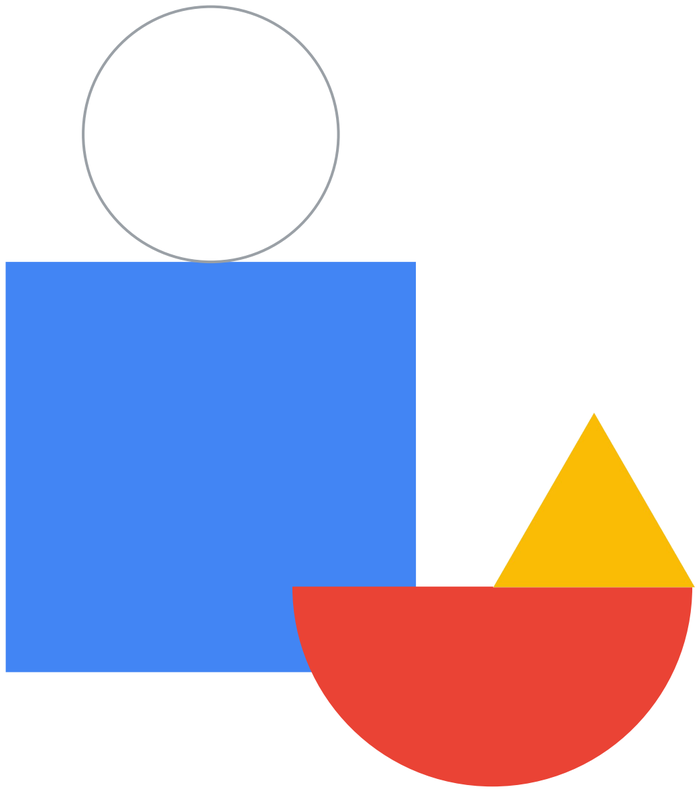
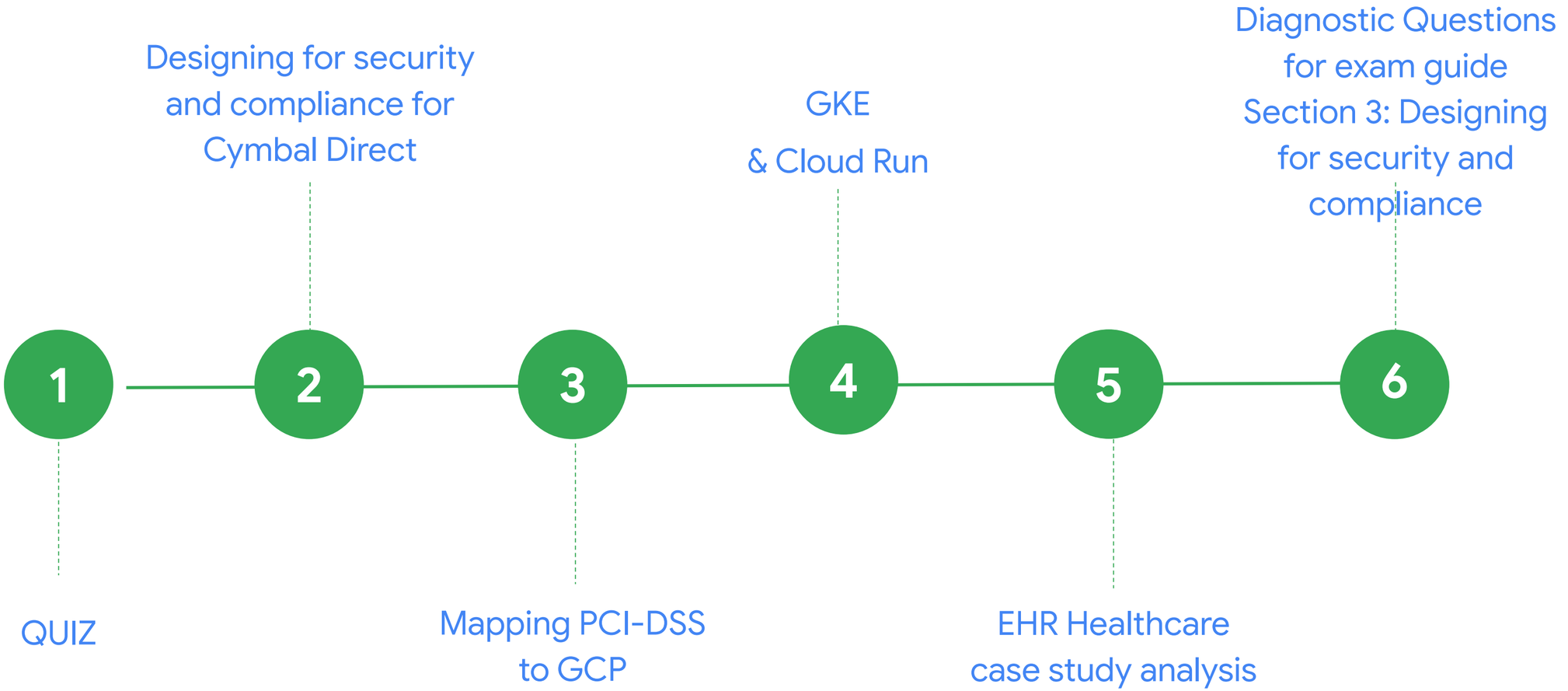
Google Cloud



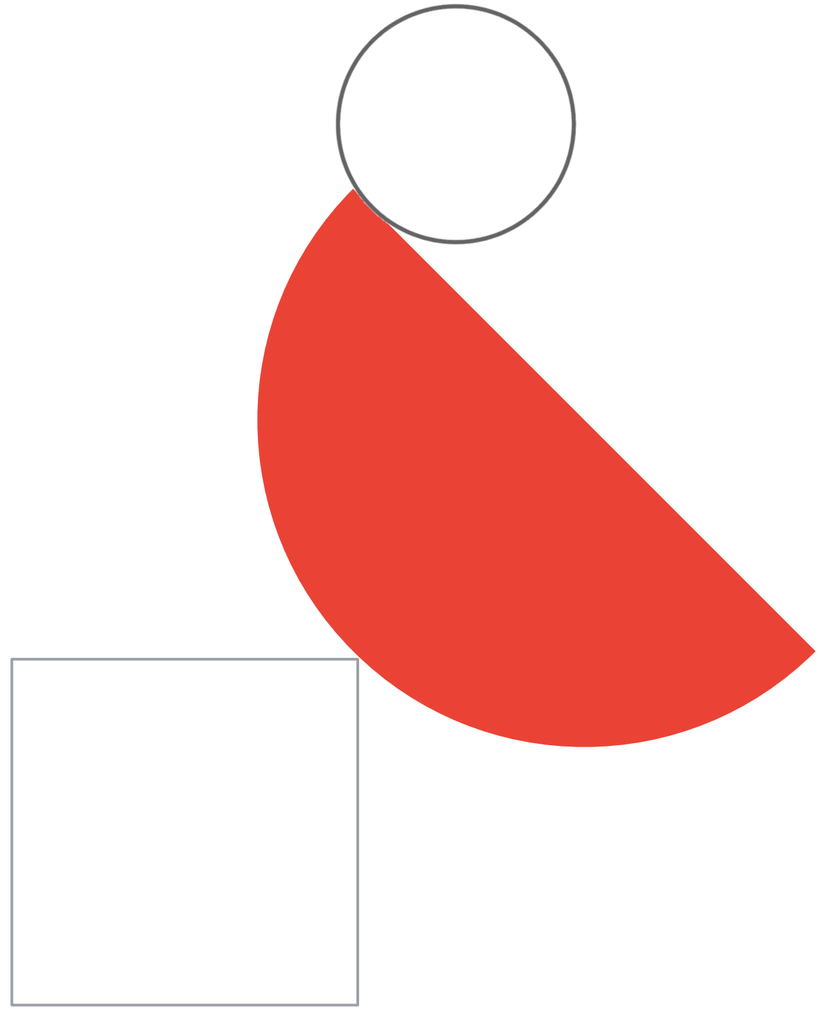
Preparing for Your Professional Cloud Architect Journey

