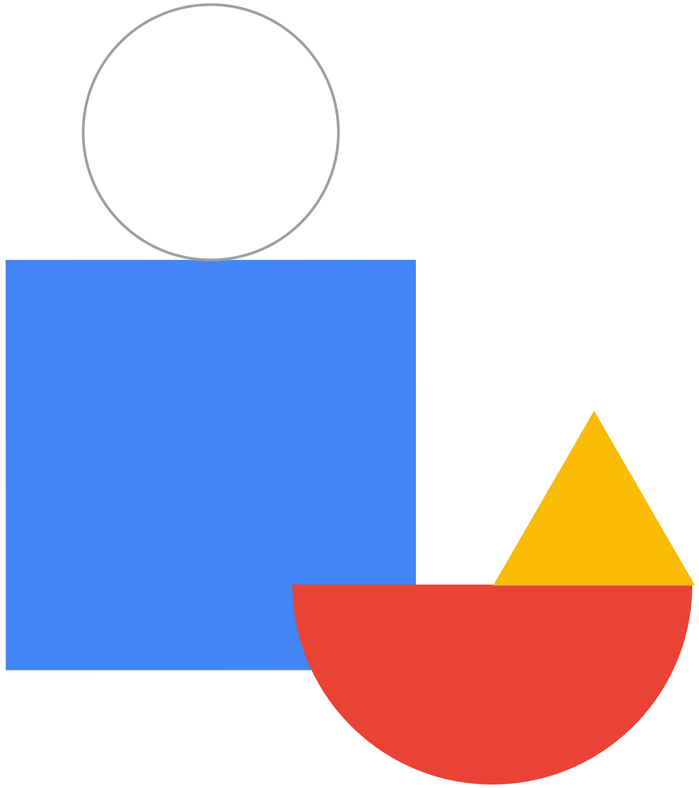
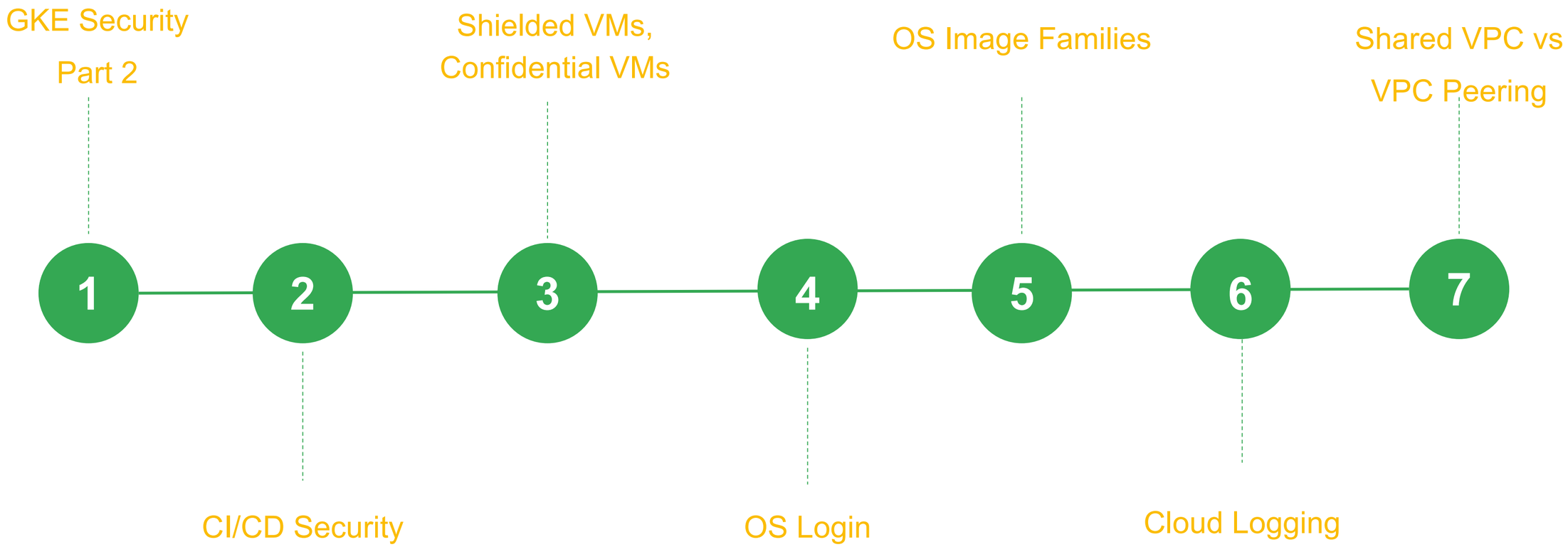
Google Cloud



Preparing for Your Professional Cloud Security Engineer Journey

Module 4: Managing Operations in a Cloud Environment

Week 4 topics



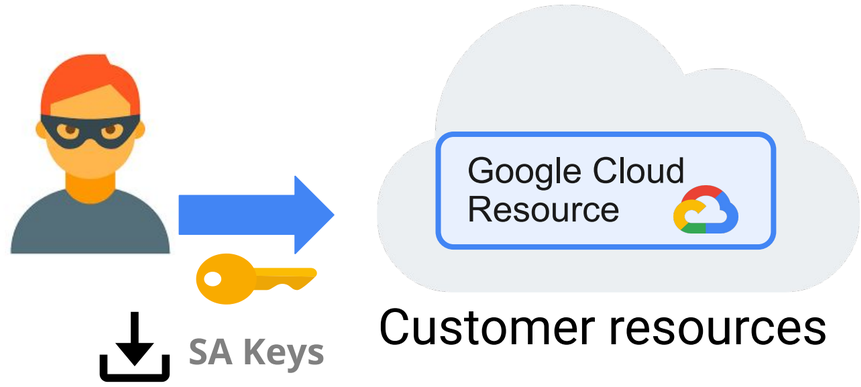
Kubernetes Engine Security Best Practices - Part 2

GKE service accounts

- When compute API is enabled, there is a default Compute Engine service account gets created automatically
- Used across compute services (GCE, GKE, Cloud Run)
- It has Project Editor role by default
- **Recommendation**: create a service account for specific clusters with minimal roles:
  - **monitoring.viewer**
  - **monitoring.metricWriter**
  - **logging.logWriter**
  - **stackdriver.resourceMetadata.writer**
  - **artifactregistry.reader**

Service account (SA) keys pose a security risk to your cloud resources

- SA keys are similar to a **password without an expiration date**.
- SA Keys can be leaked accidently and attackers can use it to access your (GCP project or org admin) sensitive GCP resources.
- Usage cannot be audited → compounding the risk



Customers have downloaded > 48 Million Service Account Keys!!

So what's the solution? Ditch the keys and use Workload Identity & Workload Identity Federation!

GCP API access from k8s *without* Workload Identity

[Authenticate to Google Cloud using a service account | Kubernetes Engine]

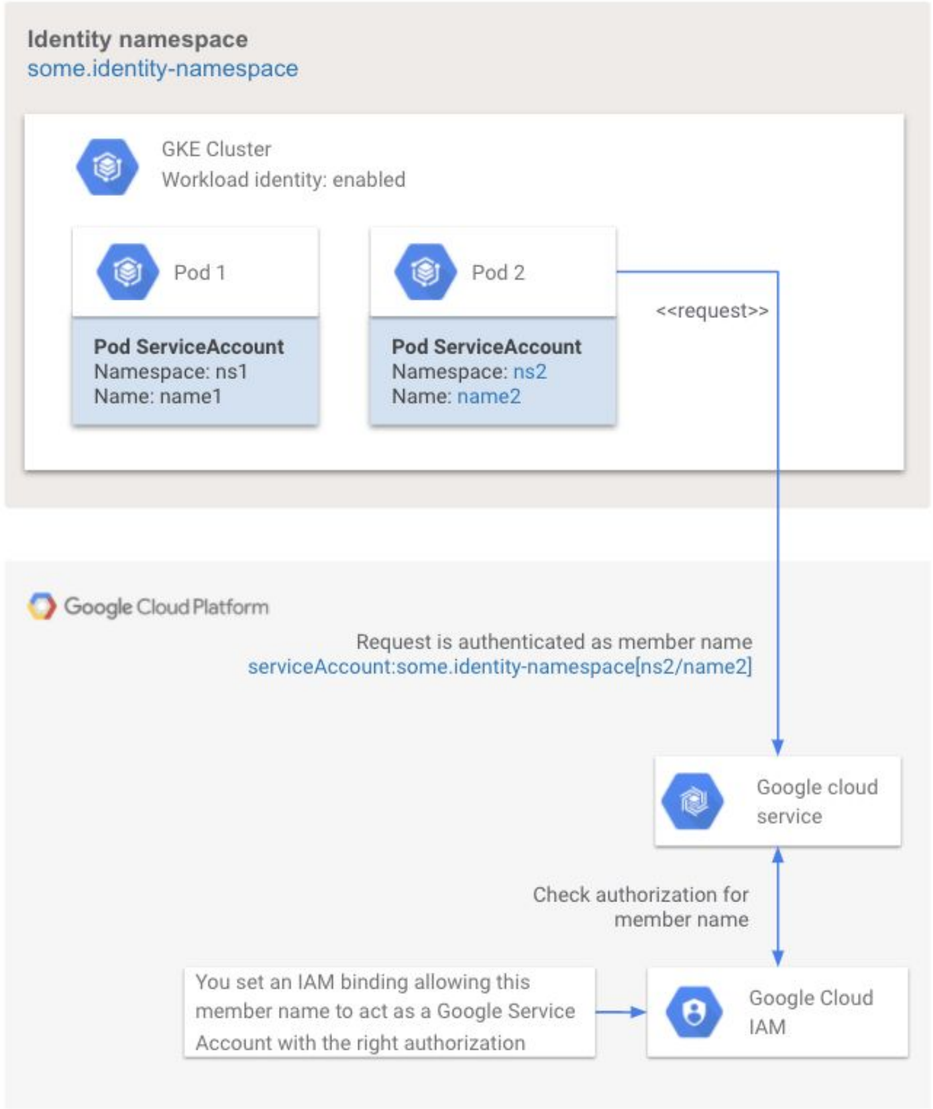
- Create a GCP Service Account (GSA)
- Create Keys for GSA
- Import GSA Keys as a k8s Secret
- For the k8s Workload:
  - Define a Volume with the Secret
  - Mount the Volume inside the container
  - Point $GOOGLE_APPLICATION_CREDENTIALS at the key file
- Workload can now authenticate to GCP APIs as the GSA

=> toilsome to setup & hard to secure

API access *with* Workload Identity

- Enable Workload Identity for the GKE cluster
- Run workload using a dedicated k8s service account (KSA)
- Grant KSA access to desired GCP resources using IAM roles
- Workload can now access GCP APIs by presenting (short-lived, auto-rotated) KSA tokens

It just works!



Workload Identity configuration 101

1. kubectl create namespace **K8S_NAMESPACE**

2. kubectl create serviceaccount --namespace **K8S_NAMESPACE KSA_NAME**

3. gcloud iam service-accounts create **GSA_NAME**

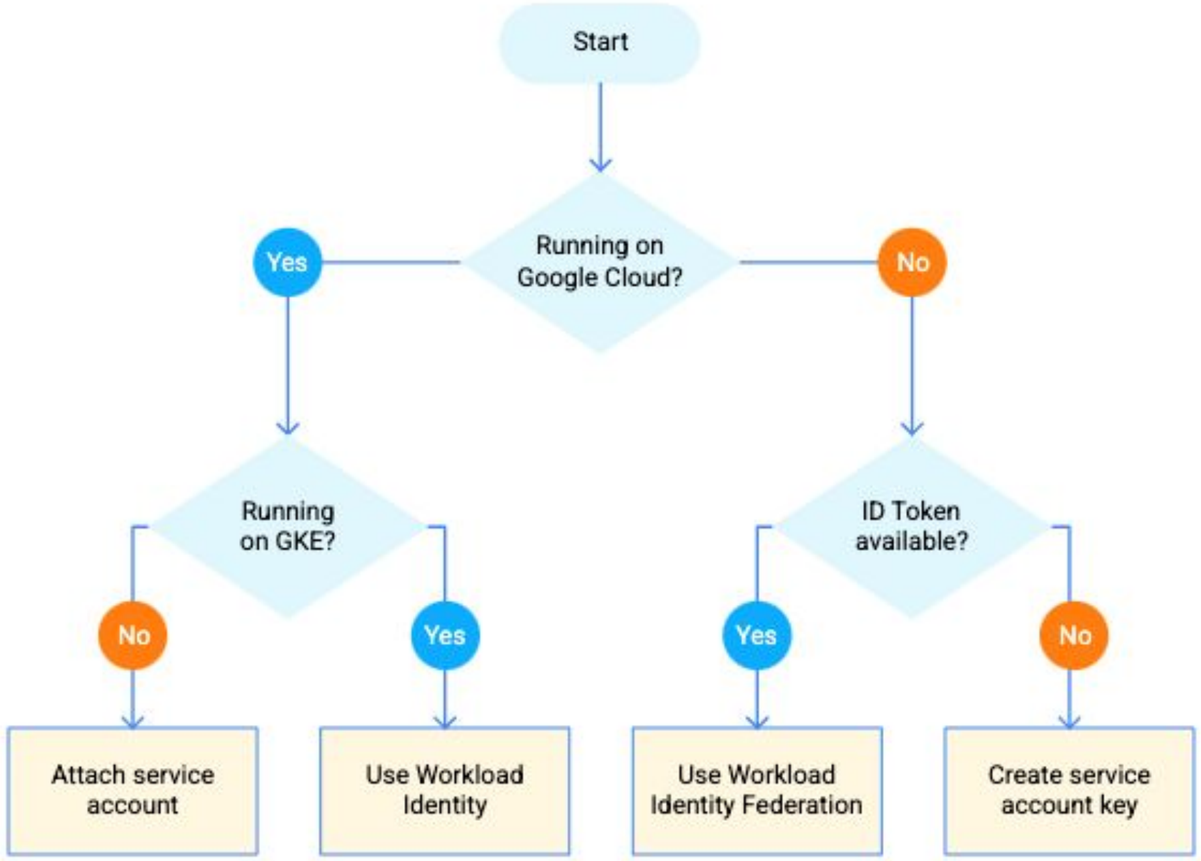
   //When you enable Workload Identity on your GKE cluster, the cluster's
   //workload identity pool will be set to PROJECT_ID.svc.id.goog

4. gcloud iam service-accounts add-iam-policy-binding \
   --role roles/iam.workloadIdentityUser \
   --member "serviceAccount:**PROJECT_ID**.svc.id.goog[**K8S_NAMESPACE/KSA_NAME**]" \
   GSA_NAME@PROJECT_ID.iam.gserviceaccount.com

5. kubectl annotate serviceaccount \
   --namespace **K8S_NAMESPACE KSA_NAME** \
   iam.gke.io/gcp-service-account=**GSA_NAME@PROJECT_ID**.iam.gserviceaccount.com

Workload Identity vs Workload Identity Federation

- Those are two different things! Both aim at limiting usage of Service Account keys, but:
  - Workload Identity = used when microservices deployed to your GKE cluster need to access other GCP resources / APIs.
  - Workload Identity Federation = when some services of yours deployed outside of GCP (in on-premises or other hyperscalers) need to access GCP resources / APIs.



