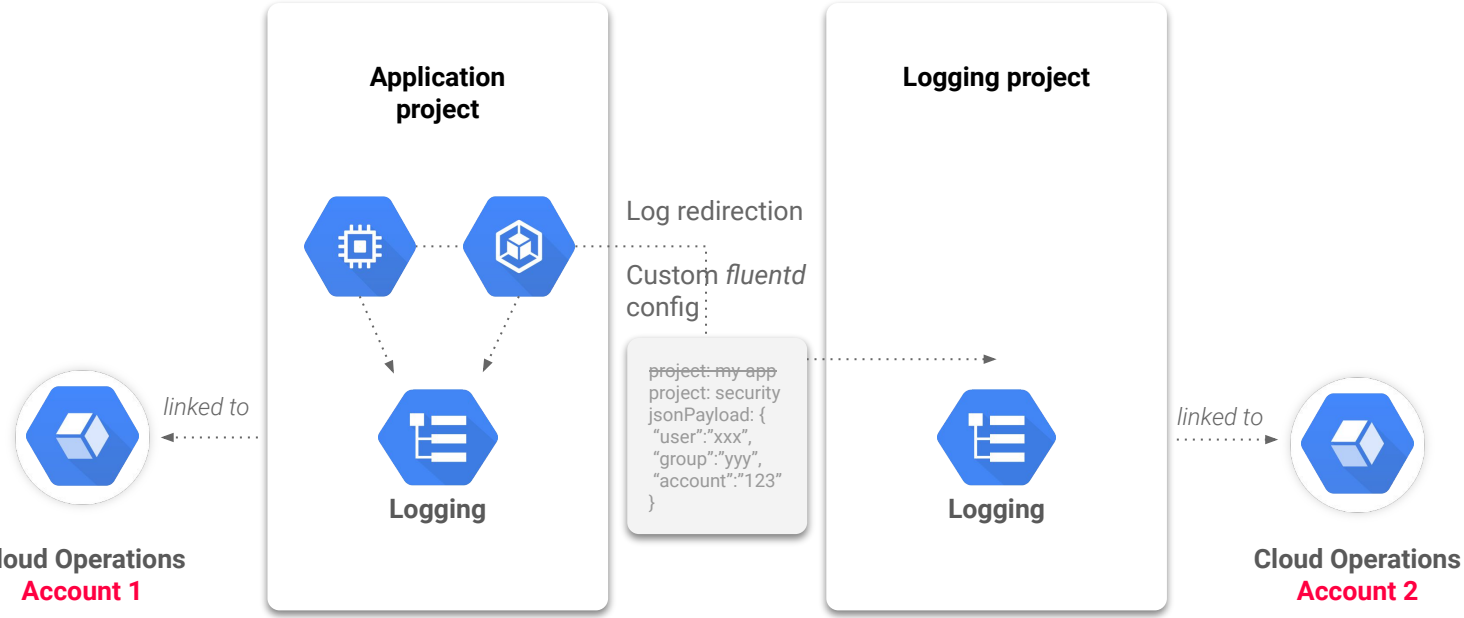
Least privilege

- Only grant the right level of permissions required on the project / bucket containing the logs
- Avoid granting permissions to delete buckets / objects