Module 3: Designing for Security and Compliance

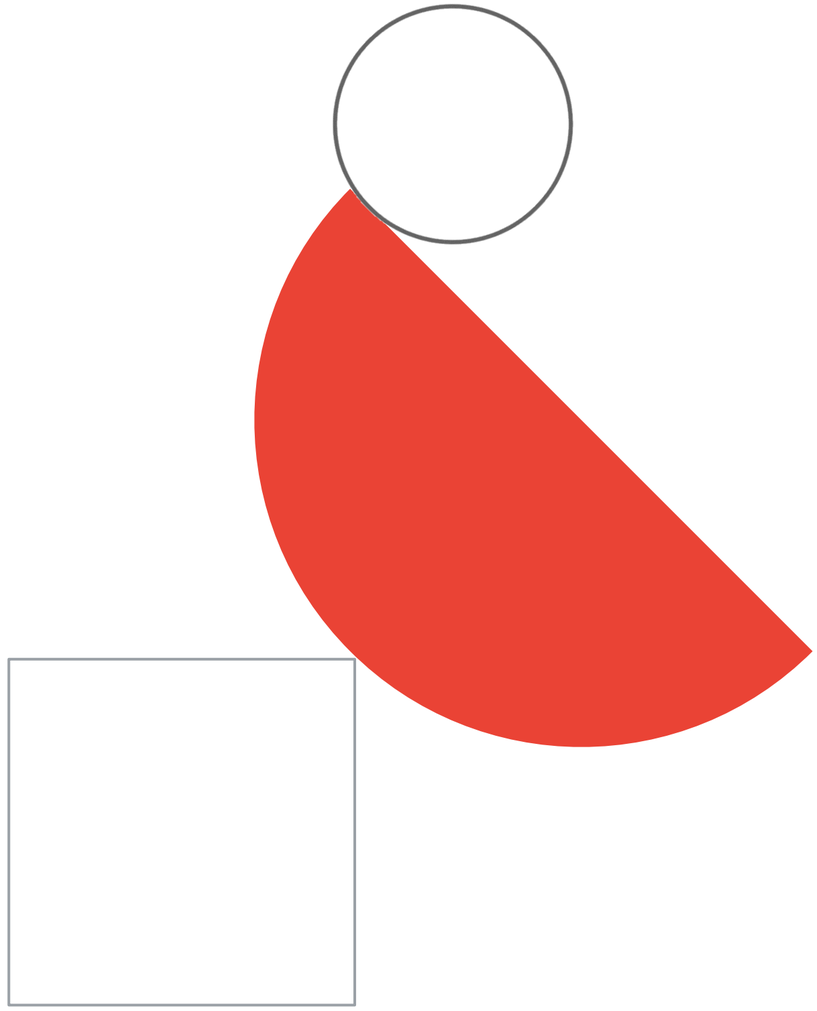
Week 4 agenda



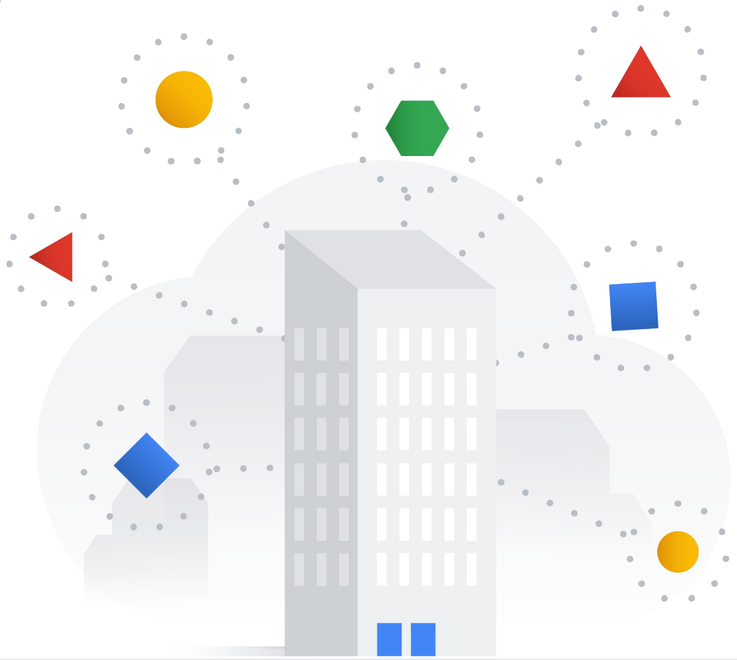
QUIZ time!



Designing for security and compliance for Cymbal Direct



Your role in architecting a secure and compliant cloud solution



- Designing for security
- Designing for compliance

Cymbal Direct

Compliance in GCP - 1/2

- ISO 27001
  - Requirements for an information security management system (ISMS), specifies a set of best practices
  - ONLY GUIDANCE, lays out allow Google to ensure a comprehensive and continually improving model for security management.
- SOC 2
  - The purpose of this report is to evaluate an organization's information systems relevant to security, availability, processing integrity, confidentiality, and privacy.
  - Relevant are different services: VPC Service Controls, DLP, Cloud Security Command Center, Cloud Armor etc
- PCI DSS
  - Appropriate practices that merchants and service providers should follow to protect cardholder data.
  - Relevant are MANY GCP services: networking, logging, encryption etc
- FIPS 140-2
  - A security standard that sets forth requirements for cryptographic modules, including hardware, software, and/or firmware, for U.S. federal agencies.
  - Google Cloud Platform uses a FIPS 140-2 validated encryption module called BoringCrypto (certificate 3318) in our production environment. This means that both data in transit to the customer and between data centers, and data at rest are encrypted using FIPS 140-2 validated encryption.

Compliance in GCP - 2/2

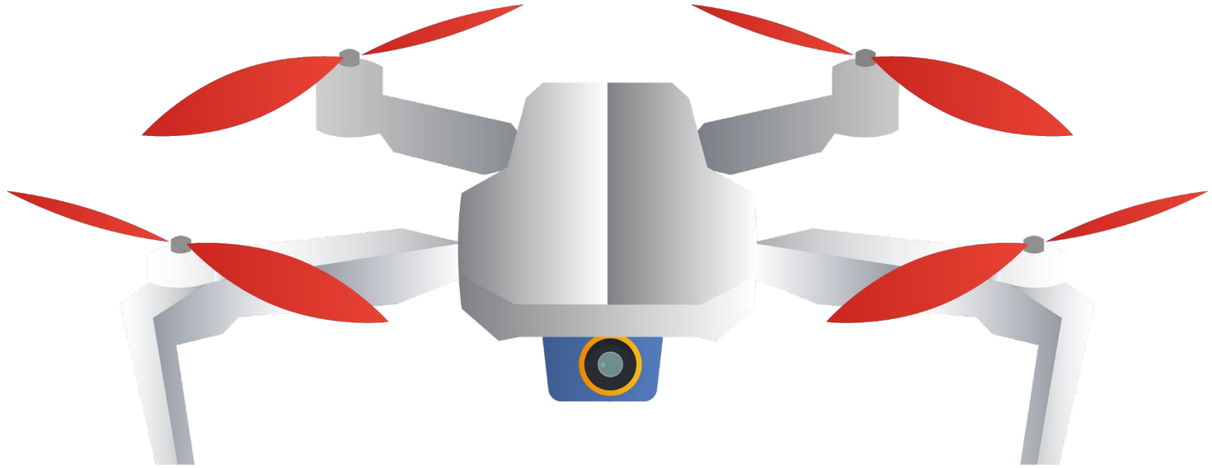
- HIPAA
  - Healthcare-related.
  - Complying with HIPAA is a shared responsibility between the customer and Google.
  - Google Cloud Platform supports HIPAA compliance (within the scope of a Business Associate Agreement) but ultimately customers are responsible for evaluating their own HIPAA compliance.
- FedRAMP
  - Government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
  - Risk impact levels (Low, Moderate, or High)
  - Google is one of the first hyperscale commercial cloud providers to achieve FedRAMP High on a commercial public cloud offering, and is one of the largest providers of FedRAMP services available on the market today.
  - NO SEPARATE 'GOVERNMENT' REGIONS EXIST IN GCP.
- GDPR
  - PII data protection in Europe.
  - Our customers own their data and we believe they should have the strongest levels of control over data stored in the cloud. Our public cloud provides customers with world-class levels of visibility and control over their data through our services.
  - Storing data in Europe, optionally manage encryption keys and store them outside of GCP, External Key Manager etc.