Workload Identity Federation: Keyless Access

NON-GKE

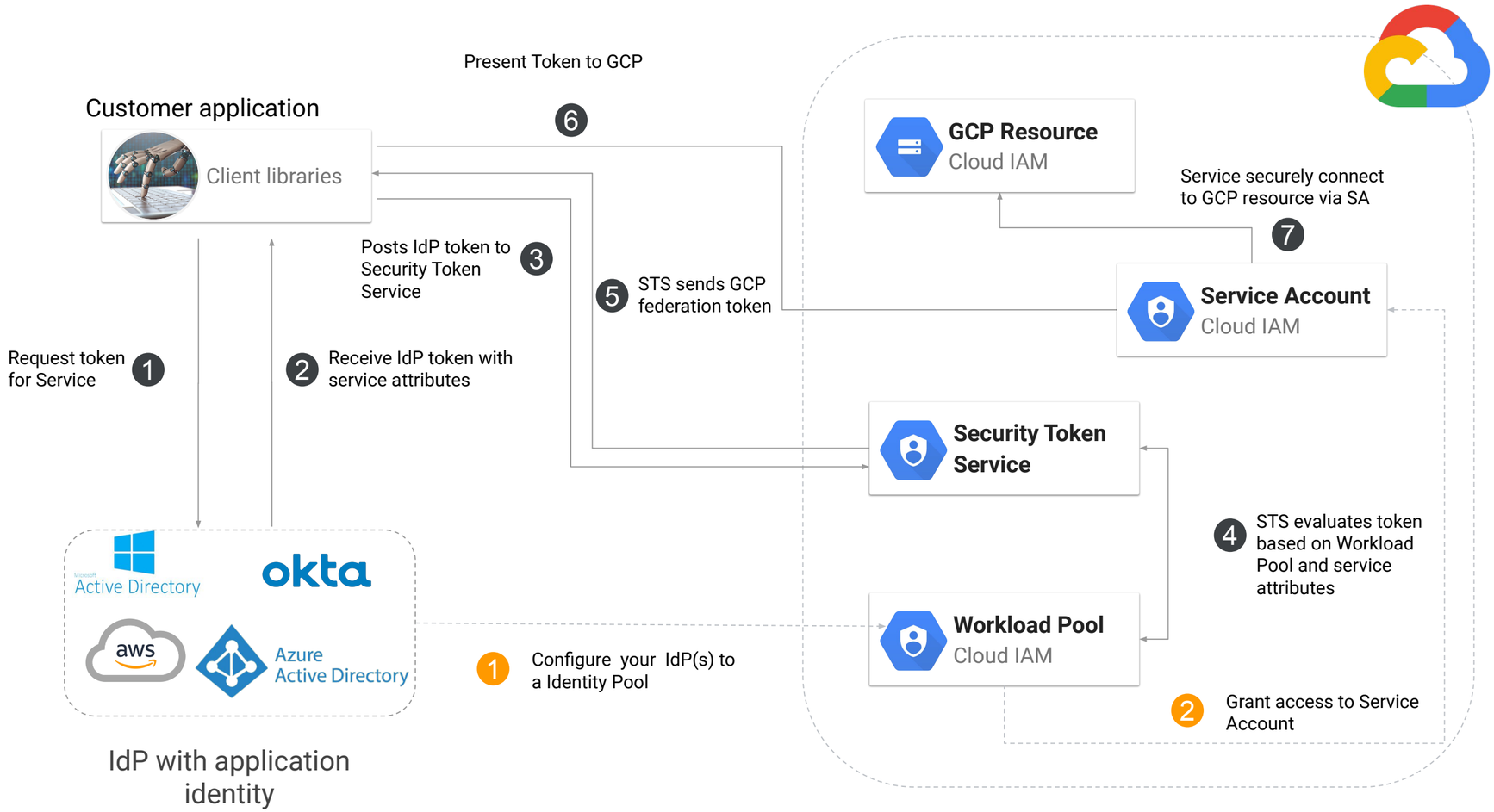
User Story: As an App Developer, I want to **securely connect my service** to GCP resources without downloading access keys.

Benefits

Keyless access to GCP APIs

Auditability through Cloud logs

Attribute-based access control

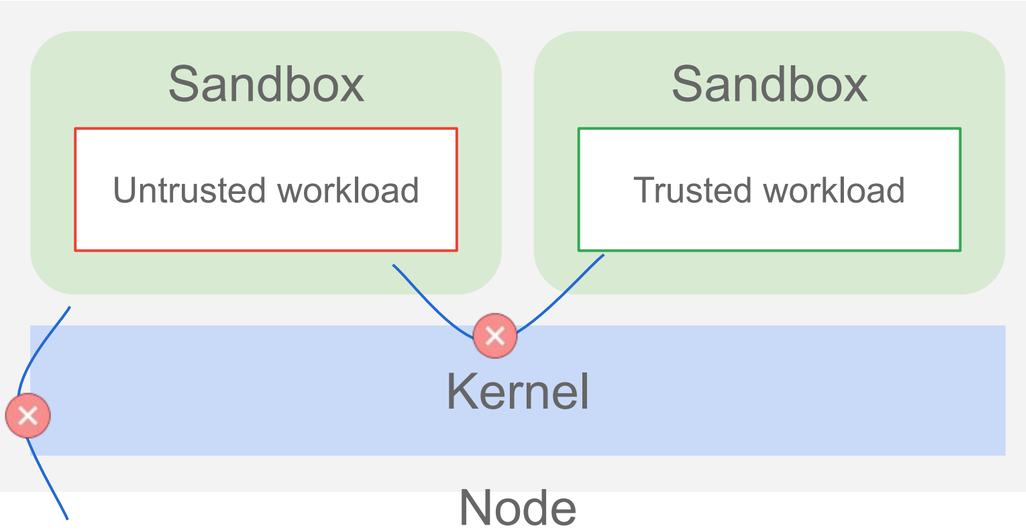


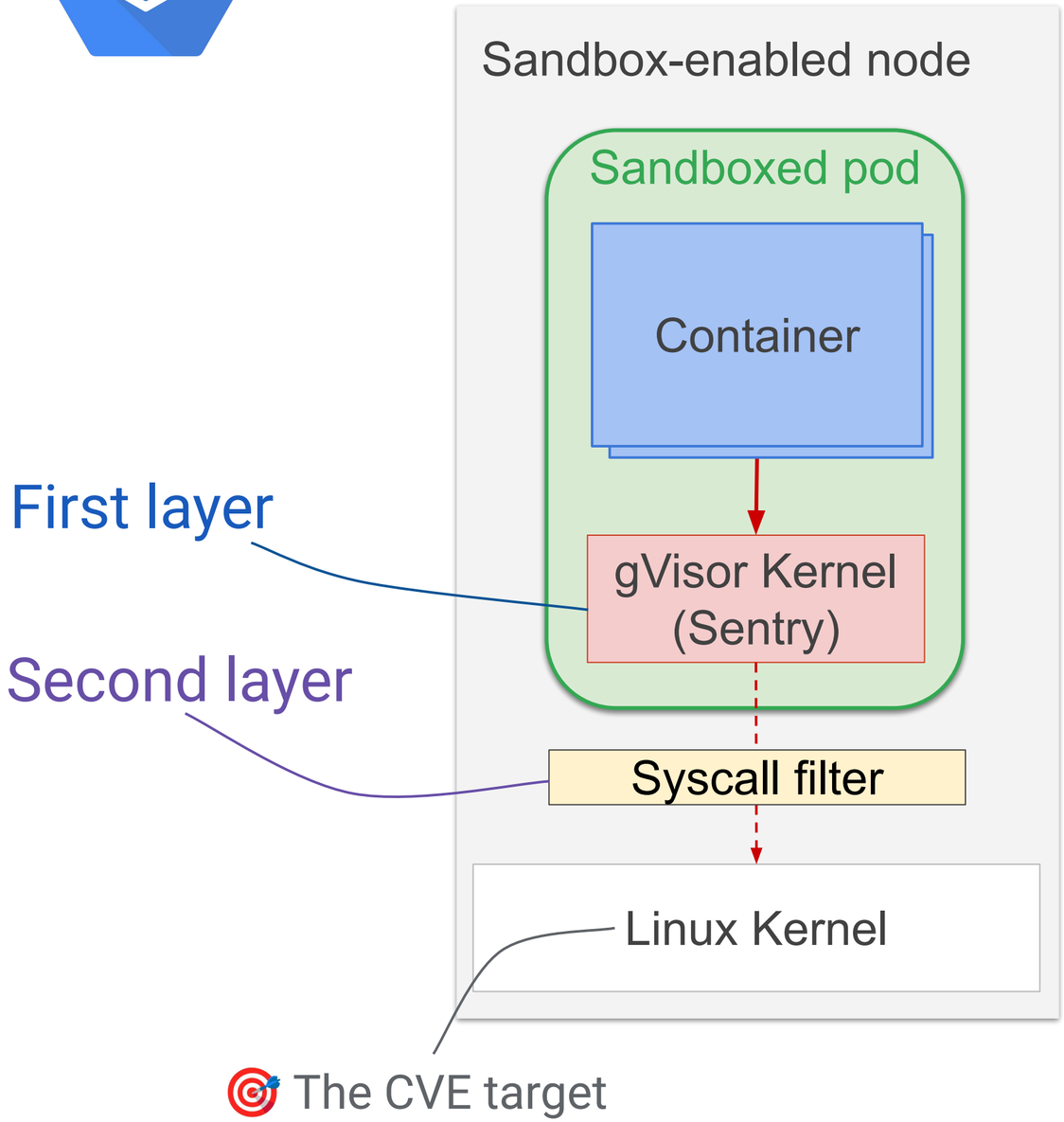
GKE Sandbox

Run **trusted and untrusted** workloads on the same node

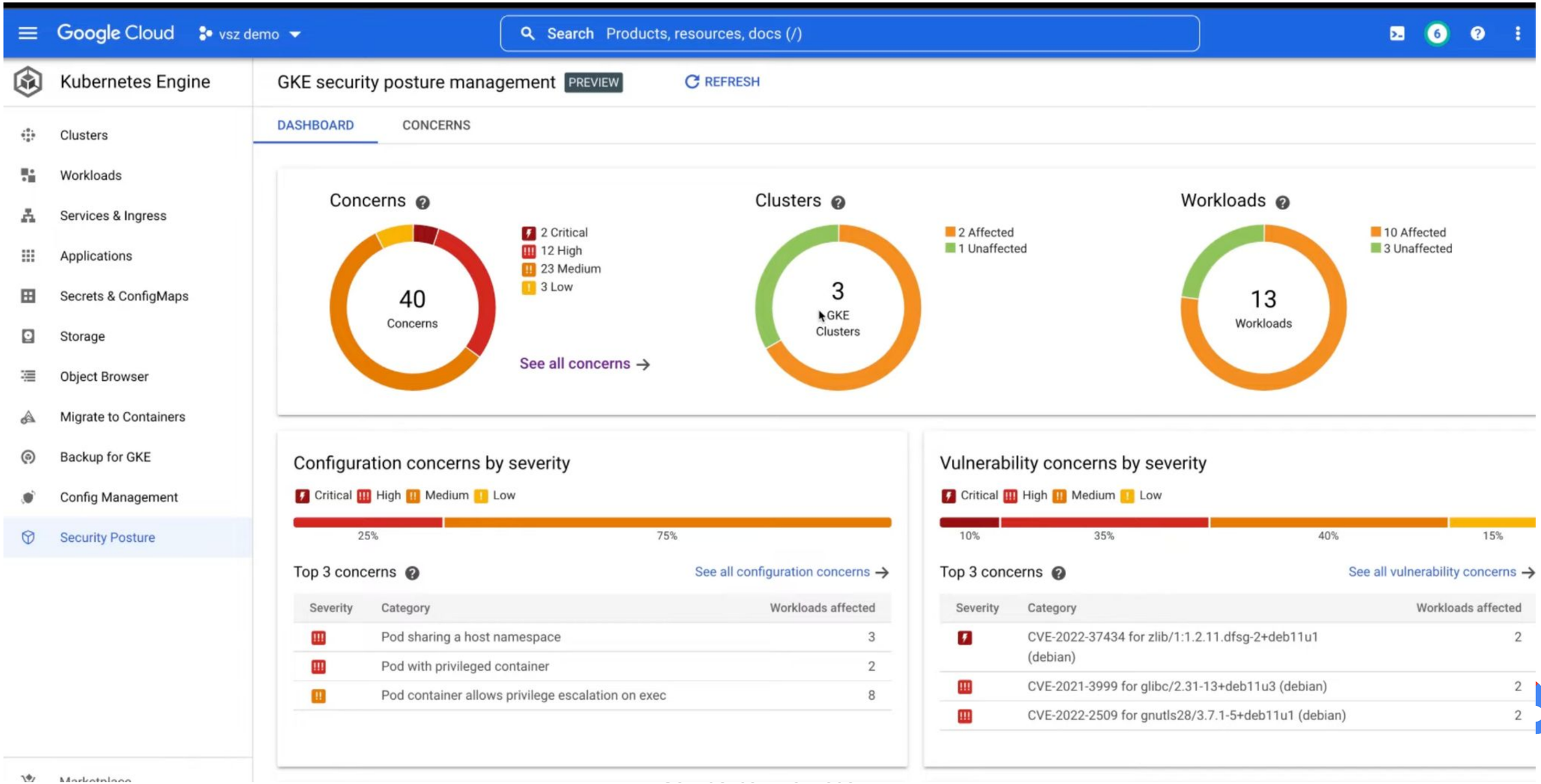
Rather than achieving isolation via separate VMs, you can run workloads of different trust levels on the same node

Performance improvements from not having to allocate a new cluster to achieve isolation





GKE Cluster Security Posture



4.2 Diagnostic Question 05 Discussion

Cymbal Bank has Docker applications deployed in Google Kubernetes Engine. The bank has no offline containers. This GKE cluster is exposed to the public internet and has recently recovered from an attack. Cymbal Bank suspects that someone in the organization changed the firewall rules and has tasked you to analyze and find all details related to the firewall for the cluster. You want the most cost-effective solution for this task.