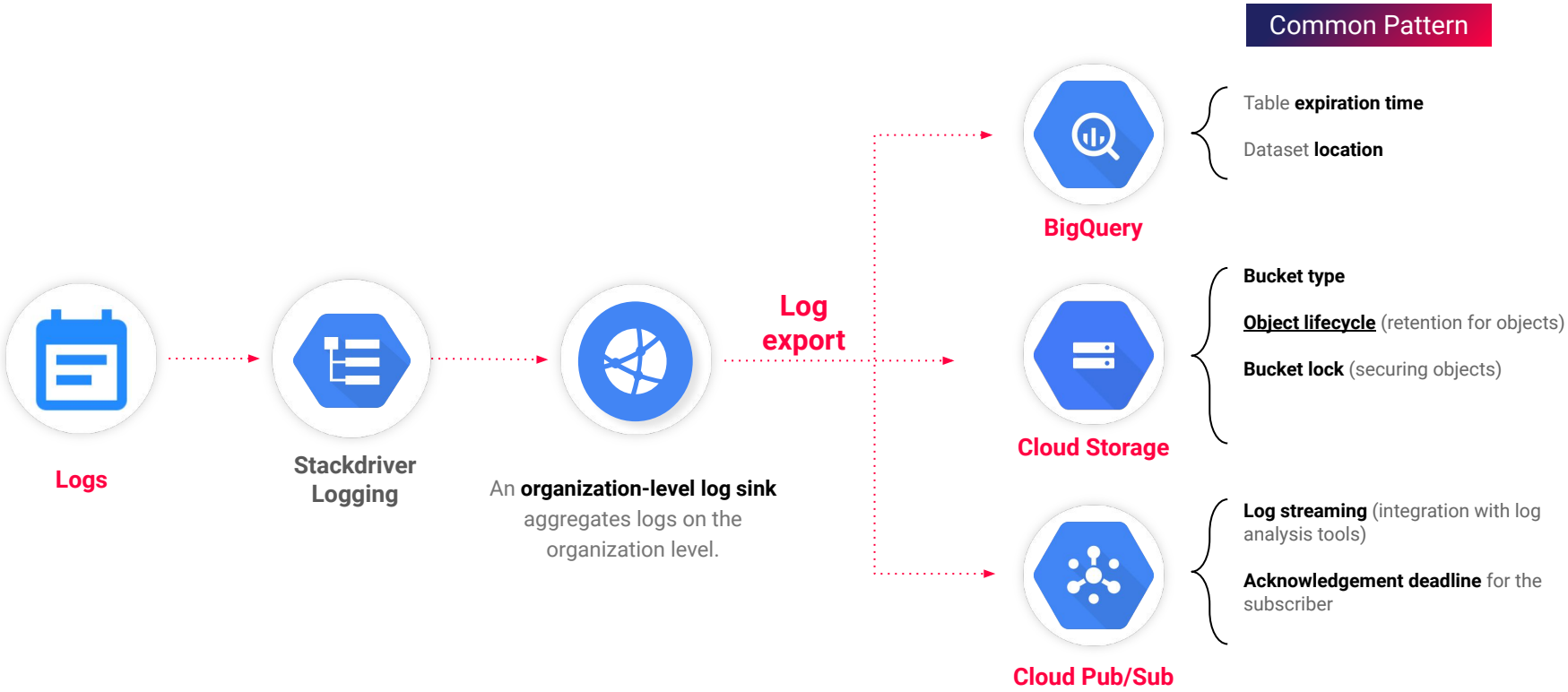
Non-repudiation

- Cloud Storage automatically encrypts all data before it is written to disk
- Additional fortification can be implemented by **object-versioning** log buckets in conjunction with a **Bucket Lock**

Security Logging



Log Exports


Common Pattern
Logs
Stackdriver Logging
An **organization-level log sink** aggregates logs on the organization level.
Log export
BigQuery
Table **expiration time**
Dataset **location**
Cloud Storage
Bucket type
Object lifecycle (retention for objects)
Bucket lock (securing objects)
Cloud Pub/Sub
Log streaming (integration with log analysis tools)
Acknowledgement deadline for the subscriber

Security Information and Event Management

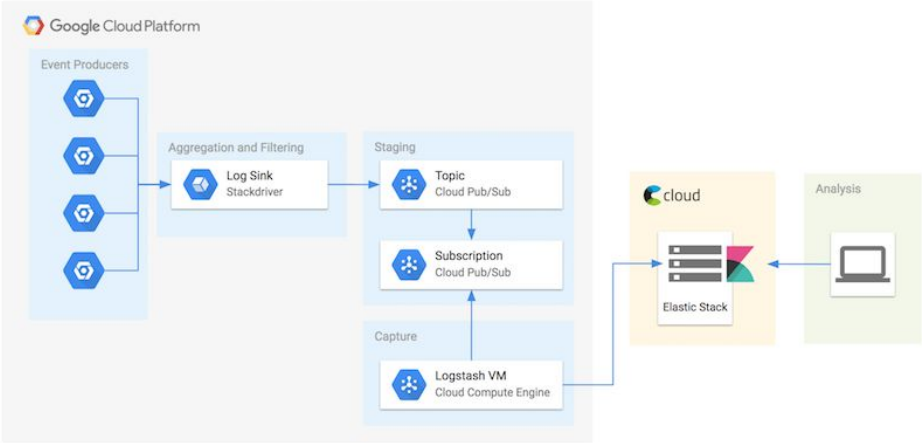
Organization can export their logs to a third party SIEM solution