Security / compliance - related GCP services & features

Google Security Overview	Shielded VMs	Identity and Access Management
Access Transparency	Confidential Computing	IAM Conditions
GCP Compliance offerings	Shared VPC	Identity-Aware Proxy
Binary Authorization	VPC Service Controls	Resource Manager
Data Loss Prevention	Cloud Armor	Private Service Connect
Key Management Service	DNSSEC	Private Google Access
Organization Policy Service	Cloud VPN	Serverless VPC Access
Anthos Service Mesh	VPC Flow Logs	Web Security Scanner
Cloud Asset Inventory	Firewall Insights	Cloud Audit Logs
OS Login	Packet Mirroring	Centralized Telemetry

and more...

Considering potential compliance issues for Cymbal Direct

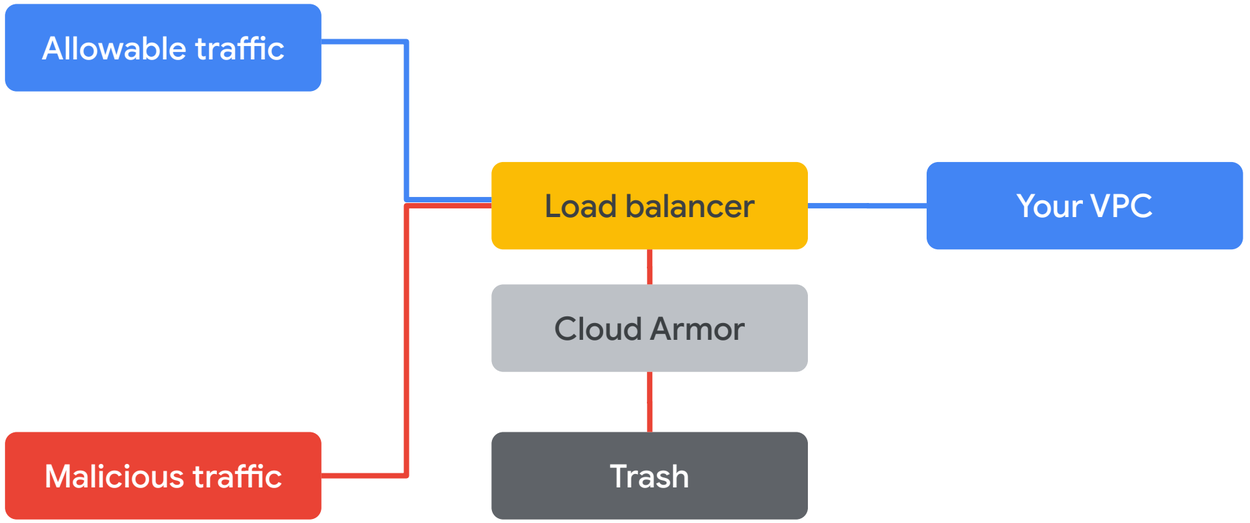


What happens if...

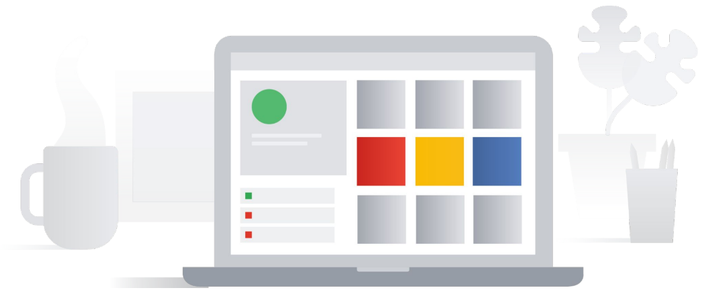
- A drone records video of PII?
- Inappropriate social media content is imported?

Security is woven into everything

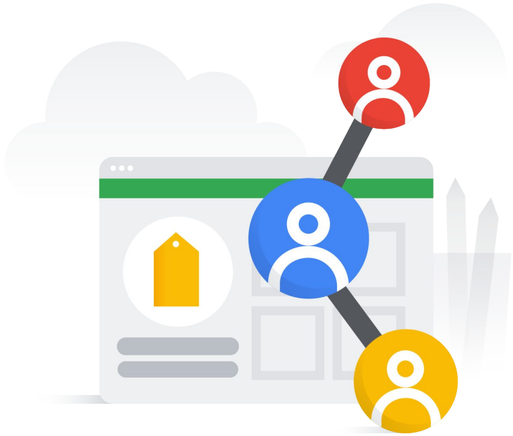
- Projects aren’t just for security
- Virtually all services and tools in Google Cloud have security options