What should you do?

A. View the GKE logs in Cloud Logging. Use the log scoping tool to filter the Firewall Rules log. Create a Pub/Sub topic. Export the logs to a Pub/Sub topic using the command gcloud logging sinks create. Use Dataflow to read from Pub/Sub and query the stream.

B. View the GKE logs in the local GKE cluster. Use the kubectl Sysdig Capture tool to filter the Firewall Rules log. Create a Pub/Sub topic. Export these logs to a Pub/Sub topic using the GKE cluster. Use Dataflow to read from Pub/Sub and query the stream.

C. View the GKE logs in the local GKE cluster. Use Docker-explorer to explore the Docker file system. Filter and export the Firewall logs to Cloud Logging. Create a dataset in BigQuery to accept the logs. Use the command gcloud logging sinks create to export the logs to a BigQuery dataset. Query this dataset.

D. View the GKE logs in Cloud Logging. Use the log scoping tool to filter the Firewall Rules log. Create a dataset in BigQuery to accept the logs. Export the logs to BigQuery using the command gcloud logging sinks create. Query this dataset.

4.2 Diagnostic Question 05 Discussion

Cymbal Bank has Docker applications deployed in Google Kubernetes Engine. The bank has no offline containers. This GKE cluster is exposed to the public internet and has recently recovered from an attack. Cymbal Bank suspects that someone in the organization changed the firewall rules and has tasked you to analyze and find all details related to the firewall for the cluster. You want the most cost-effective solution for this task.

What should you do?

A. View the GKE logs in Cloud Logging. Use the log scoping tool to filter the Firewall Rules log. Create a Pub/Sub topic. Export the logs to a Pub/Sub topic using the command gcloud logging sinks create. Use Dataflow to read from Pub/Sub and query the stream.

B. View the GKE logs in the local GKE cluster. Use the kubectl Sysdig Capture tool to filter the Firewall Rules log. Create a Pub/Sub topic. Export these logs to a Pub/Sub topic using the GKE cluster. Use Dataflow to read from Pub/Sub and query the stream.

C. View the GKE logs in the local GKE cluster. Use Docker-explorer to explore the Docker file system. Filter and export the Firewall logs to Cloud Logging. Create a dataset in BigQuery to accept the logs. Use the command gcloud logging sinks create to export the logs to a BigQuery dataset. Query this dataset.

D. View the GKE logs in Cloud Logging. Use the log scoping tool to filter the Firewall Rules log. Create a dataset in BigQuery to accept the logs. Export the logs to BigQuery using the command gcloud logging sinks create. Query this dataset.

3.2 Diagnostic Question 08 Discussion

Cymbal Bank uses Google Kubernetes Engine (GKE) to deploy its Docker containers. You want to encrypt the boot disk for a cluster running a custom image so that the key rotation is controlled by the Bank. GKE clusters will also generate up to 1024 randomized characters that will be used with the keys with Docker containers.

What steps would you take to apply the encryption settings with a dedicated hardware security layer?

A. In the Google Cloud console, navigate to Google Kubernetes Engine. Select your cluster and the boot node inside the cluster. Enable customer-managed encryption. Use Cloud HSM to generate random bytes and provide an additional layer of security.

B. Create a new GKE cluster with customer-managed encryption and HSM enabled. Deploy the containers to this cluster. Delete the old GKE cluster. Use Cloud HSM to generate random bytes and provide an additional layer of security.

C. Create a new key ring using Cloud Key Management Service. Extract this key to a certificate. Use the kubectl command to update the Kubernetes configuration. Validate using MAC digital signatures, and use a startup script to generate random bytes.

D. Create a new key ring using Cloud Key Management Service. Extract this key to a certificate. Use the Google Cloud Console to update the Kubernetes configuration. Validate using MAC digital signatures, and use a startup script to generate random bytes.

3.2 Diagnostic Question 08 Discussion

Cymbal Bank uses Google Kubernetes Engine (GKE) to deploy its Docker containers. You want to encrypt the boot disk for a cluster running a custom image so that the key rotation is controlled by the Bank. GKE clusters will also generate up to 1024 randomized characters that will be used with the keys with Docker containers.

What steps would you take to apply the encryption settings with a dedicated hardware security layer?

A. In the Google Cloud console, navigate to Google Kubernetes Engine. Select your cluster and the boot node inside the cluster. Enable customer-managed encryption. Use Cloud HSM to generate random bytes and provide an additional layer of security.

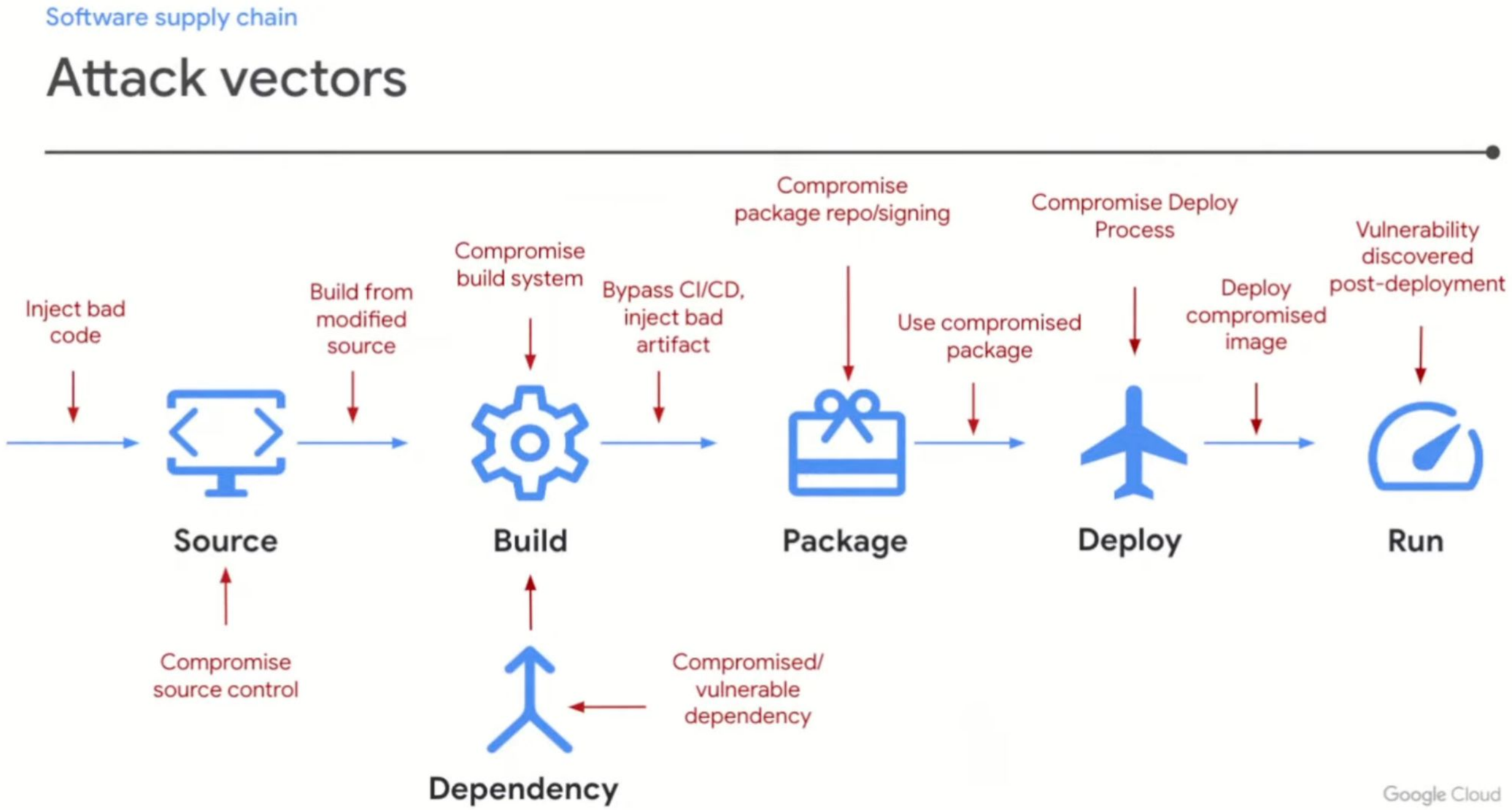
B. Create a new GKE cluster with customer-managed encryption and HSM enabled. Deploy the containers to this cluster. Delete the old GKE cluster. Use Cloud HSM to generate random bytes and provide an additional layer of security.

C. Create a new key ring using Cloud Key Management Service. Extract this key to a certificate. Use the kubectl command to update the Kubernetes configuration. Validate using MAC digital signatures, and use a startup script to generate random bytes.

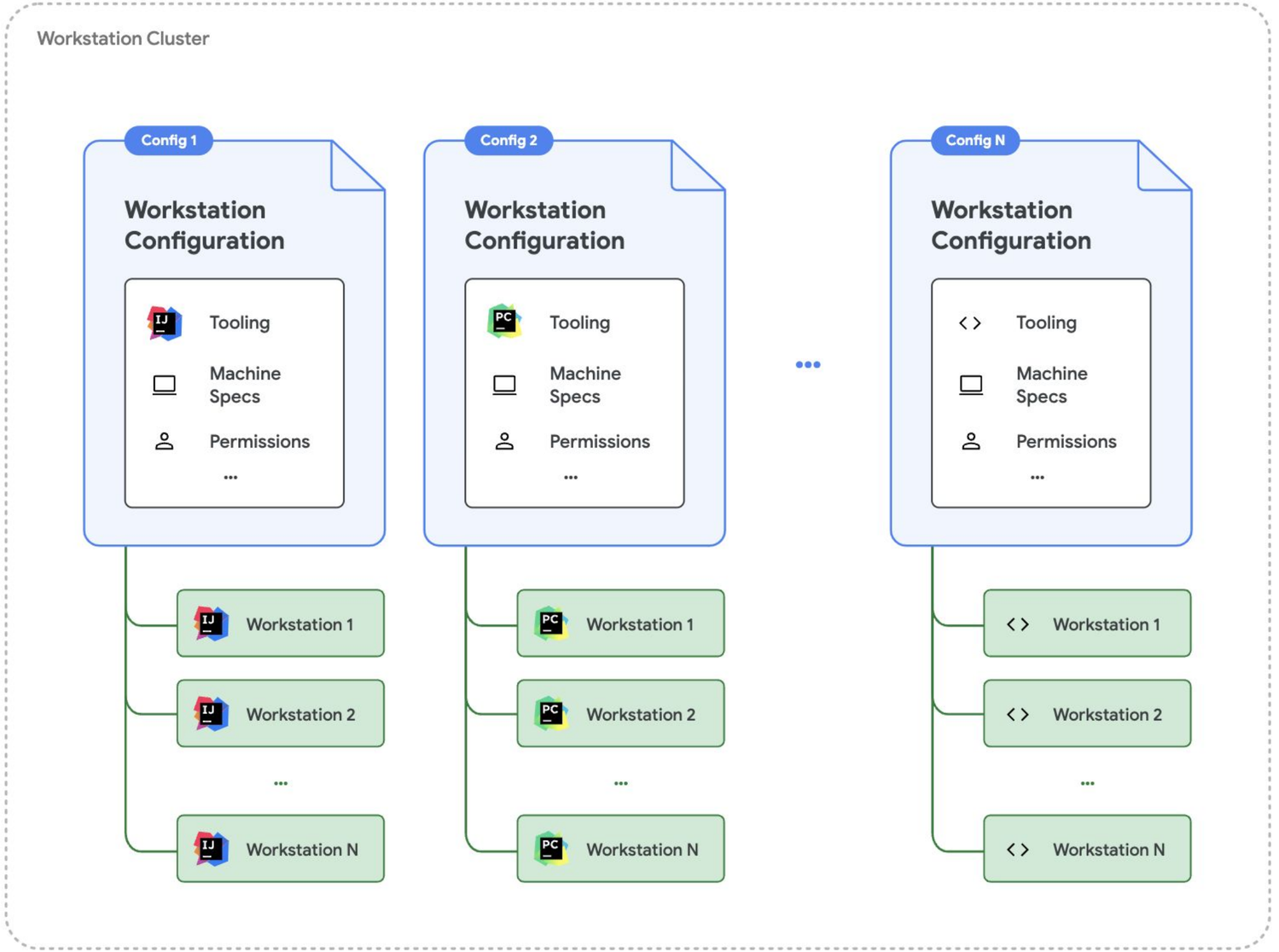
D. Create a new key ring using Cloud Key Management Service. Extract this key to a certificate. Use the Google Cloud Console to update the Kubernetes configuration. Validate using MAC digital signatures, and use a startup script to generate random bytes.