Integration through

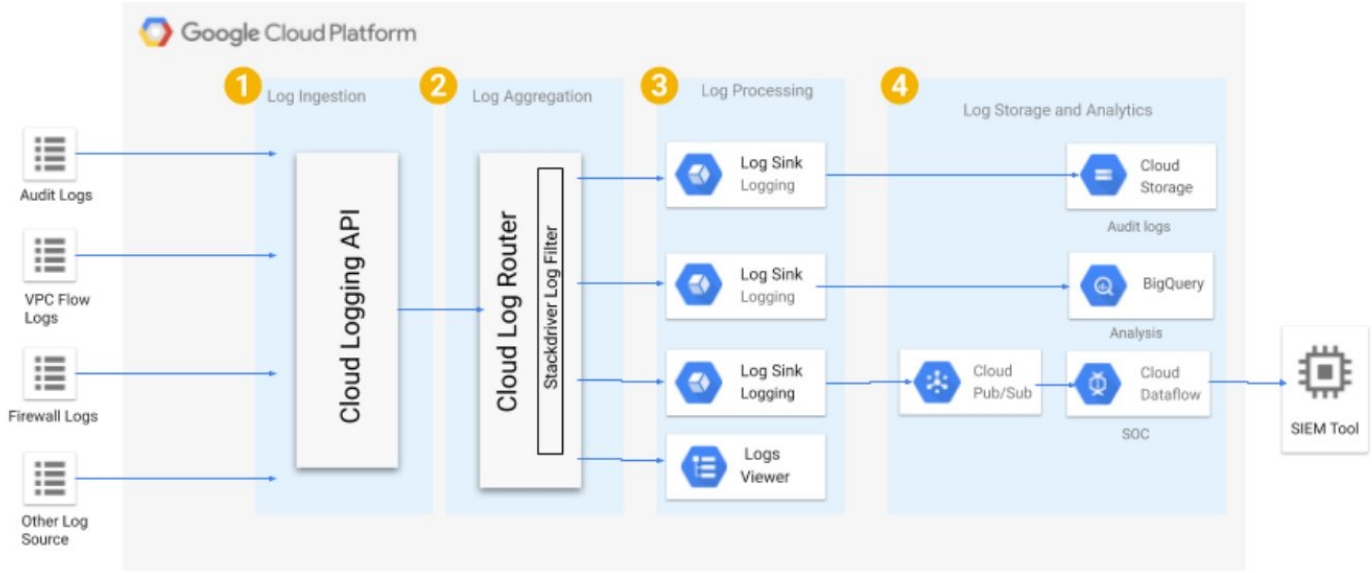
- Agents @ SIEM side
- Add-on or connector