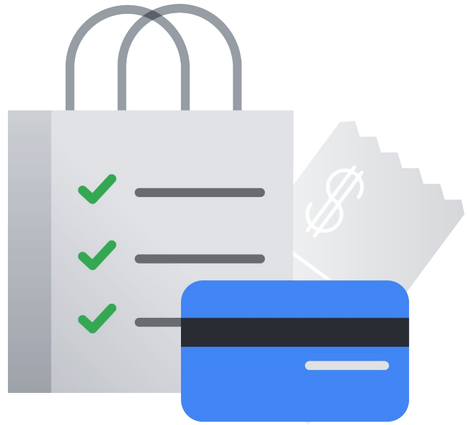
Compliance



Drones &
Social Media

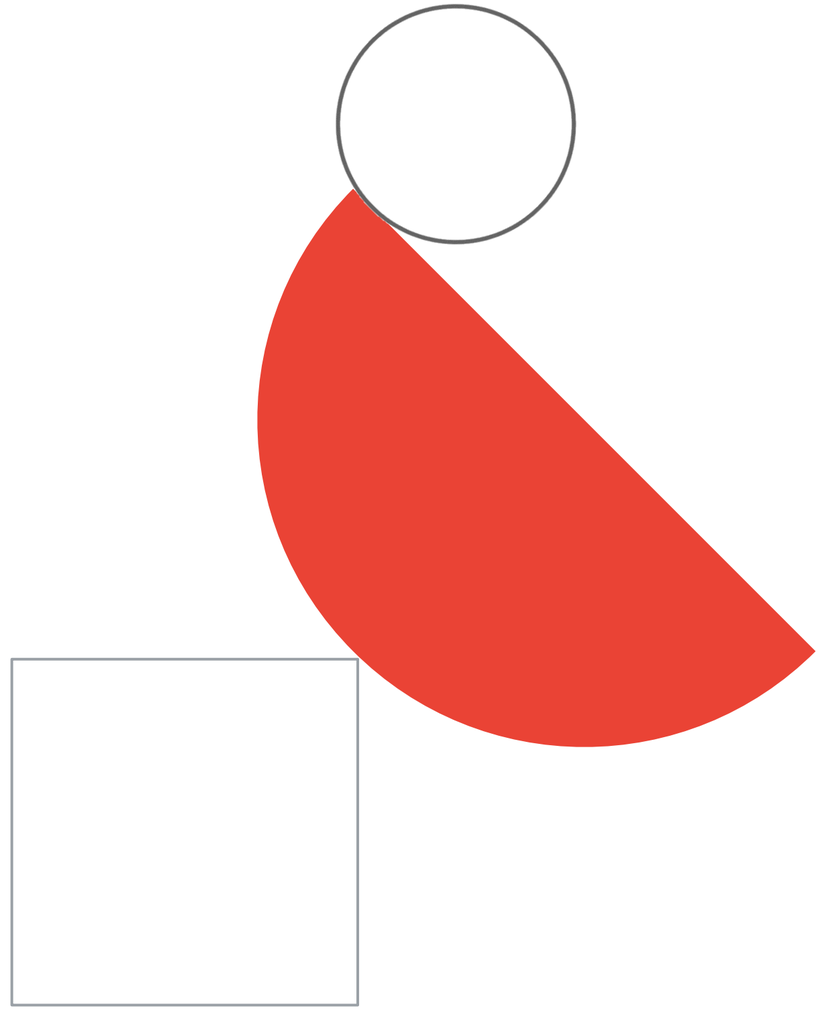


Retention



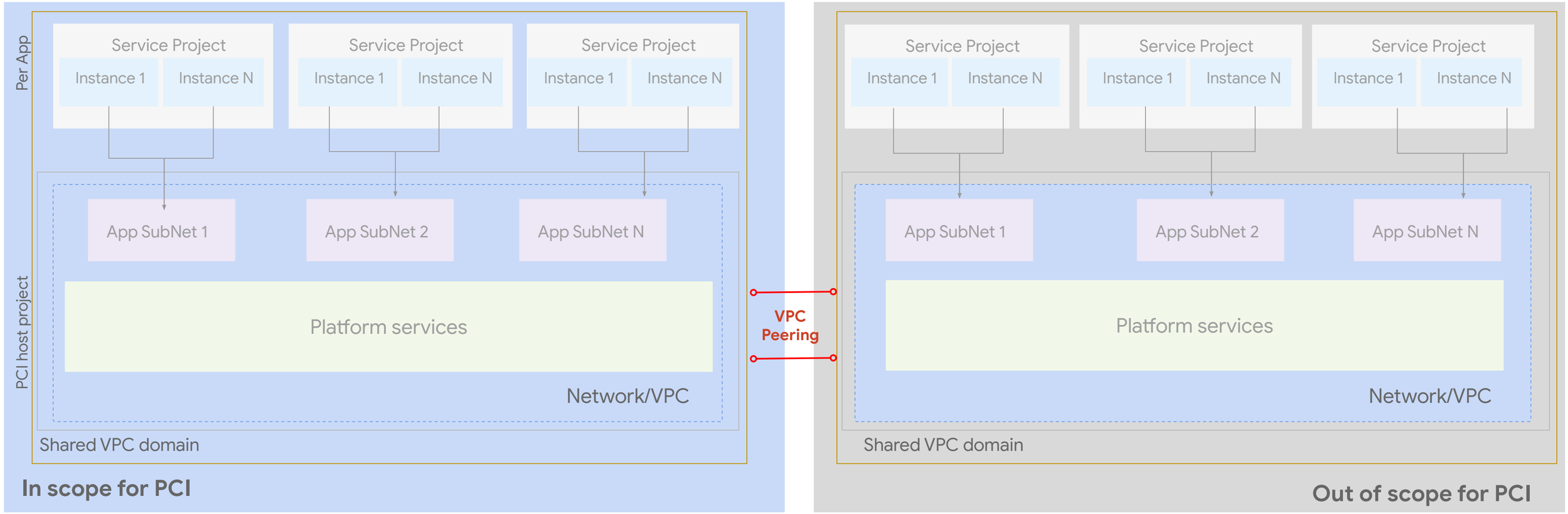
Credit
Cards

Mapping PCI-DSS requirements to GCP



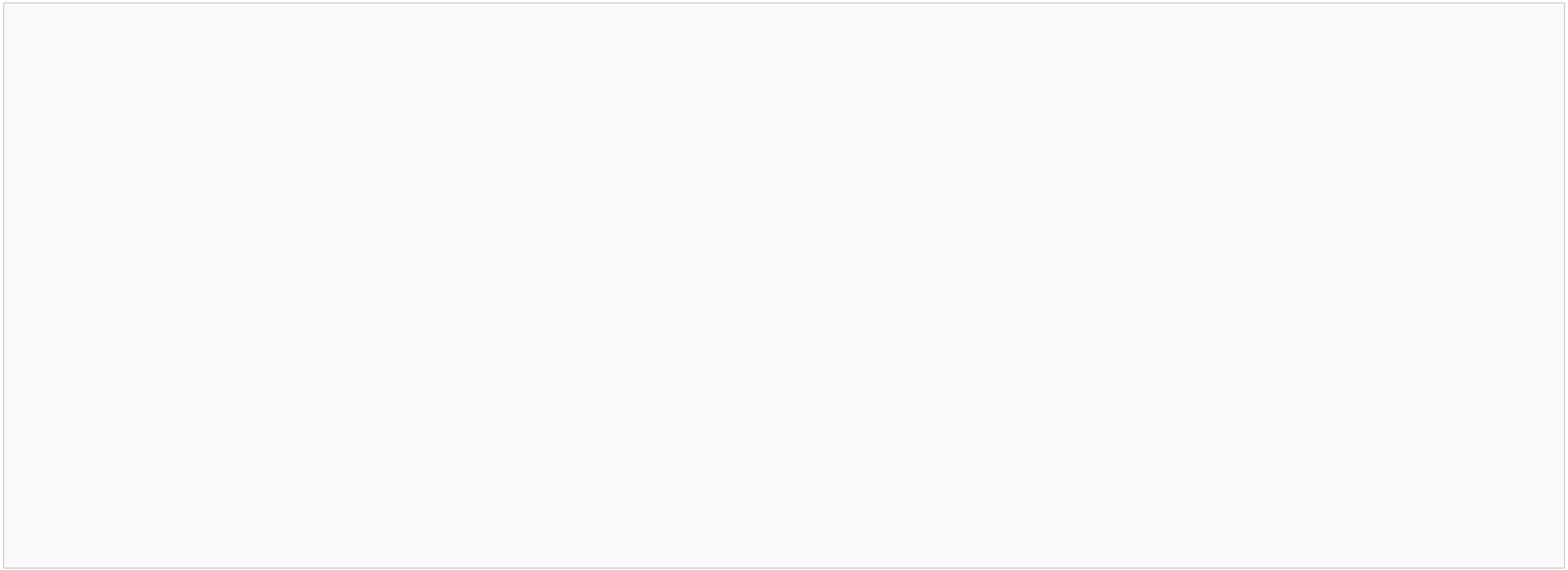
Requirement 1

Install and maintain a firewall configuration to protect cardholder data



Architecture - Using Shared VPC, host, and service projects to reduce scope of PCI environment through segmentation of networks. VPC network peering makes services available across VPC networks in private RFC 1918 space using Firewall access control lists.

Requirement 2 | Do not use vendor-supplied defaults



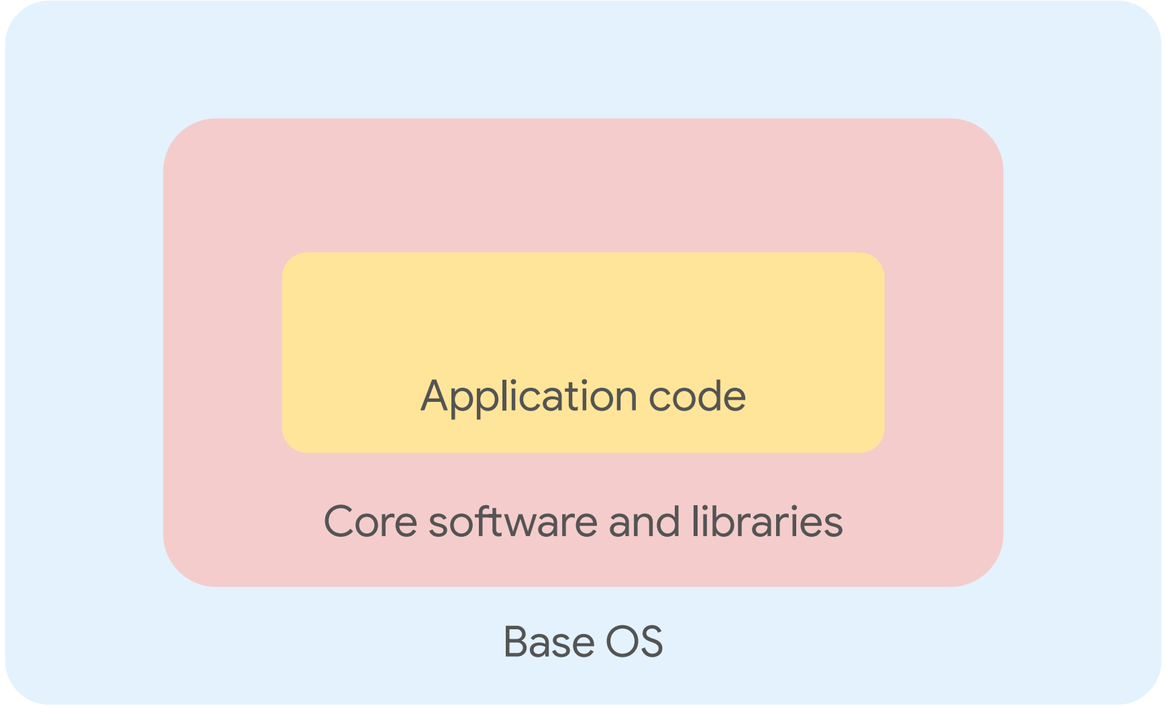
Requirement 2 | Do not use vendor-supplied defaults

Image baking

Base image - OS or hardened image from CIS with unnecessary packages removed

Core - packages and libraries needed for all instances (security, monitoring, language specific packages)

Application - application code



Requirement 3 | Protect stored cardholder data

Requirement 3 | Protect stored cardholder data

Enjoy world class encryption without further need for configurations
By default

Keep keys in the cloud, for direct use by cloud services
Generally available

Keep keys on-premises, and use them to encrypt your cloud services
Available for Cloud Storage and Compute Engine

More Simple

Encryption by default (only in GCP)

Cloud key management service

Customer-supplied encryption keys

More control

Requirement 3 | Protect stored cardholder data (cont.)