CI/CD Security

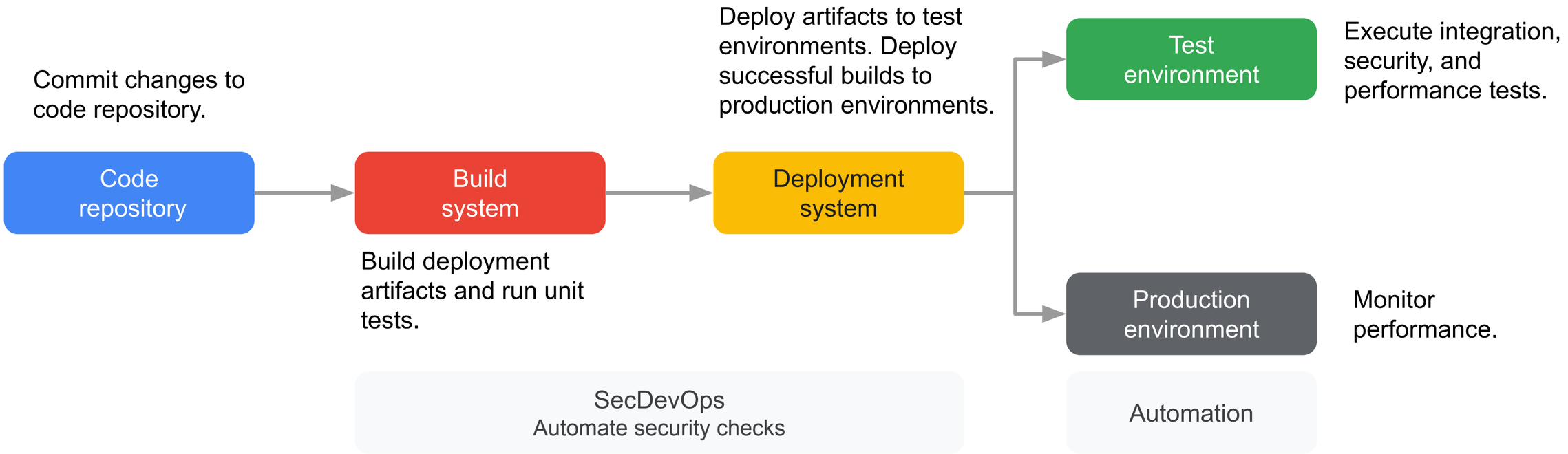
Why do we need to talk about security in CI/CD?



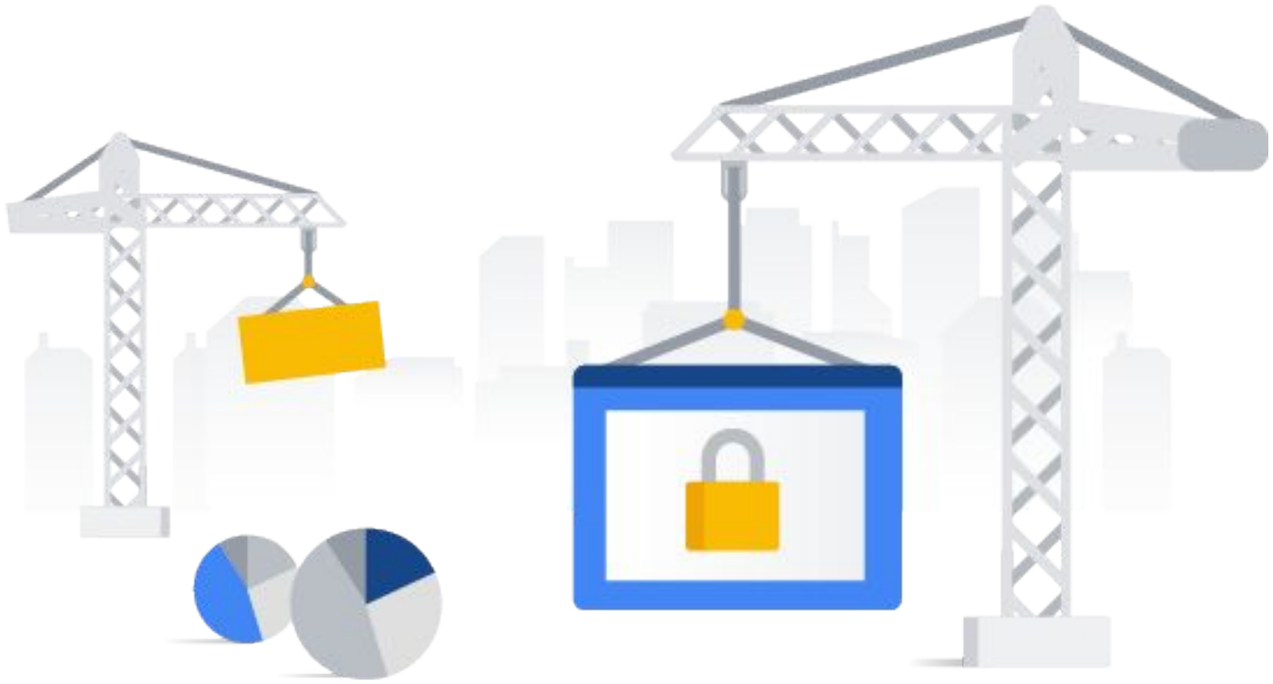
Cloud Workstations



Automated security operations in CI/CD pipelines

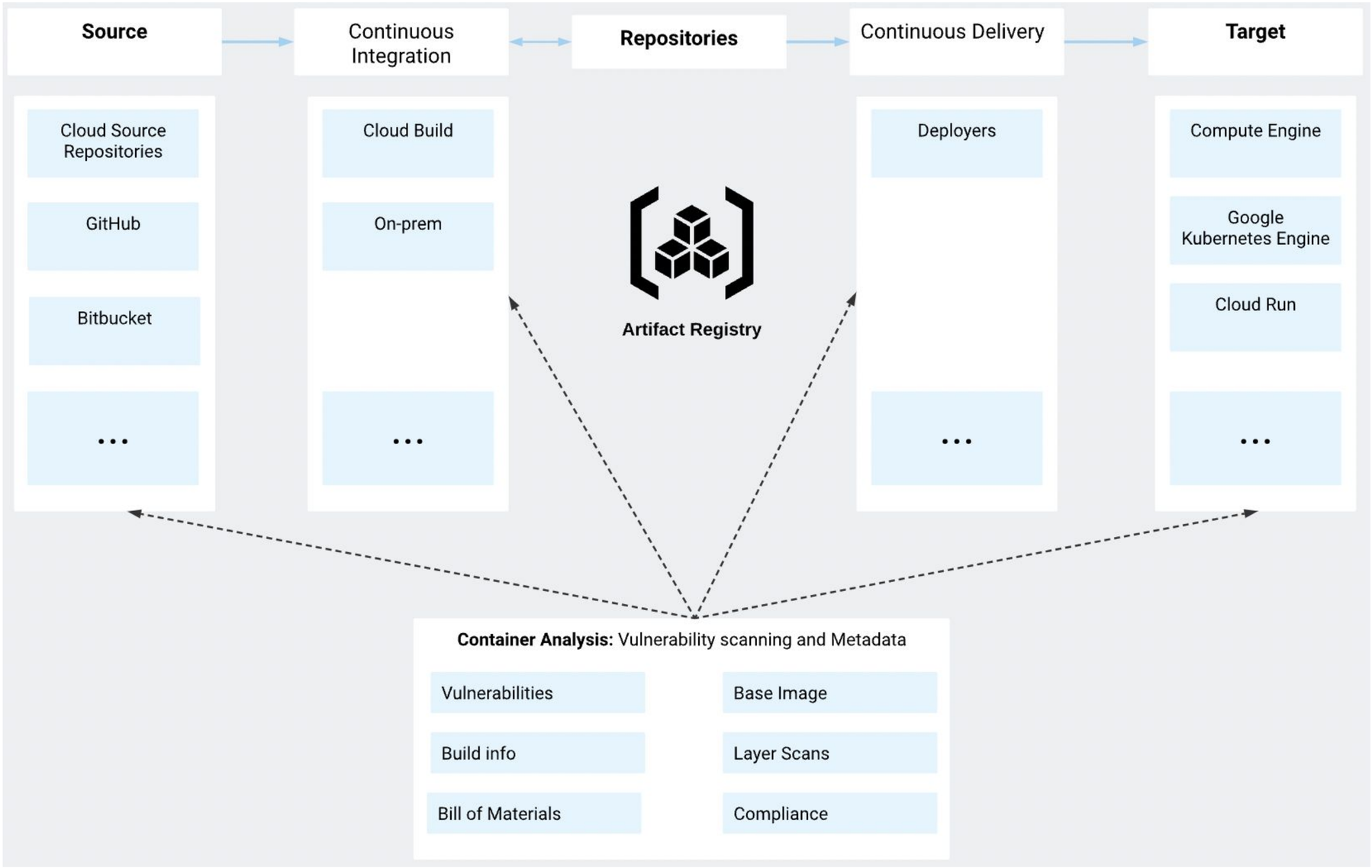


Infrastructure as code (IaC) for infrastructure creation and updates in CI/CD



- Terraform can be used to create immutable infrastructure which can be modified or deleted and recreated quickly in an automated response to incidents or attacks.
- Packer can be used to create baked images so software and configurations of virtual machines can remain fixed, reducing chance of insecure configuration.

Container analysis and vulnerability scanning



Binary Authorization

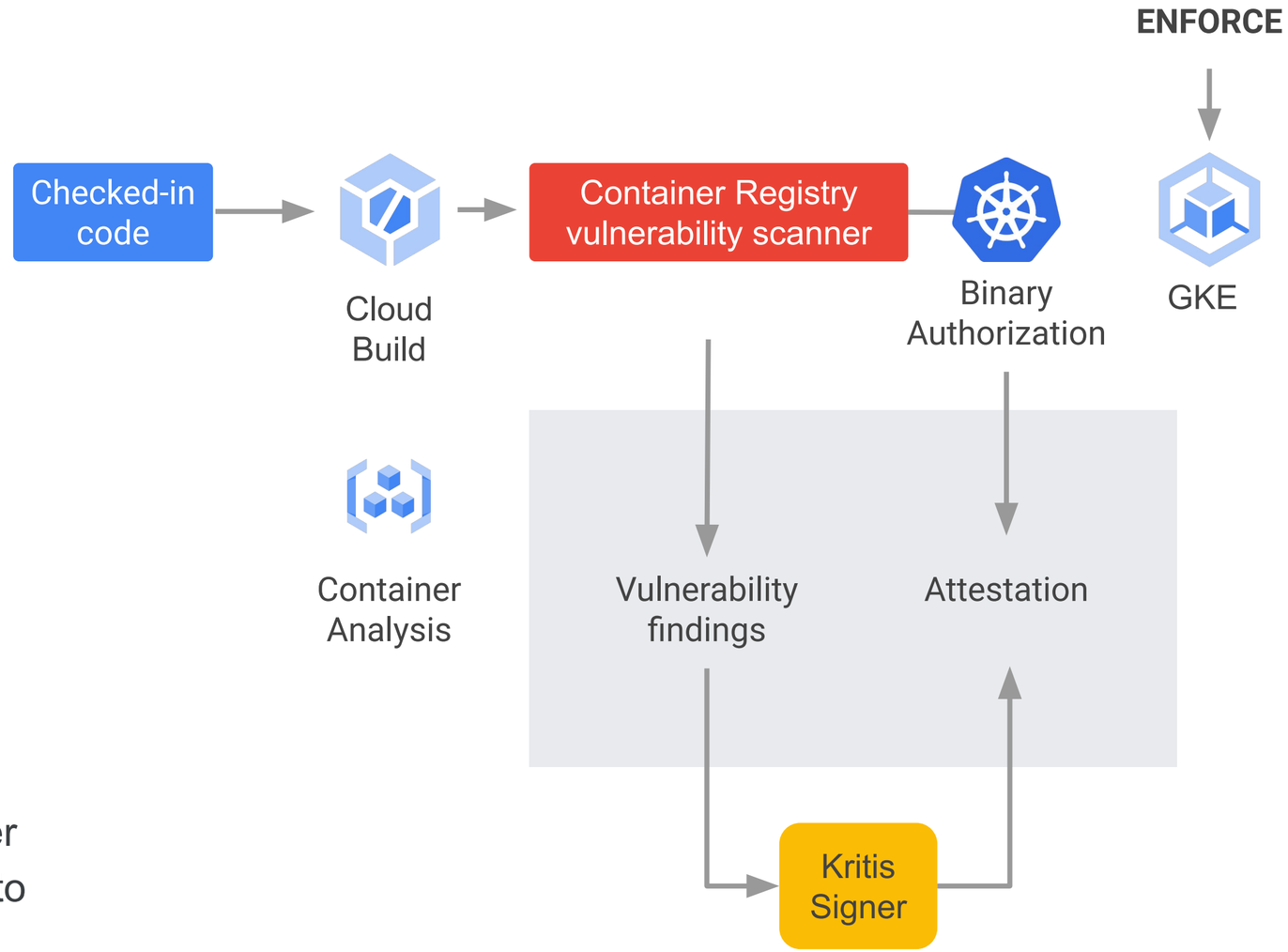
Run only what you trust. Allow only signed images or trusted repos