Example integrations

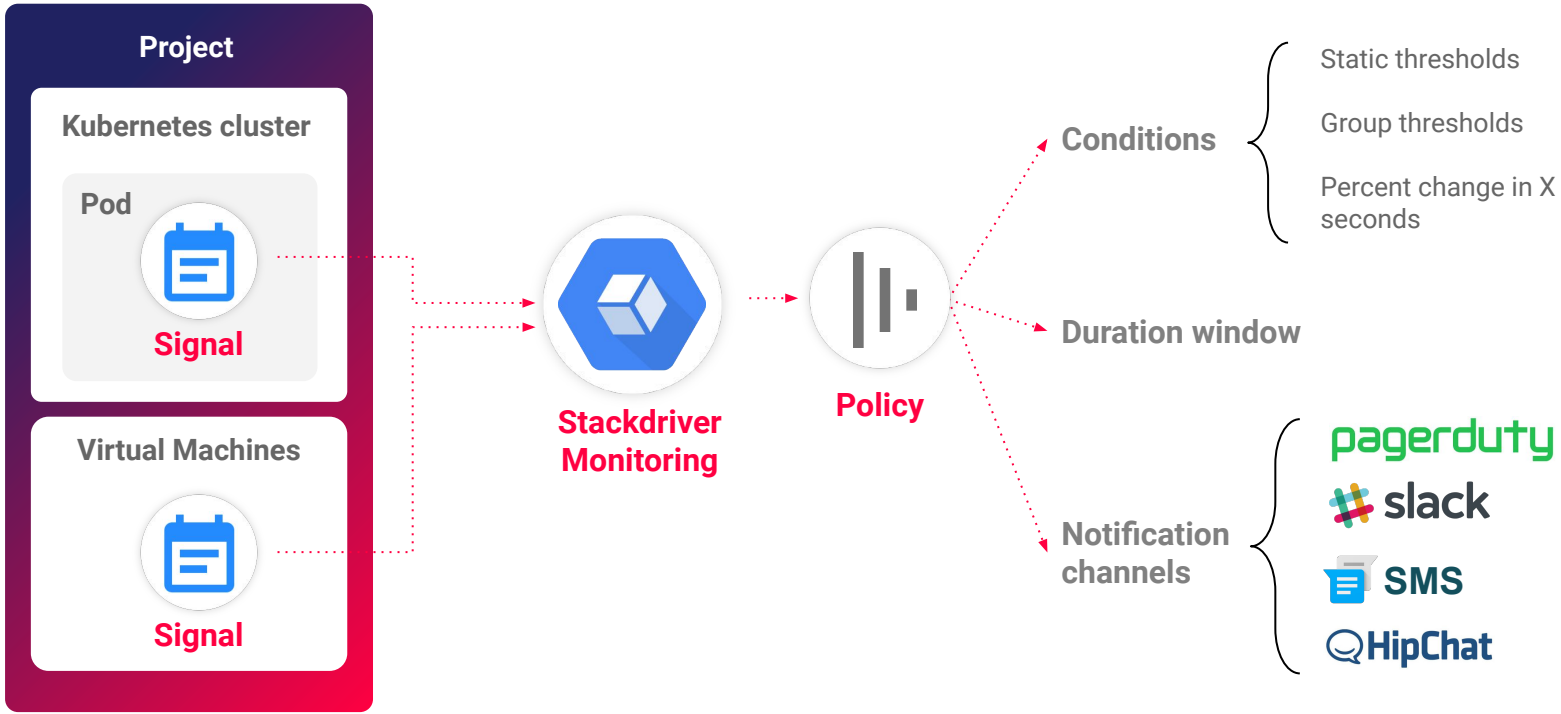
- **Splunk**
  Add-on for Google Cloud
- **Elasticsearch**
  Cloud Pub/Sub -> Logstash|Beats -> ES -> Kibana
- **Sumo Logic**
  Cloud Pub/Sub -> API webhook -> Sumo
- **ArcSight**
  FlexConnector for REST