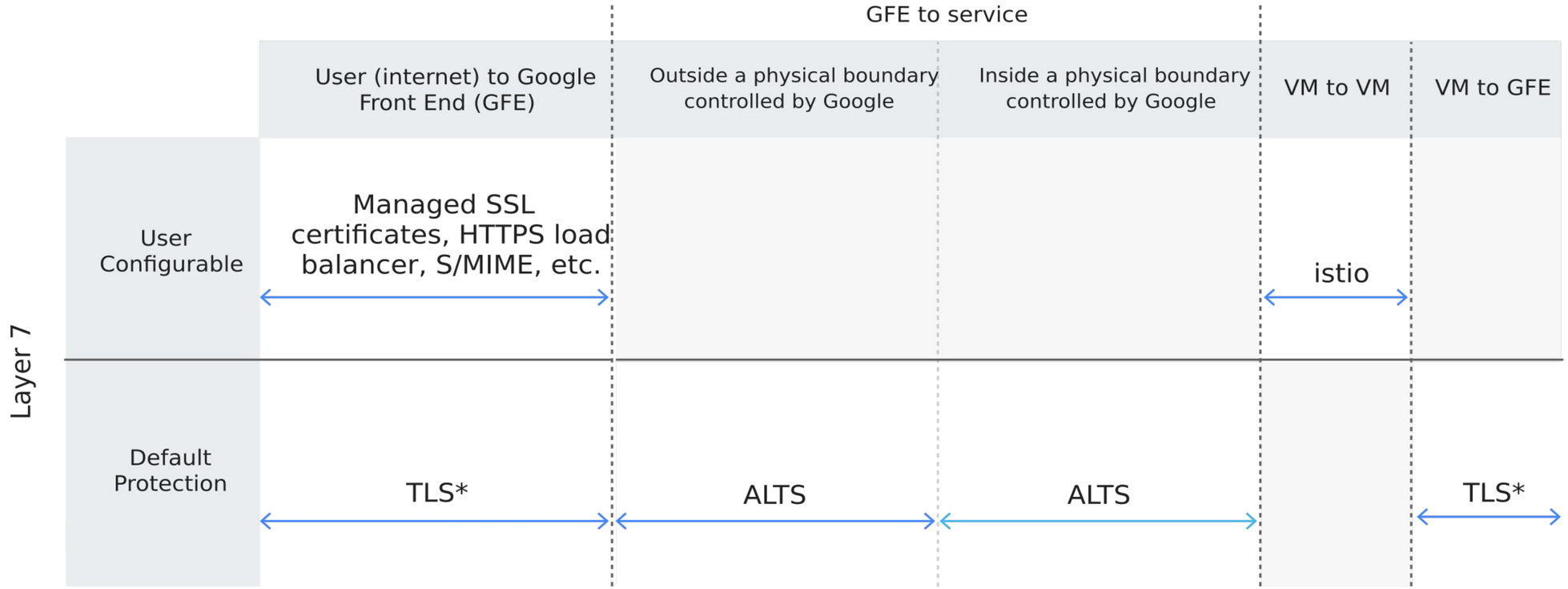
Data Loss Prevention API can be used to sanitize PCI data

Requirement 4

Encrypt transmission of cardholder data across open, public networks

Requirement 4

Encrypt transmission of cardholder data across open, public networks



→ Authentication only → Authentication and integrity → Authentication and integrity and encryption

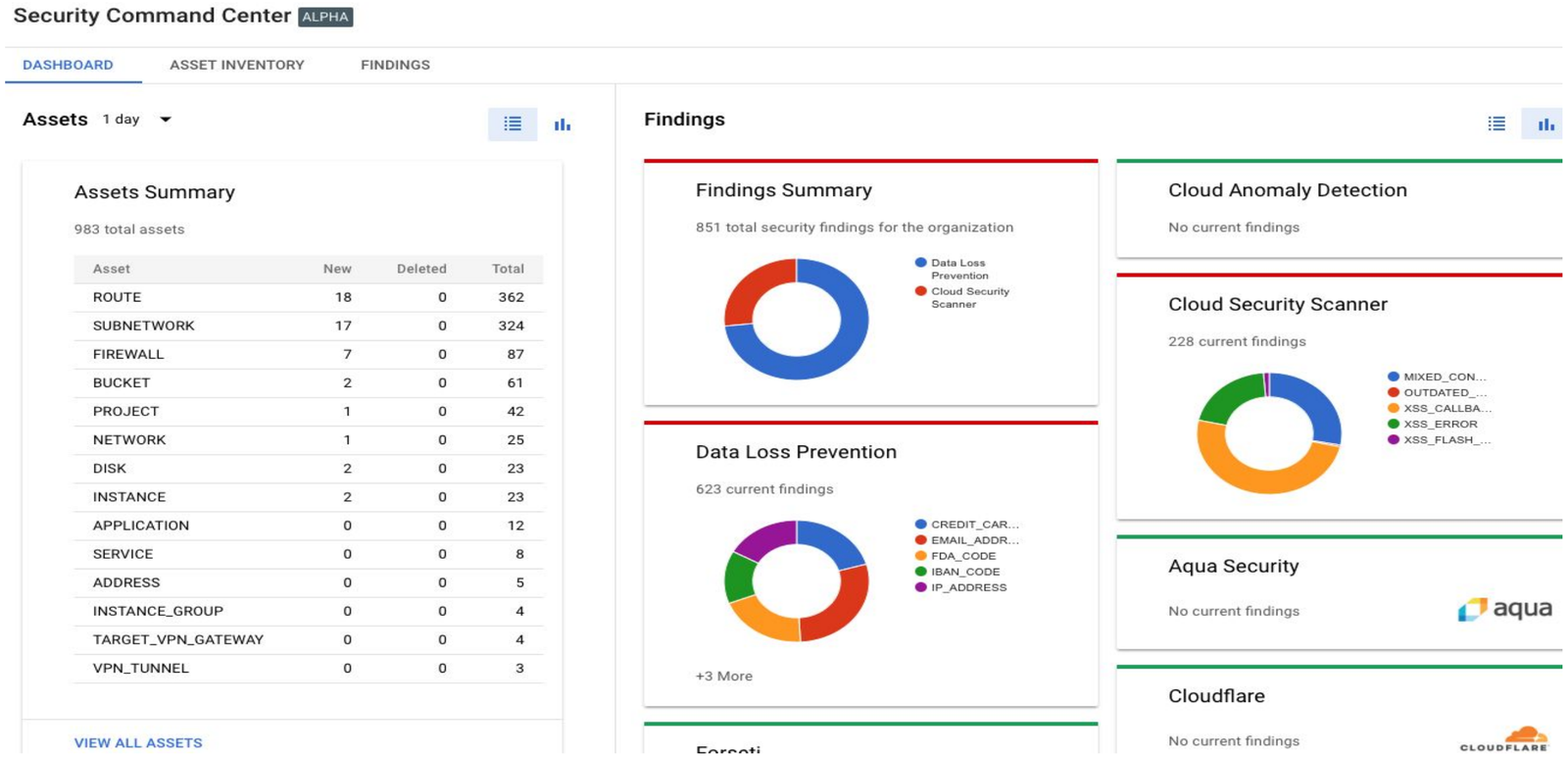
* TLS is by default for Google Cloud services. For a customer application hosted on Google Cloud, this is something that needs to be configured by the customer.

Requirement 5

Protect all systems against malware and regularly update anti-virus software or programs

Requirement 5

Protect all systems against malware and regularly update anti-virus software or programs



Cloud Security Command Center can help gather security information, identify threats, and take action.