Images signed in CI/CD

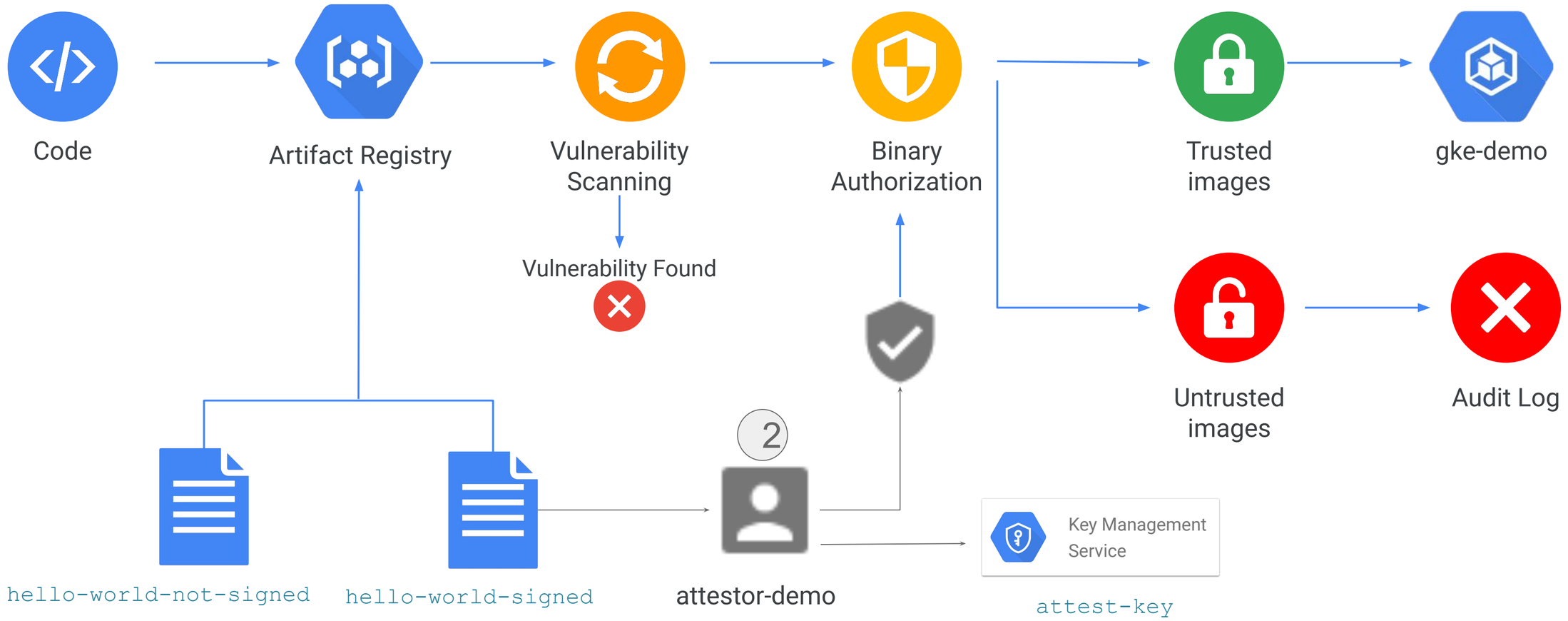
Deployments blocked/allowed at GKE control plane based on policy

Binary authorization to enforce secure container image deployment

- When an image is built by Cloud Build an “attestor” verifies that it was from a trusted repository, built by a specific pipeline, passed tests, and was scanned for vulnerabilities.
- Artifact Registry includes a vulnerability scanner that scans containers and results can be used to apply attestations allowing or blocking deployment.



Example of end-to-end CI/CD pipeline



Google Cloud

4.1 Diagnostic Question 01 Discussion

Cymbal Bank has received Docker source files from its third-party developers in an Artifact Registry repository. These Docker fil2es will be part of a CI/CD pipeline to update Cymbal Bank's personal loan offering. The bank wants to prevent the possibility of remote users arbitrarily using the Docker files to run any code. You have been tasked with using Container Analysis' On-Demand scanning to scan the images for a one-time

What should you do?

A. Prepare a cloudbuild.yaml file. In this file, add four steps in order—build, scan, severity check, and push—specifying the location of Artifact Registry repository. Specify severity level as **CRITICAL**. Start the build with the command `gcloud builds submit.`

B. Prepare a cloudbuild.yaml file. In this file, add four steps in order—scan, build, severity check, and push—specifying the location of the Artifact Registry repository. Specify severity level as **HIGH**. Start the build with the command `gcloud builds submit.`

C. Prepare a cloudbuild.yaml file. In this file, add four steps in order—scan, severity check, build, and—push specifying the location of the Artifact Registry repository. Specify severity level as **HIGH**. Start the build with the command `gcloud builds submit.`

D. Prepare a cloudbuild.yaml file. In this file, add four steps in order—build, severity check, scan, and push—specifying the location of the Artifact Registry repository. Specify severity level as **CRITICAL**. Start the build with the command `gcloud builds submit.`

4.1 Diagnostic Question 01 Discussion

Cymbal Bank has received Docker source files from its third-party developers in an Artifact Registry repository. These Docker fil2es will be part of a CI/CD pipeline to update Cymbal Bank's personal loan offering. The bank wants to prevent the possibility of remote users arbitrarily using the Docker files to run any code. You have been tasked with using Container Analysis' On-Demand scanning to scan the images for a one-time

What should you do?

A. **Prepare a cloudbuild.yaml file. In this file, add four steps in order—build, scan, severity check, and push—specifying the location of Artifact Registry repository. Specify severity level as CRITICAL. Start the build with the command `gcloud builds submit.`**

B. Prepare a cloudbuild.yaml file. In this file, add four steps in order—scan, build, severity check, and push—specifying the location of the Artifact Registry repository. Specify severity level as **HIGH**. Start the build with the command `gcloud builds submit.`

C. Prepare a cloudbuild.yaml file. In this file, add four steps in order—scan, severity check, build, and—push specifying the location of the Artifact Registry repository. Specify severity level as **HIGH**. Start the build with the command `gcloud builds submit.`

D. Prepare a cloudbuild.yaml file. In this file, add four steps in order—build, severity check, scan, and push—specifying the location of the Artifact Registry repository. Specify severity level as **CRITICAL**. Start the build with the command `gcloud builds submit.`

4.1 Diagnostic Question 04 Discussion

Cymbal Bank uses Docker containers to interact with APIs for its personal banking application. These APIs are under PCI-DSS compliance. The Kubernetes environment running the containers will not have internet access to download required packages.

How would you automate the pipeline that is building these containers?

A. Create a Dockerfile with container definition and cloudbuild.yaml file. Use Cloud Build to build the image from Dockerfile. Upload the built image to a Google Container registry and Dockerfile to a Git repository. In the cloudbuild.yaml template, include attributes to tag the Git repository path with a Google Kubernetes Engine cluster. Create a trigger in Cloud Build to automate the deployment using the Git repository.

B. Create a Dockerfile with a container definition and a Cloud Build configuration file. Use the Cloud Build configuration file to build and deploy the image from Dockerfile to a Google Container registry. In the configuration file, include the Google Container Registry path and the Google Kubernetes Engine cluster. Upload the configuration file to a Git repository. Create a trigger in Cloud Build to automate the deployment using the Git repository.

C. Build a foundation image. Store all artifacts and a Packer definition template in a Git repository. Use Container Registry to build the artifacts and Packer definition. Use Cloud Build to extract the built container and deploy it to a Google Kubernetes Engine (GKE) cluster. Add the required users and groups to the GKE project.

D. Build an immutable image. Store all artifacts and a Packer definition template in a Git repository. Use Container Registry to build the artifacts and Packer definition. Use Cloud Build to extract the built container and deploy it to a Google Kubernetes Engine Cluster (GKE). Add the required users and groups to the GKE project.

4.1 Diagnostic Question 04 Discussion

Cymbal Bank uses Docker containers to interact with APIs for its personal banking application. These APIs are under PCI-DSS compliance. The Kubernetes environment running the containers will not have internet access to download required packages.

How would you automate the pipeline that is building these containers?

A. Create a Dockerfile with container definition and cloudbuild.yaml file. Use Cloud Build to build the image from Dockerfile. Upload the built image to a Google Container registry and Dockerfile to a Git repository. In the cloudbuild.yaml template, include attributes to tag the Git repository path with a Google Kubernetes Engine cluster. Create a trigger in Cloud Build to automate the deployment using the Git repository.

B. Create a Dockerfile with a container definition and a Cloud Build configuration file. Use the Cloud Build configuration file to build and deploy the image from Dockerfile to a Google Container registry. In the configuration file, include the Google Container Registry path and the Google Kubernetes Engine cluster. Upload the configuration file to a Git repository. Create a trigger in Cloud Build to automate the deployment using the Git repository.

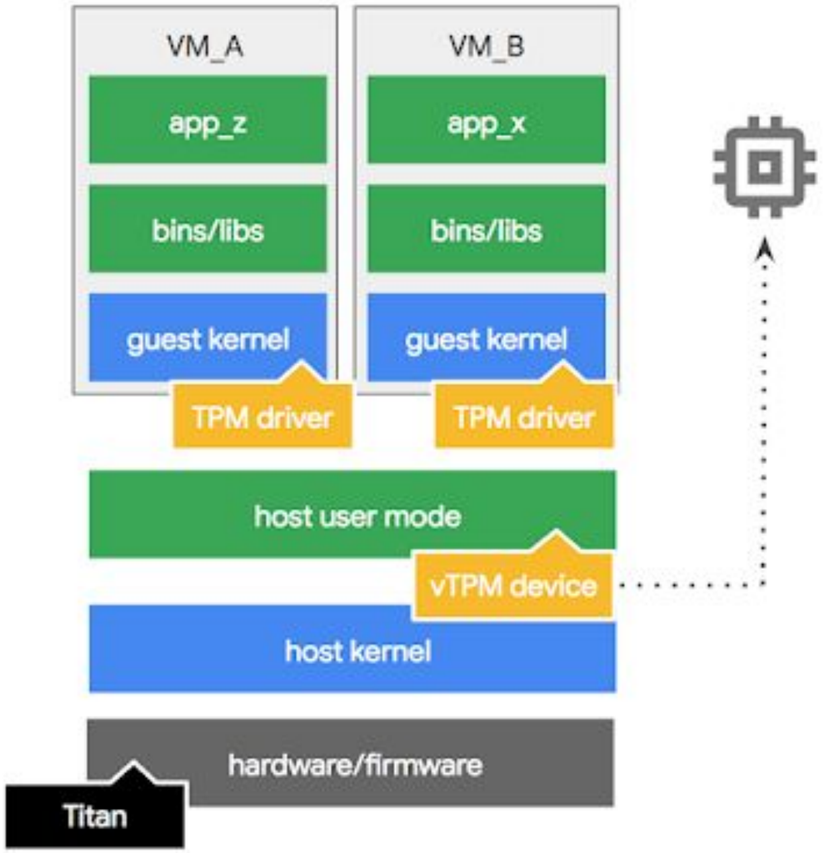
C. Build a foundation image. Store all artifacts and a Packer definition template in a Git repository. Use Container Registry to build the artifacts and Packer definition. Use Cloud Build to extract the built container and deploy it to a Google Kubernetes Engine (GKE) cluster. Add the required users and groups to the GKE project.

D. Build an immutable image. Store all artifacts and a Packer definition template in a Git repository. Use Container Registry to build the artifacts and Packer definition. Use Cloud Build to extract the built container and deploy it to a Google Kubernetes Engine Cluster (GKE). Add the required users and groups to the GKE project.

Securing VMs

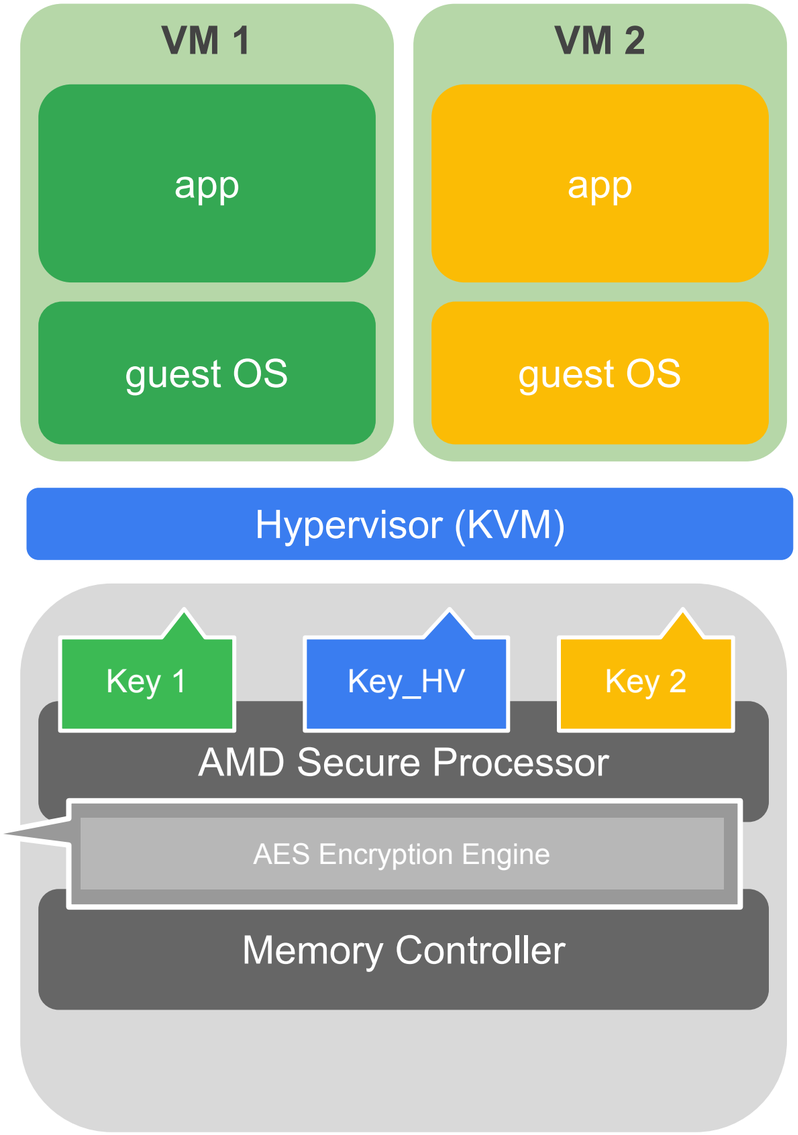
Shielded VM: Secure Boot

- Instances firmware signed and verified using Google's Certificate Authority
- Ensures firmware is unmodified
- Establishes the root of trust for Secure Boot
- Unified Extensible Firmware Interface (UEFI) firmware securely stores the keys used by the software manufacturers to sign the system firmware, the system boot loader, and any binaries they load.
- Requirements:
  - Must use OS images with shielded VM features
    - Container-Optimized OS, Ubuntu, and Windows Server
    - CLI option: `--image-project=gce-uefi-images`
  - Custom images can be built from shielded VM images