Cloud Logging



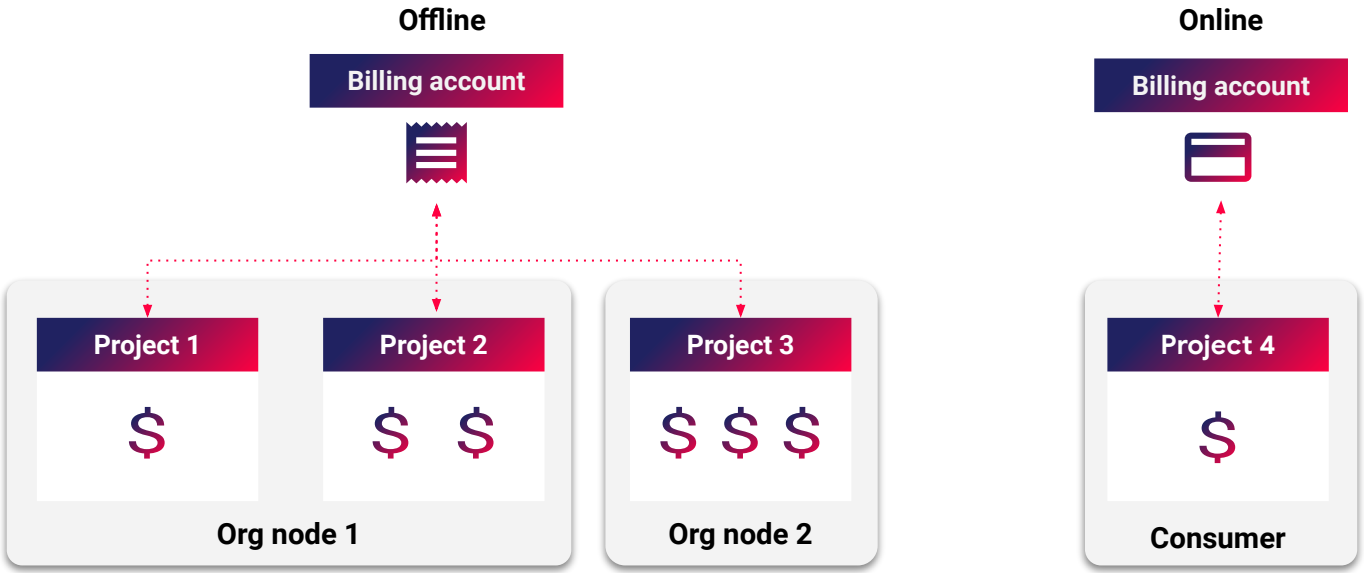
Alerting


Project
Kubernetes cluster
Pod
Signal
Virtual Machines
Signal
Stackdriver Monitoring
Policy
Conditions
Static thresholds
Group thresholds
Percent change in X seconds
Duration window
Notification channels
pagerduty
slack
SMS
HipChat

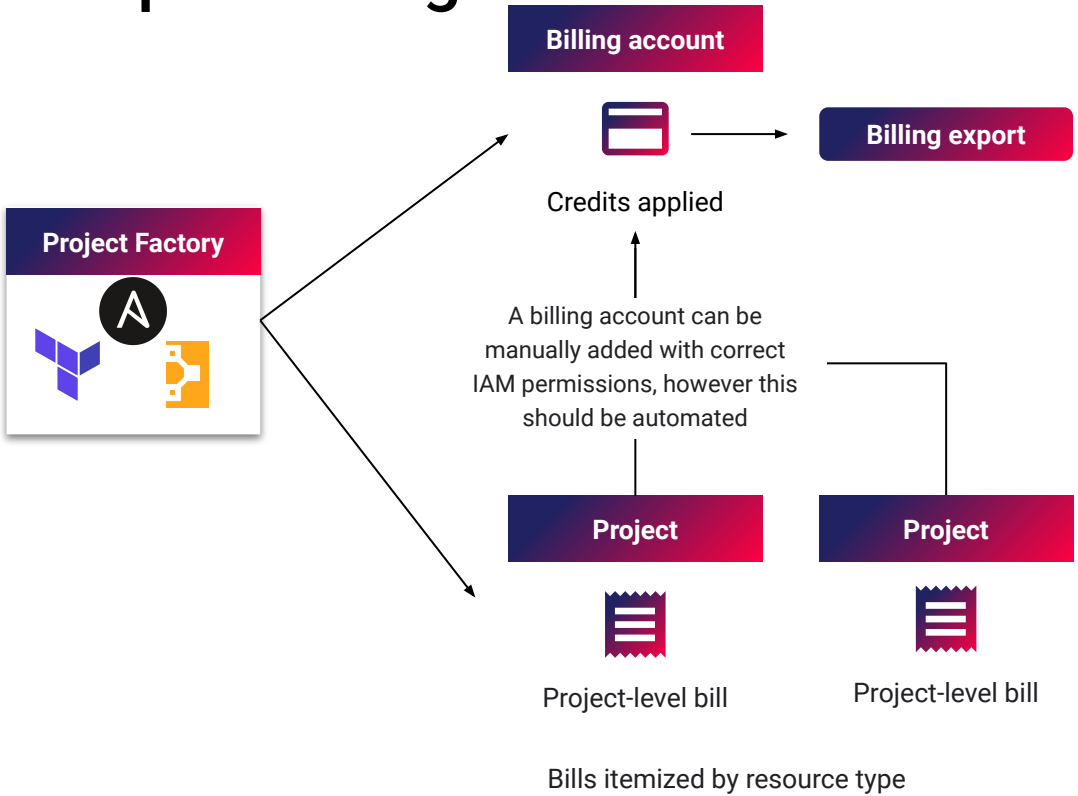
FinOps - Billing

FinOps - Billing

Billing accounts are payment vehicles for your Google Cloud spend.
They come in two types:



FinOps - Billing



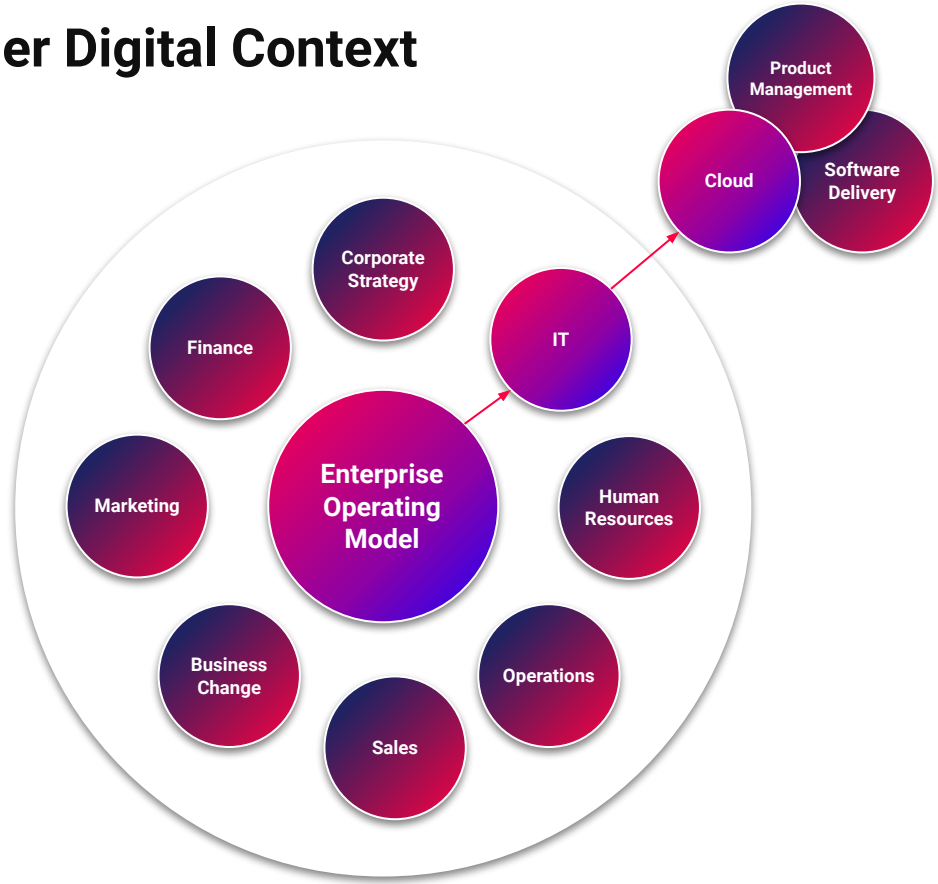
- Use Project Factory to (IaC) provision projects and set billing accounts
- Hierarchical
- Resources have consistent naming and labelling standards to allow for cost attribution
- Report on costs
- Ensure budgets and spend alerts are in place to control spend
- Forecast usage costs