Requirement 6

Restrict access to cardholder data by business need to know

Requirement 6 | Restrict access to cardholder data by business need to know

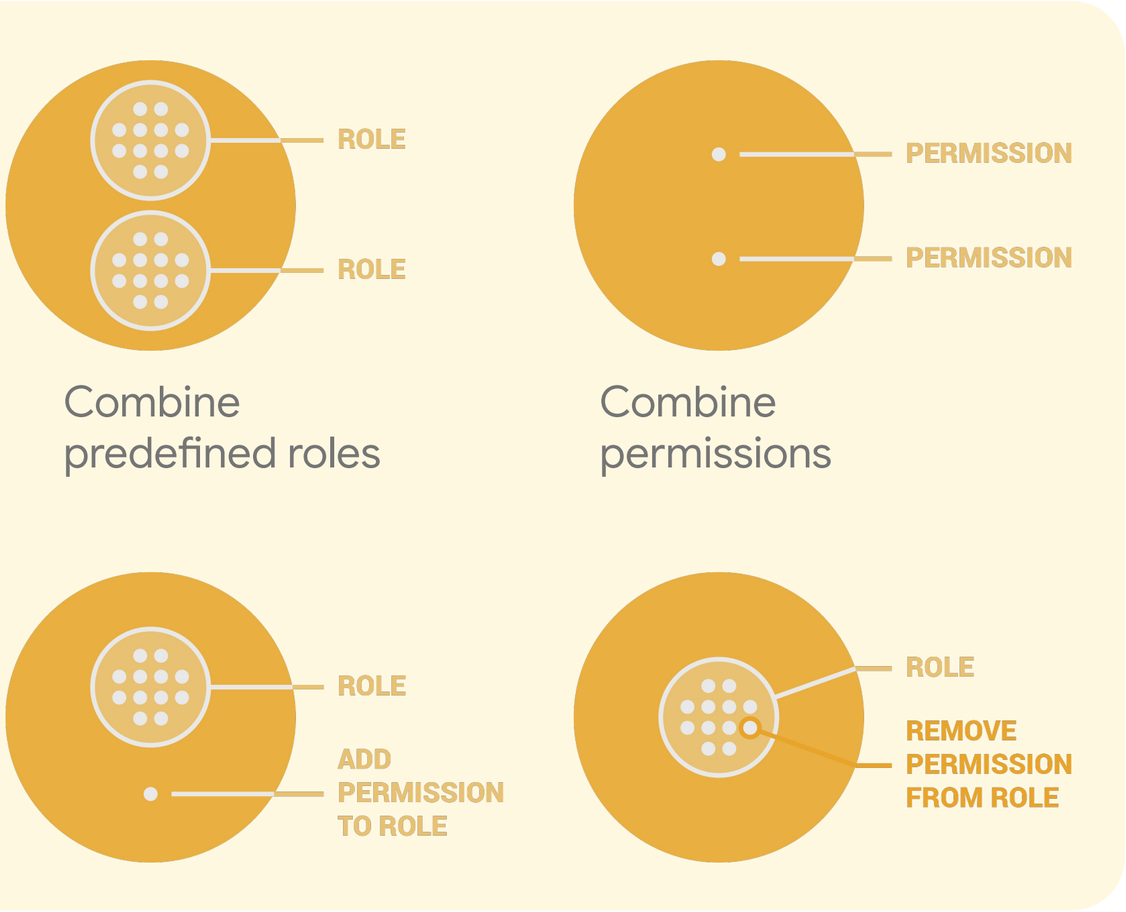
Once access needs for each job function are defined, **custom roles** can be created provide granular control over the exact permissions to access system components and data resources

- Create groups based on job functions, and assign custom roles to those groups.
- Job function groups can be nested in job classification groups.
- Custom roles can be defined at the organizational level

Review available permissions and their purpose through the API Explorer (search for product)

Services > App Engine Admin API v1

appengine.apps.authorizedCertificates.create	Uploads the specified SSL certificate.
appengine.apps.authorizedCertificates.delete	Deletes the specified SSL certificate.
appengine.apps.authorizedCertificates.get	Gets the specified SSL certificate.
appengine.apps.authorizedCertificates.list	Lists all SSL certificates the user is authorized to administer.



Requirement 7

Track and monitor all access to network resources and cardholder data

Requirement 7

Track and monitor all access to network resources and cardholder data

Admin console logs

- Admin console audits
- User audits
- Separate API and UI
- Export to BigQuery

Cloud audit logs

- Admin activity logs (always enabled)
- Data access logs (disabled by default)

Stackdriver logging agent

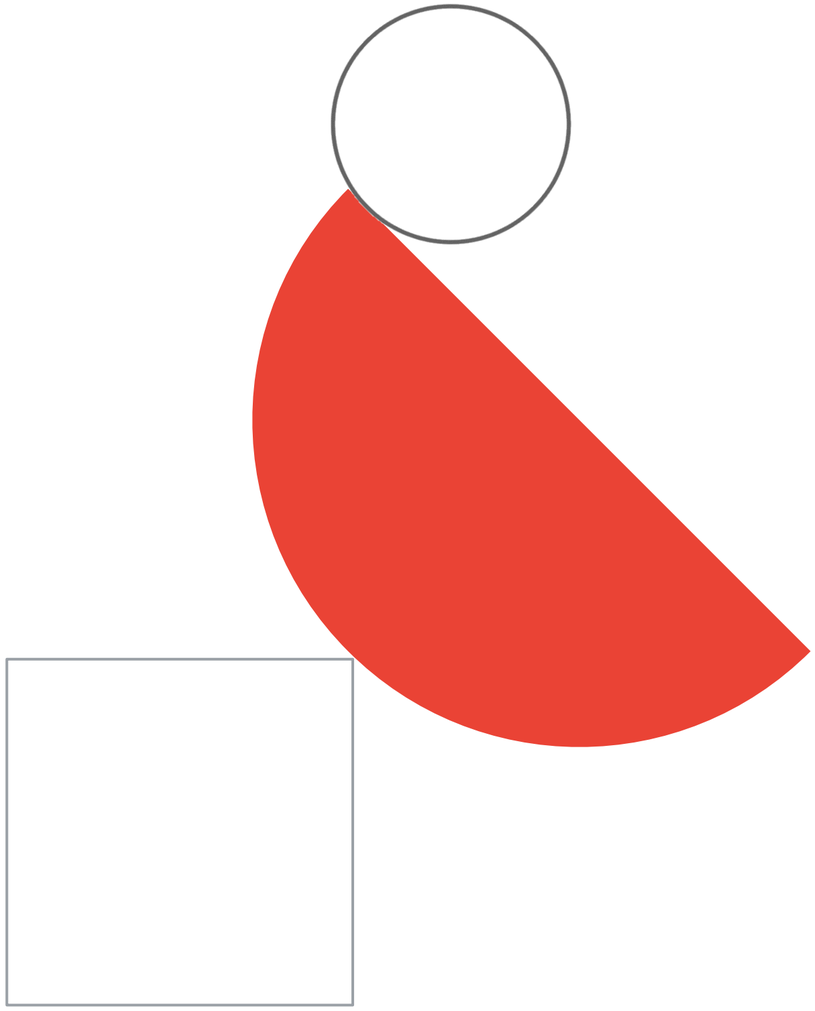
- FluentD agent
- Common third-party applications
- System software

Network logs

- VPC flow
- CDN (Alpha)
- HTTP(S) load balancing (Alpha)
- Firewall rules logging

Google Kubernetes Engine (GKE)

Exam Tip: I can't stress enough how important it is to understand Kubernetes concepts. Commit at least few hours for learning GKE - especially if you're not familiar with this technology. Slides below will give you a high level overview, but you should be much more familiar with this topic to feel comfortable during the exam.