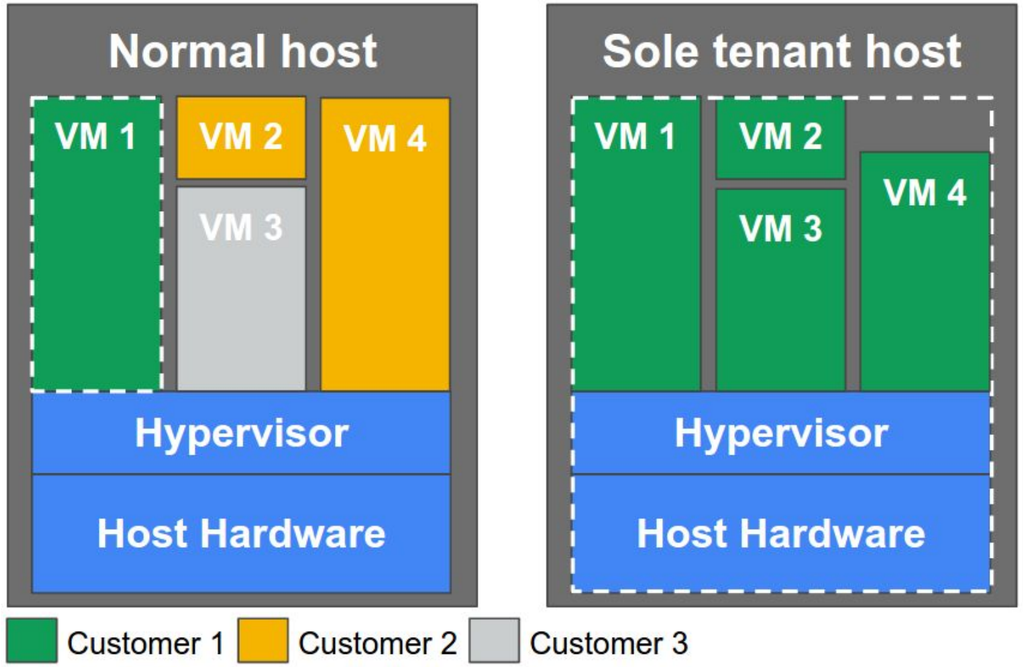
Confidential VM

- Same as a regular Compute Engine VM
  - Anything that runs on VM runs on confidential VM
- Data encrypted while in use
  - Memory encrypted, decrypted only on CPU chip
  - A key per VM
    - Random, ephemeral, generated by HW
    - Not extractable from HW
- Scale up to 224 vCPUs and 896 GiB memory



Sole-tenant nodes

- Launch your instances on dedicated, physical servers
- Helps meet compliance requirements
- Supports live migration
- Use the placement algorithm or specify placement with labels
- Customize your machine types or “shapes” for best utilization
- Eligible for committed and sustained use discounts



OS Login

Accessing Compute Engine instances

SSH Keys vs **OS Login**

SSH Keys

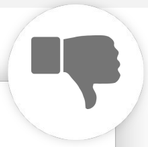
Generate and upload keys as **metadata**

- Requires appropriate permissions

Instance/project level

Cloud Console / gcloud automatically manages key lifecycle

Easy to start using



Complex access lifecycle management

Risk allowing access by non-org users

No granular access control (root vs. non-root)

OS Login

Best practice

Ties Linux accounts with Google identities and **Cloud IAM**

Supports **2FA** (Google Authenticator app, text, phone)

Instance/project level

Easy access lifecycle management

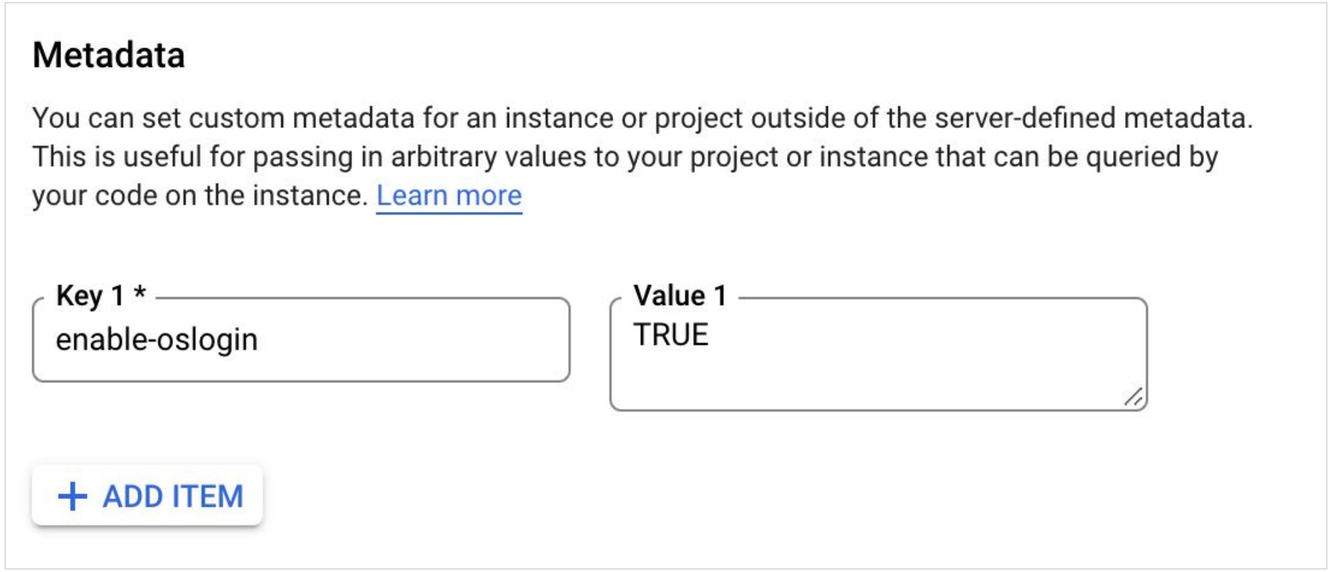
Permissions updated immediately

Granular access control

Not enabled by default, and requires a methodology to ensure consistency (e.g IaC)

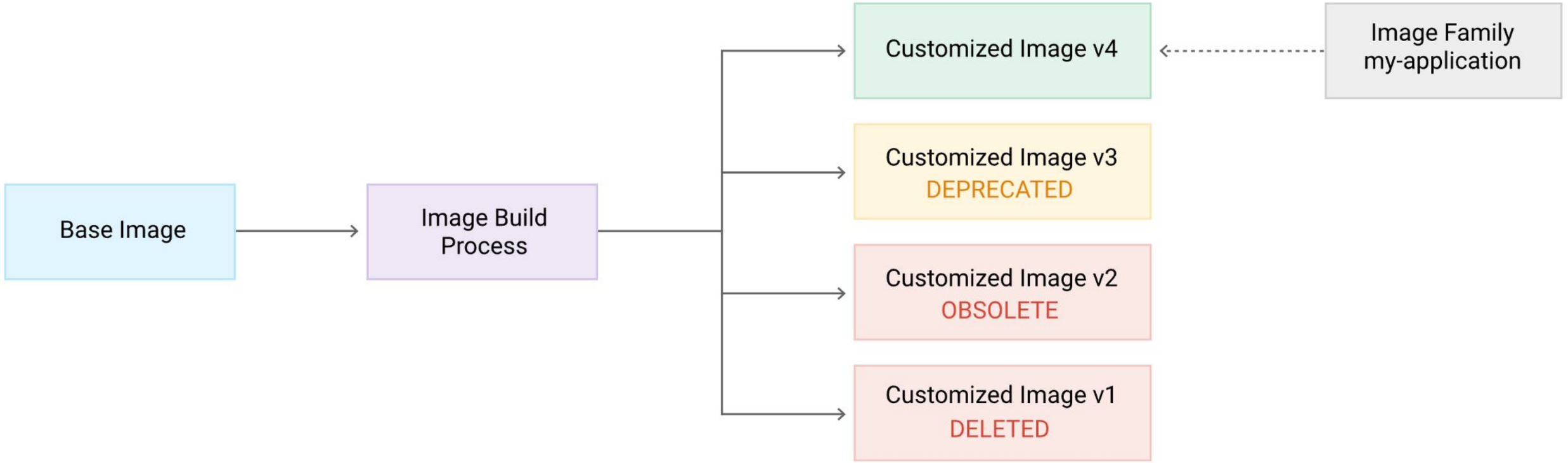
OS Login - Overview

- Manage SSH access to your instances using IAM
- Maintains consistent Linux user identity across VM instances
- Recommended way to manage many users across multiple instances or projects
- Simplifies SSH access management



OS Image Families

OS Image Families



Be familiar with:

- Image life cycle (DEPRECATED / OBSOLETE / DELETED)
- Trusted image policies (based on Org policy; centralization)
- Sharing images between projects
- Image Families best practices

4.1 Diagnostic Question 02 Discussion

Cymbal Bank's management is concerned about virtual machines being compromised by bad actors. More specifically, they want to receive immediate alerts if there have been changes to the boot sequence of any of their Compute Engine instances.

What should you do?

A. Set an organization-level policy that requires all Compute Engine VMs to be configured as Shielded VMs. Use Secure Boot enabled with Unified Extensible Firmware Interface (UEFI). Validate integrity events in Cloud Monitoring and place alerts on launch attestation events.

B. Set Cloud Logging measurement policies on the VMs. Use Cloud Logging to place alerts whenever actualMeasurements and policyMeasurements don't match.

C. Set an organization-level policy that requires all Compute Engine VMs to be configured as Shielded VMs. Use Measured Boot enabled with Virtual Trusted Platform Module (vTPM). Validate integrity events in Cloud Monitoring and place alerts on late boot validation events.

D. Set project-level policies that require all Compute Engine VMs to be configured as Shielded VMs. Use Measured Boot enabled with Virtual Trusted Platform Module (vTPM). Validate integrity events in Cloud Monitoring and place alerts on late boot validation events.

4.1 Diagnostic Question 02 Discussion

Cymbal Bank's management is concerned about virtual machines being compromised by bad actors. More specifically, they want to receive immediate alerts if there have been changes to the boot sequence of any of their Compute Engine instances.

What should you do?

A. Set an organization-level policy that requires all Compute Engine VMs to be configured as Shielded VMs. Use Secure Boot enabled with Unified Extensible Firmware Interface (UEFI). Validate integrity events in Cloud Monitoring and place alerts on launch attestation events.

B. Set Cloud Logging measurement policies on the VMs. Use Cloud Logging to place alerts whenever actualMeasurements and policyMeasurements don't match.

C. Set an organization-level policy that requires all Compute Engine VMs to be configured as Shielded VMs. Use Measured Boot enabled with Virtual Trusted Platform Module (vTPM). Validate integrity events in Cloud Monitoring and place alerts on late boot validation events.

D. Set project-level policies that require all Compute Engine VMs to be configured as Shielded VMs. Use Measured Boot enabled with Virtual Trusted Platform Module (vTPM). Validate integrity events in Cloud Monitoring and place alerts on late boot validation events.

4.1 Diagnostic Question 03 Discussion

Cymbal Bank runs a Node.js application on a Compute Engine instance. Cymbal Bank needs to share this base image with a ‘development’ Google Group. This base image should support secure boot for the Compute Engine instances deployed from this image. How would you automate the image creation?

How would you automate the image creation?

A. Prepare a shell script. Add the command gcloud compute instances stop with the Node.js instance name. Set up certificates for secure boot. Add gcloud compute images create, and specify the Compute Engine instance’s persistent disk and zone and the certificate files. Add gcloud compute images add-iam-policy-binding and specify the ‘development’ group.

B. Start the Compute Engine instance. Set up certificates for secure boot. Prepare a cloudbuild.yaml configuration file. Specify the persistent disk location of the Compute Engine and the ‘development’ group. Use the command gcloud builds submit --tag, and specify the configuration file path and the certificates.

C. Prepare a shell script. Add the command gcloud compute instances start to the script to start the Node.js Compute Engine instance. Set up Measured Boot for secure boot. Add gcloud compute images create, and specify the persistent disk and zone of the Compute Engine instance.

D. Stop the Compute Engine instance. Set up Measured Boot for secure boot. Prepare a cloudbuild.yaml configuration file. Specify the persistent disk location of the Compute Engine instance and the ‘development’ group. Use the command gcloud builds submit --tag, and specify the configuration file path.

4.1 Diagnostic Question 03 Discussion

Cymbal Bank runs a Node.js application on a Compute Engine instance. Cymbal Bank needs to share this base image with a ‘development’ Google Group. This base image should support secure boot for the Compute Engine instances deployed from this image. How would you automate the image creation?

How would you automate the image creation?

A. **Prepare a shell script. Add the command gcloud compute instances stop with the Node.js instance name. Set up certificates for secure boot. Add gcloud compute images create, and specify the Compute Engine instance’s persistent disk and zone and the certificate files. Add gcloud compute images add-iam-policy-binding and specify the ‘development’ group.**

B. Start the Compute Engine instance. Set up certificates for secure boot. Prepare a cloudbuild.yaml configuration file. Specify the persistent disk location of the Compute Engine and the ‘development’ group. Use the command gcloud builds submit --tag, and specify the configuration file path and the certificates.