Operating Model

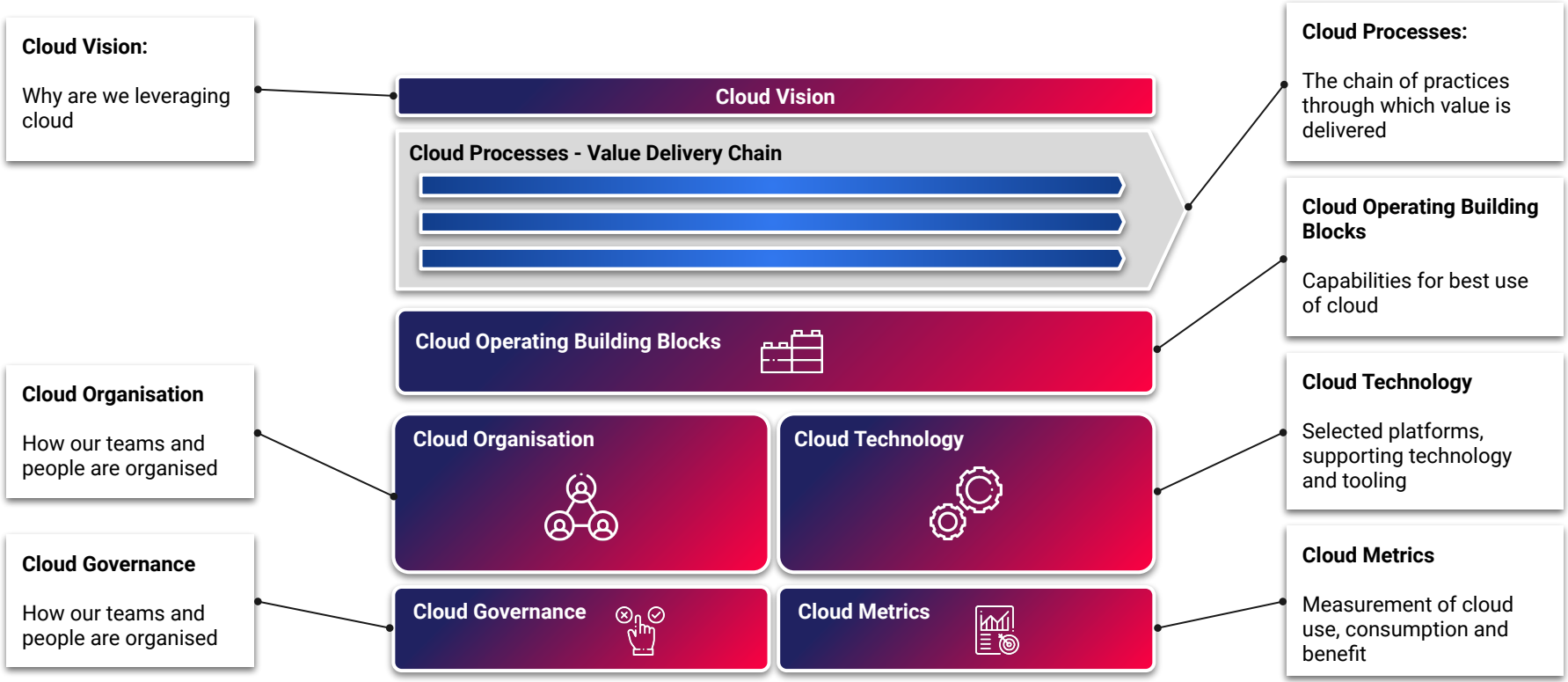
The Model Needs to Fit in the Wider Digital Context

Key Points:

- Cloud op model is only a part of the overall IT op model
- The IT op model is only a part of the broader enterprise op model
- There are a number of dependencies, intersects and dependencies across the enterprise wide op model



Elements of Cloud Operating Model



There is a Need to Transition to a New Shared Responsibility Model

Key Points:

- Customer is a supplier of requirements with shared responsibility for build within your company.
- Customer teams consume reusable assets from central repository.
- Run responsibilities owned by your company and partners

Operating Model

Decentralized

Access to and control of Google Cloud is shared among developers and engineers across the company. Corporate IT has little to no involvement with running the platform.

- **Corporate IT**: Creation of folders, shared services, and common configuration
- **Developers and engineers**: Creation of projects and, optionally, additional folders under the relevant folder

Centralized

Access and control of Google Cloud is centrally controlled by **Corporate IT** or **Operations**.

- Administering the platform
- Granting access to engineers and developers as required

CONTINO

Questions ?

federico.fregosi@contino.io

https://www.linkedin.com/in/federico-fregosi/