GKE: Autopilot Mode

GKE manages underlying infrastructure of the cluster, including the nodes

High availability

Regional cluster; Regular Release Channel; Auto-Update; Auto-Repair; Surge Upgrade;

Network

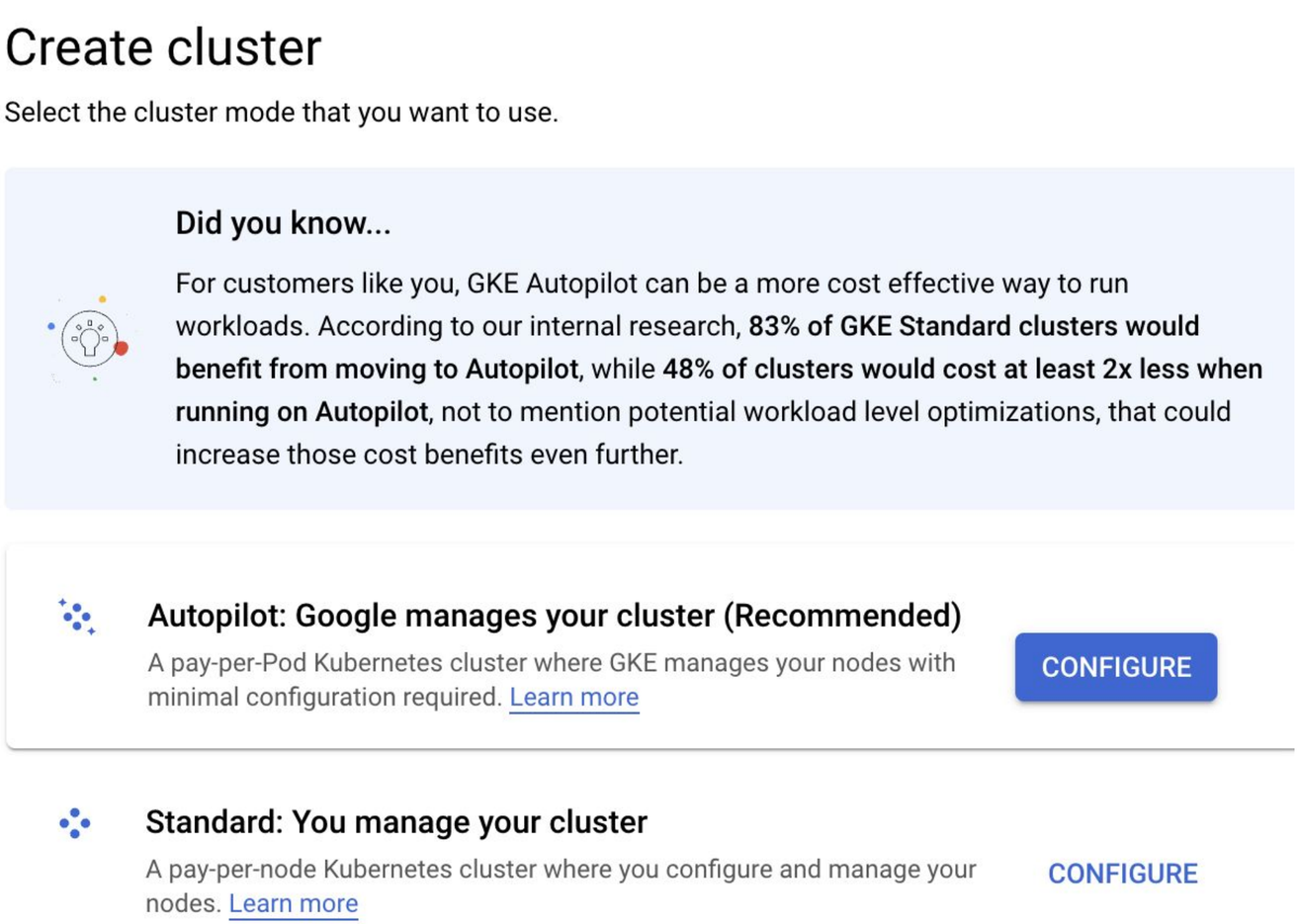
VPC Native (alias IP); IP-friendly (limit cluster size/ pods per node); full network flexibility

Highly Scalable

Node Auto Provision; Horizontal Pod Autoscaler; Vertical Pod Autoscaler

Secured by default

Workload Identity; Shielded Nodes; Secure-boot-disk; COS and Containerd, block known unsecure features.



Pod Disruption Budget, Readiness and Liveness Probes

A **PDB (Pod Disruption Budget)** limits the number of pods of a replicated application that can be taken down **simultaneously** from **voluntary** disruptions.

An Application Owner can create a **PodDisruptionBudget** object (PDB) for each application.

Readiness probes: designed to know when your app is ready to serve traffic.

Liveness probes: designed to let Kubernetes know if your app is alive or dead.

```
kind: PodDisruptionBudget
metadata:
 name: km-pdb
spec:
 minAvailable: 2
 selector:
   matchLabels:
     app: kobimysql
```

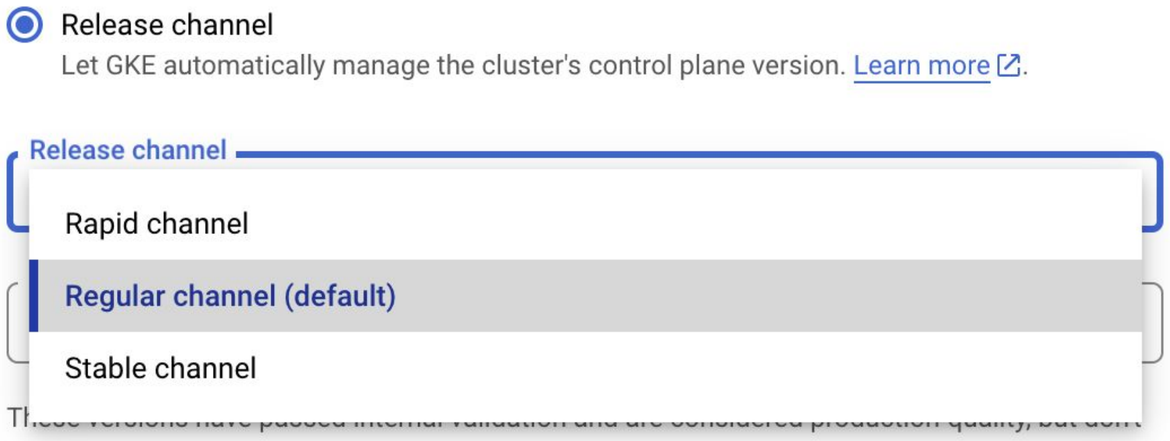
```
maxUnavailable: 1
```

Exam Tip:

- *See how to ensure stateful workloads are disruption-ready*
- *Great explanation of Readiness and Liveness probes here.*

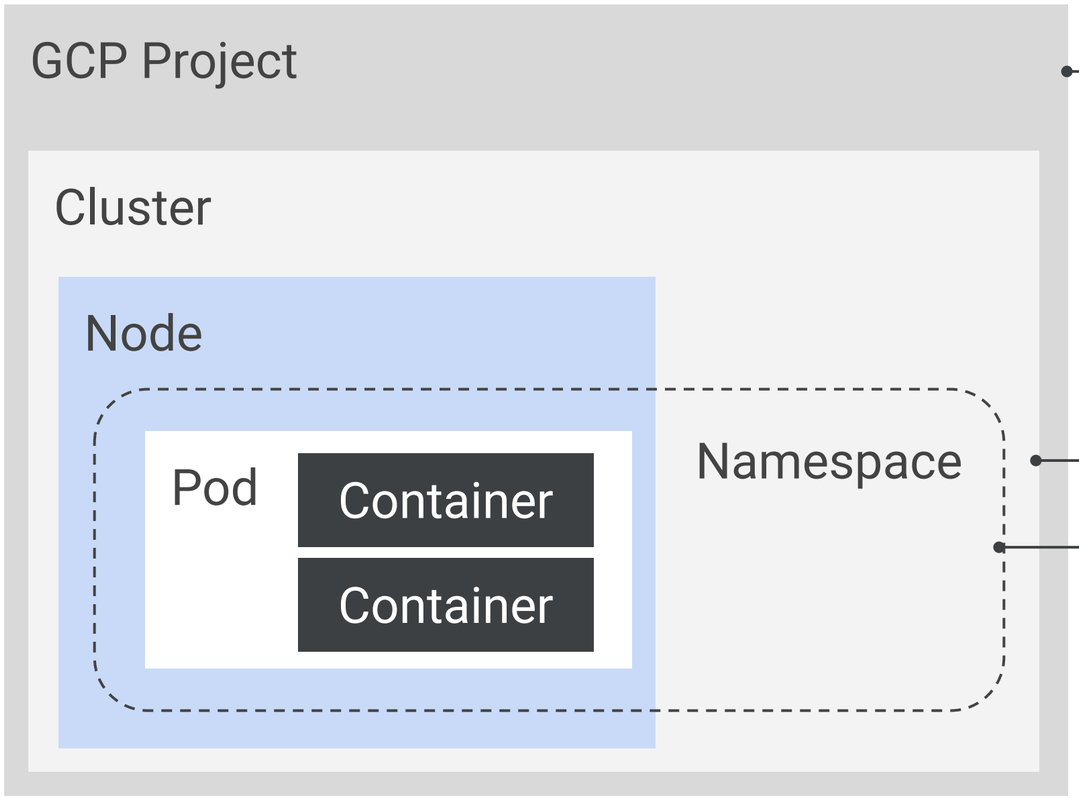
Best practices for GKE upgrades

1. **Setup multiple environments:** at a minimum pre-production and production clusters
2. **Enroll Clusters in Release Channels**: Stable or Regular release channels for production clusters.