C. Prepare a shell script. Add the command gcloud compute instances start to the script to start the Node.js Compute Engine instance. Set up Measured Boot for secure boot. Add gcloud compute images create, and specify the persistent disk and zone of the Compute Engine instance.

D. Stop the Compute Engine instance. Set up Measured Boot for secure boot. Prepare a cloudbuild.yaml configuration file. Specify the persistent disk location of the Compute Engine instance and the ‘development’ group. Use the command gcloud builds submit --tag, and specify the configuration file path.

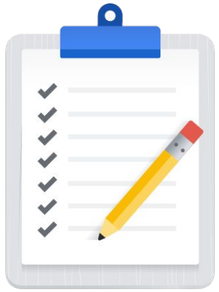
Cloud Logging

Security monitoring and incident response process

Cymbal Bank will use Google Cloud's operations suite to capture, visualize, and alert on logs or metrics indicating security incidents.

Monitoring dashboard

Alerting regimen



Plans and tools for responding to issues

Log categories

Security Logs

Google Cloud audit logs, Google Workspace audit logs and access transparency logs

Multi-cloud and On-premises Logs

Logs from other cloud services providers or on-prem workloads

Platform Logs

Service-specific logs generated by Google Cloud

System/App Logs

Logs generated by system services or applications

SECURITY LOGS

Google Cloud audit logs

Record who did what when in your Cloud org

Admin activity

API calls / actions **modifying resource configuration or metadata**
e.g. create VM instance, create object in bucket

Data access

API calls **reading resources or resource metadata**
e.g. admin-read, list Cloud Storage buckets; data-read read/write Cloud Storage object data

Access transparency

Actions and accesses **performed by Google staff** on your resources
e.g. support troubleshooting an open case

System event

Google Cloud **managed service modifying resources**
e.g. *Compute Engine VM live migration, reclaiming a Spot instance*

Policy denied

Google Cloud **service denying access** to an identity because of a policy violation
e.g. user is not authorized to list bucket contents

SECURITY LOGS

Google Cloud audit logs (Cont.)

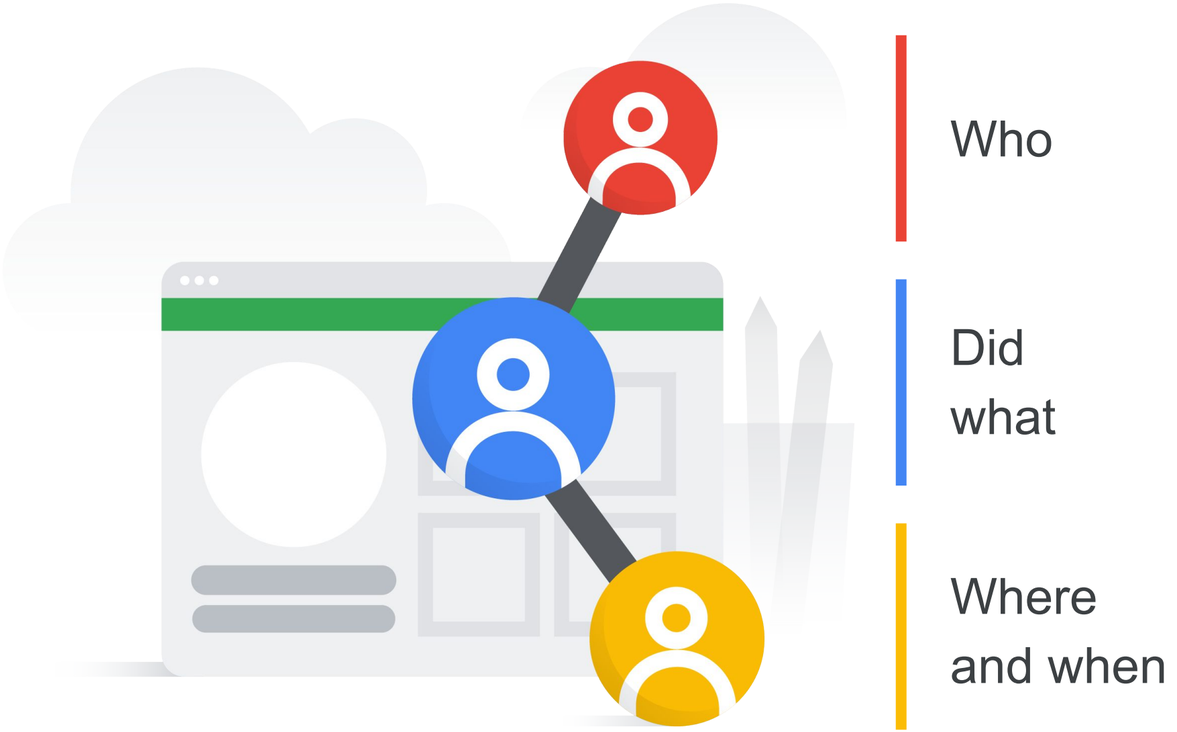
		enabled by default?	can be disabled?	free of charge?	retention	min-max retention
admin activity		Yes	No	Yes*	400d	N/A*
data access	BigQuery	Yes	No	Yes*	30d	1d-10y
	other services	No	Yes	No	30d	1d-10y
access transparency		No	Yes	Yes	400d	N/A*
system event		Yes	No	Yes*	400d	N/A*
policy denied		Yes	Yes	No	30d	1d-10y

** As long as they have not been routed to another storage destination.*

Cloud Audit Logs to detect invalid administrative activity

Audit logs provide a complete capture of administrative activity and should be periodically audited to ensure compliance

- Optionally enable data access logs to capture reads and writes to managed data storage
- Optionally export logs for long-term storage or analysis



3.2 Diagnostic Question 10 Discussion

Cymbal Bank needs to migrate existing loan processing applications to Google Cloud. These applications transform confidential financial information. All the data should be encrypted at all stages, including sharing between sockets and RAM. An integrity test should also be performed every time these instances boot. You need to use Cymbal Bank's encryption keys to configure the Compute Engine instances.

What should you do?

A. Create a Confidential VM instance with Customer-Supplied Encryption Keys. In Cloud Logging, collect all logs for sevLaunchAttestationReportEvent.

B. Create a Shielded VM instance with Customer-Supplied Encryption Keys. In Cloud Logging, collect all logs for earlyBootReportEvent.

C. Create a Confidential VM instance with Customer-Managed Encryption Keys. In Cloud Logging, collect all logs for earlyBootReportEvent.

D. Create a Shielded VM instance with Customer-Managed Encryption Keys. In Cloud Logging, collect all logs for sevLaunchAttestationReportEvent.

3.2 Diagnostic Question 10 Discussion

Cymbal Bank needs to migrate existing loan processing applications to Google Cloud. These applications transform confidential financial information. All the data should be encrypted at all stages, including sharing between sockets and RAM. An integrity test should also be performed every time these instances boot. You need to use Cymbal Bank's encryption keys to configure the Compute Engine instances.

What should you do?

A. **Create a Confidential VM instance with Customer-Supplied Encryption Keys. In Cloud Logging, collect all logs for sevLaunchAttestationReportEvent.**

B. Create a Shielded VM instance with Customer-Supplied Encryption Keys. In Cloud Logging, collect all logs for earlyBootReportEvent.

C. Create a Confidential VM instance with Customer-Managed Encryption Keys. In Cloud Logging, collect all logs for earlyBootReportEvent.

D. Create a Shielded VM instance with Customer-Managed Encryption Keys. In Cloud Logging, collect all logs for sevLaunchAttestationReportEvent.

4.2 Diagnostic Question 07 Discussion

Cymbal Bank wants to use Cloud Storage and BigQuery to store safe deposit usage data. Cymbal Bank needs a cost-effective approach to auditing only Cloud Storage and BigQuery data access activities.

How would you use Cloud Audit Logs to enable this analysis?

A. Enable Data Access Logs for ADMIN_READ, DATA_READ, and DATA_WRITE at the service level for BigQuery and Cloud Storage.

B. Enable Data Access Logs for ADMIN_READ, DATA_READ, and DATA_WRITE at the organization level.

C. Enable Data Access Logs for ADMIN_READ, DATA_READ, and DATA_WRITE for Cloud Storage. All Data Access Logs are enabled for BigQuery by default.

D. Enable Data Access Logs for ADMIN_READ, DATA_READ, and DATA_WRITE for BigQuery. All Data Access Logs are enabled for Cloud Storage by default.

4.2 Diagnostic Question 07 Discussion

Cymbal Bank wants to use Cloud Storage and BigQuery to store safe deposit usage data. Cymbal Bank needs a cost-effective approach to auditing only Cloud Storage and BigQuery data access activities.

How would you use Cloud Audit Logs to enable this analysis?

A. Enable Data Access Logs for ADMIN_READ, DATA_READ, and DATA_WRITE at the service level for BigQuery and Cloud Storage.

B. Enable Data Access Logs for ADMIN_READ, DATA_READ, and DATA_WRITE at the organization level.

C. Enable Data Access Logs for ADMIN_READ, DATA_READ, and DATA_WRITE for Cloud Storage. All Data Access Logs are enabled for BigQuery by default.

D. Enable Data Access Logs for ADMIN_READ, DATA_READ, and DATA_WRITE for BigQuery. All Data Access Logs are enabled for Cloud Storage by default.

4.2 Diagnostic Question 09 Discussion

The loan application from Cymbal Bank's lending department collects credit reports that contain credit payment information from customers. According to bank policy, the PDF reports are stored for six months in Cloud Storage, and access logs for the reports are stored for three years. You need to configure a cost-effective storage solution for the access logs.

What should you do?

A. Set up a logging export dataset in BigQuery to collect data from Cloud Logging and Cloud Monitoring. Create table expiry rules to delete logs after three years.

B. Set up a logging export dataset in BigQuery to collect data from Cloud Logging and the Security Command Center. Create table expiry rules to delete logs after three years.

C. Set up a logging export bucket in Cloud Storage to collect data from the Security Command Center. Configure object lifecycle management rules to delete logs after three years.

D. Set up a logging export bucket in Cloud Storage to collect data from Cloud Audit Logs. Configure object lifecycle management rules to delete logs after three years.

4.2 Diagnostic Question 09 Discussion

The loan application from Cymbal Bank's lending department collects credit reports that contain credit payment information from customers. According to bank policy, the PDF reports are stored for six months in Cloud Storage, and access logs for the reports are stored for three years. You need to configure a cost-effective storage solution for the access logs.

What should you do?

A. Set up a logging export dataset in BigQuery to collect data from Cloud Logging and Cloud Monitoring. Create table expiry rules to delete logs after three years.

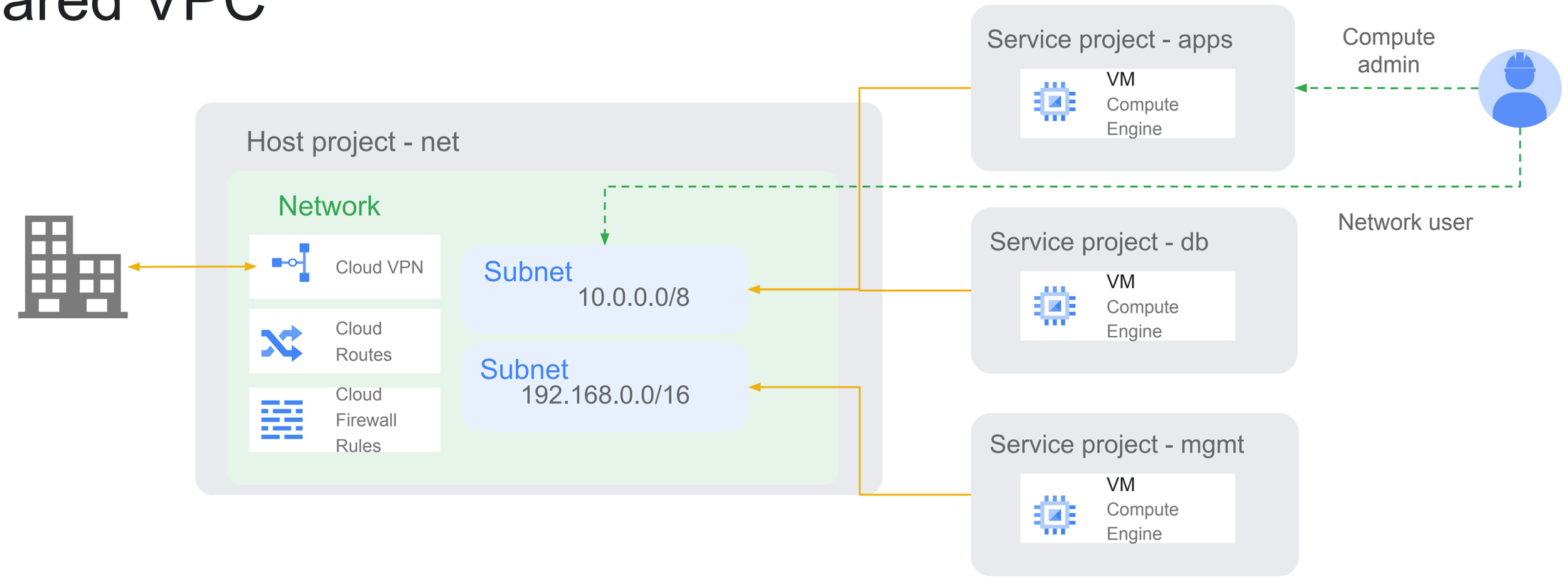
B. Set up a logging export dataset in BigQuery to collect data from Cloud Logging and the Security Command Center. Create table expiry rules to delete logs after three years.

C. Set up a logging export bucket in Cloud Storage to collect data from the Security Command Center. Configure object lifecycle management rules to delete logs after three years.

D. Set up a logging export bucket in Cloud Storage to collect data from Cloud Audit Logs. Configure object lifecycle management rules to delete logs after three years.

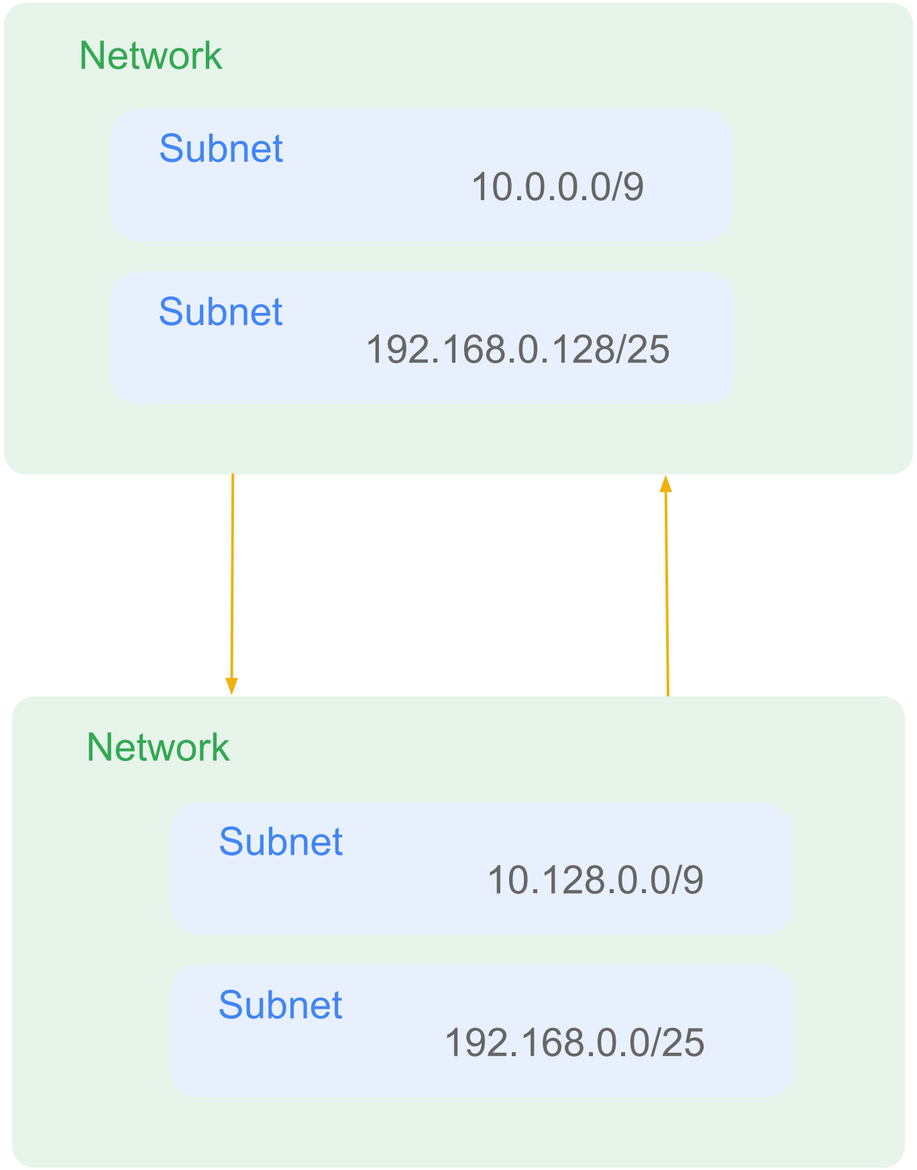
Shared VPC vs VPC Peering

Shared VPC



- ➔ Shared VPC is the most common way to share networks. Allows you the flexibility of having many projects (good for security / billings / etc) without the overhead of managing a lot of VPCs.
- ➔ Allows you to setup a robust network in the host project and share subnet(s) with service projects.
- ➔ Allows good security segmentation as admins on compute nodes don't need to admin network functions (only need user permissions).
- ➔ Connectivity to other networks (VPN and interconnects) and firewall rules can be centrally managed in the host project.
- ➔ Host and service projects ***must*** belong to the same GCP organization

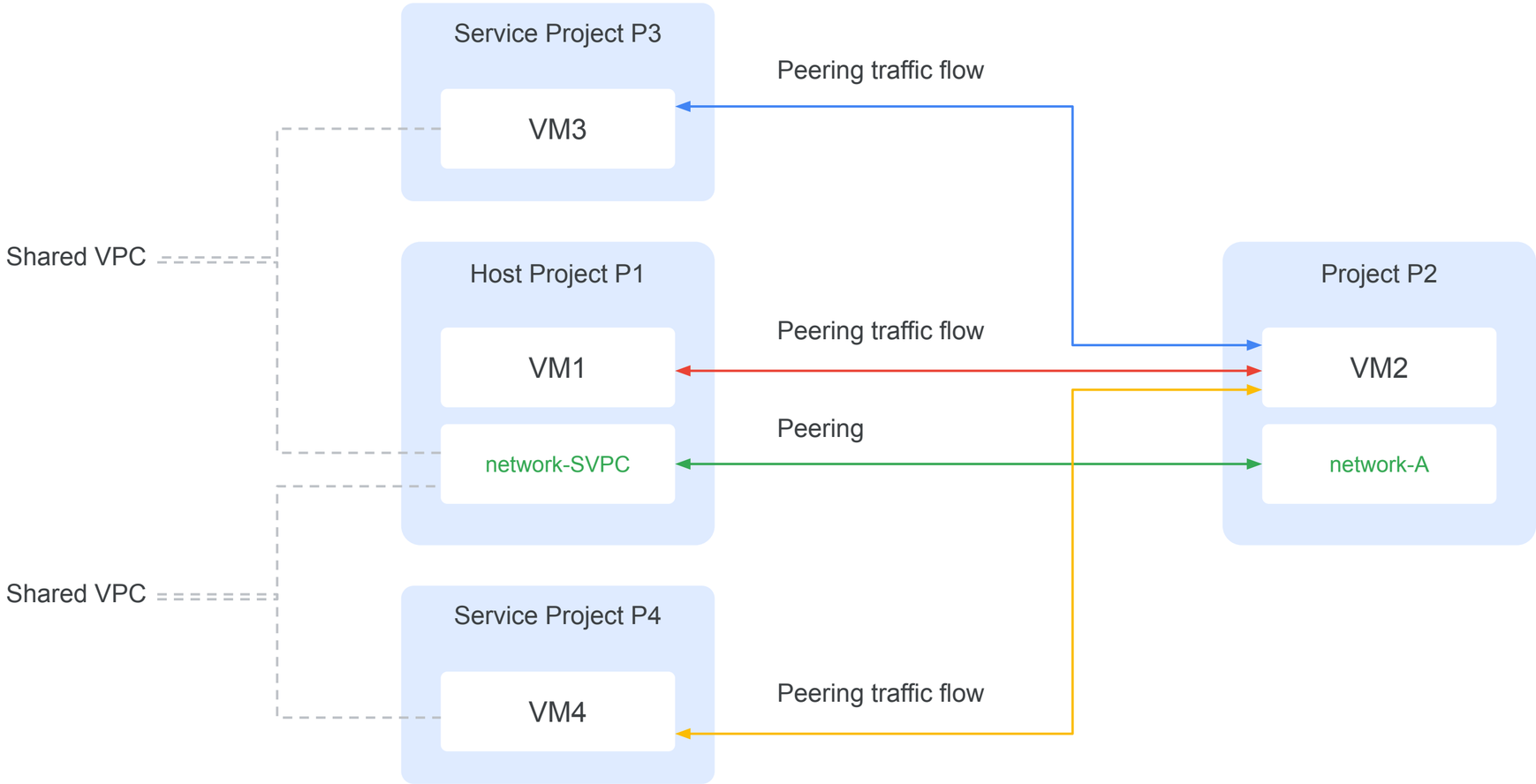
VPC Peering



- ➔ Peering works both within and between GCP organizations
- ➔ When setting up the peering you determine which subnet(s) to publish routes to
- ➔ Administrators on both sides must configure the peering in order for it to work
- ➔ The peering between the networks is **not** transitive, so traffic will not route to any other networks peered
- ➔ Links between the networks are high throughput and very low latency (unlike connecting via a VPN)
- ➔ IP Networks ***cannot*** overlap

Note: Starting to see peering as part of the solution for GCP Products: Apigee X and Datastream configurations both require peering as part of the setup

Shared VPCs AND VPC network peering…



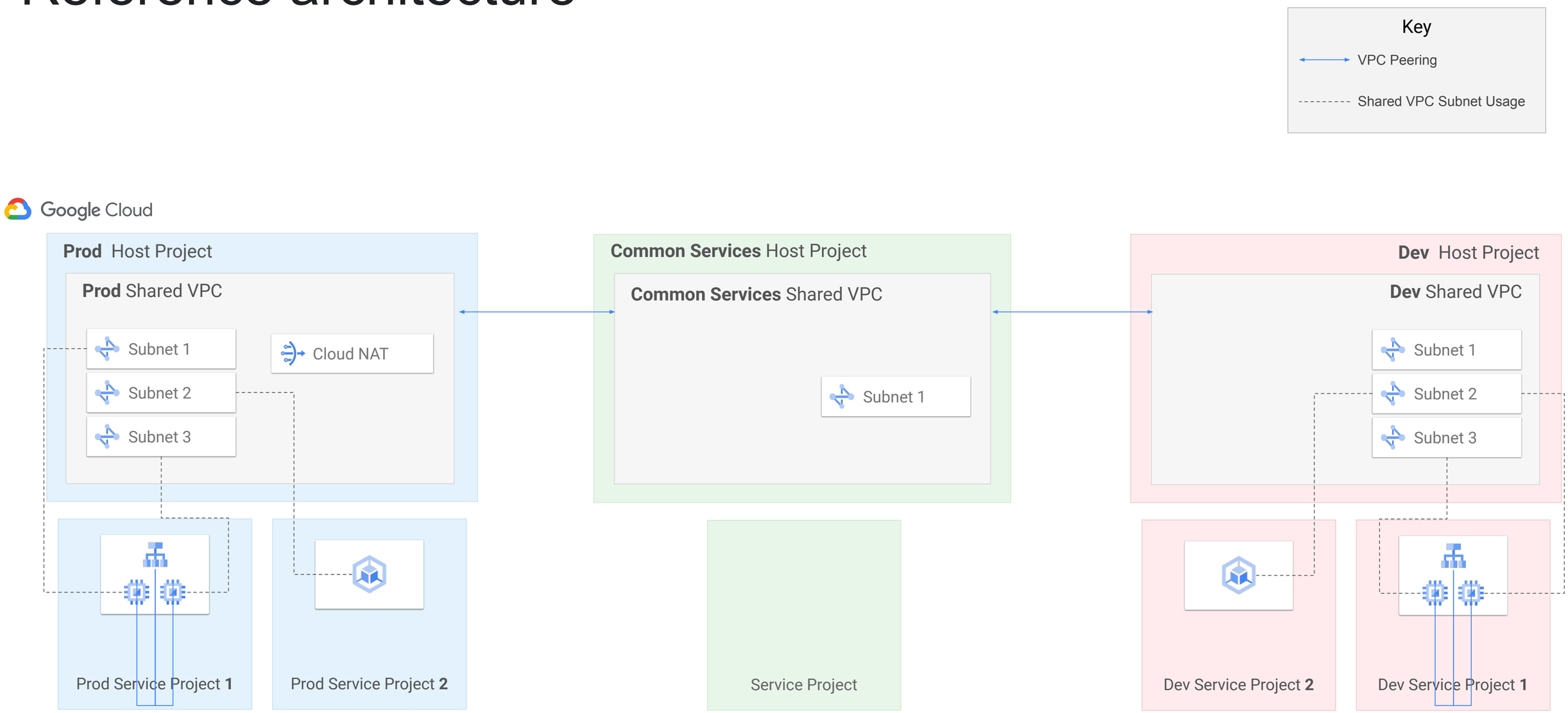
Shared VPC vs VPC Network Peering

Consideration	Shared VPC	VPC Network Peering
Across organizations	No	Yes
Within project	No	Yes
Network Administration	Centralized	Decentralized

Organization Admin		
Shared VPC Admin		
Security and Network Admins		
Project Owner	Project Owner	Project Owner

Organization Admin (if same org)		
Security and Network Admins	Security and Network Admins	Security and Network Admins
Project Owner	Project Owner	Project Owner

Reference architecture



Additional content

QUIZ week 4

(the one we went through during the meeting)

Reminder:

- NOT as complex as questions on the exam
- Technical knowledge validation (No business context)

Additional content 1

[READING]

- Disaster recovery scenarios for data
- Data incident response process - Creating and automating an incident response plan
- Cloud Audit Logs overview - Log sinks, audit logs, and data access logs for near-real-time monitoring
- Container analysis and vulnerability scanning - Automate security scanning for Common Vulnerabilities and Exposures (CVEs) through a CI/CD pipeline
- Create a Binary Authorization attestation in a Cloud Build pipeline
- OS Image management best practices
- Securing artifacts in Artifact Registry
- Monitoring and alerting on logs
- Trusted image policies - based on Organization Policy service
- Cloud Asset Inventory overview
- Monitoring asset changes
- VPC Flow logs + PAcket Mirroring + Cloud IDS explained
- Web Security Scanner overview
- Packet Mirroring overview and a blog post with a use-case.
- How to set up Packet Mirroring?
- Firewall Insights explained

Additional content 2

- Exporting security logs to SIEM system - a step-by-step tutorial, highly recommended.
- Overview of Forseti
- Granting access to an image in a different project to a MIG
- Container Threat Detection conceptual overview
- Firewall Insights - based on firewall logs
- Exporting logs to Splunk
- Scenarios for exporting logging data: Security and access analytics

[VIDEOS]

- [Recommended] How to secure your software supply chain from dependencies to deployment
- Security Command Center playlist (9 short videos)
- How to use Cloud Logging to detect security breaches
- Chronicle in a minute
- Security Command Center introduction: Cloud posture and workload protection with Security Command Center

[PODCASTS]

- The Magic of Cloud Migration: Learn Security Lessons from the Field

Make sure to…

Enjoy the journey as much as the destination!