3. **Create continuous upgrade strategy**: Receive updates about new GKE versions through cluster upgrade notifications through Pub/Sub
4. **Schedule maintenance windows and exclusions**: to increase upgrade predictability
5. **Set tolerance for disruption**: To ensure that pods sufficient number of replicas, use Pod Disruption Budget

GKE: Using IAM and RBAC



Use IAM at the project level
Set roles for

- Cluster Admin: manage clusters
- Container Developer: API access within clusters

Use RBAC at the cluster and namespace level
Set permissions on individual clusters and namespaces

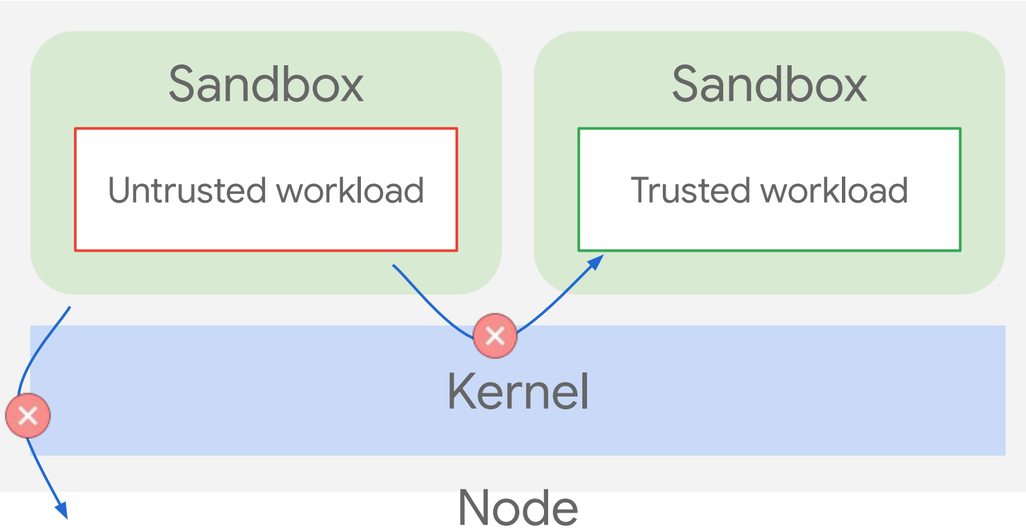
Exam Tip: *IAM and Kubernetes RBAC work together to help manage access to your cluster. RBAC controls access on a cluster and namespace level, while IAM works on the project level*

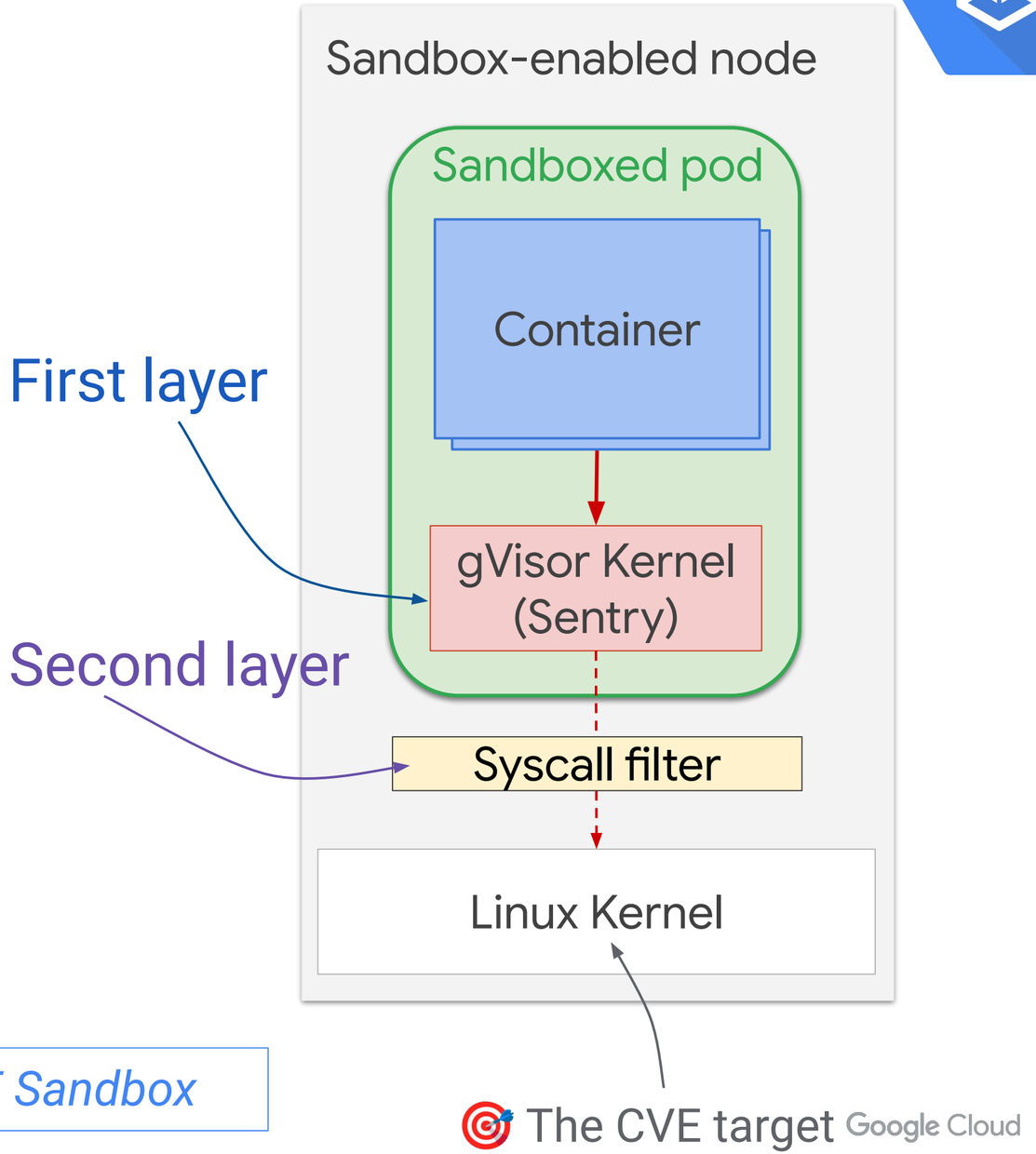
GKE Sandbox

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





***Exam Tip**: Commit 10 minutes to get an overview ofGKE Sandbox*

GKE networking: Subnet sizes

Subnet size for nodes	Maximum nodes	Maximum Pod IP addresses needed	Recommended Pod address range
/29	4	1,024	/21
/28	12	3,072	/20
/27	28	7,168	/19
/26	60	15,360	/18
/25	124	31,744	/17
/24	252	64,512	/16
/23	508	130,048	/15
/22	1,020	261,120	/14
/21	2,044	523,264	/13
/20	4,092	1,047,552	/12
/19	8,188	2,096,128	/11 (maximum Pod address range)

***Exam Tip**: make sure to watch this video to understand GKE networking well!*

GKE networking: Example

Subnet size for nodes	Maximum nodes	Maximum Pod IP addresses needed	Recommended Pod address range
/29	4	1,024	/21

$2^{(32-29)} = 8$ (4 of these are reserved for GCP)

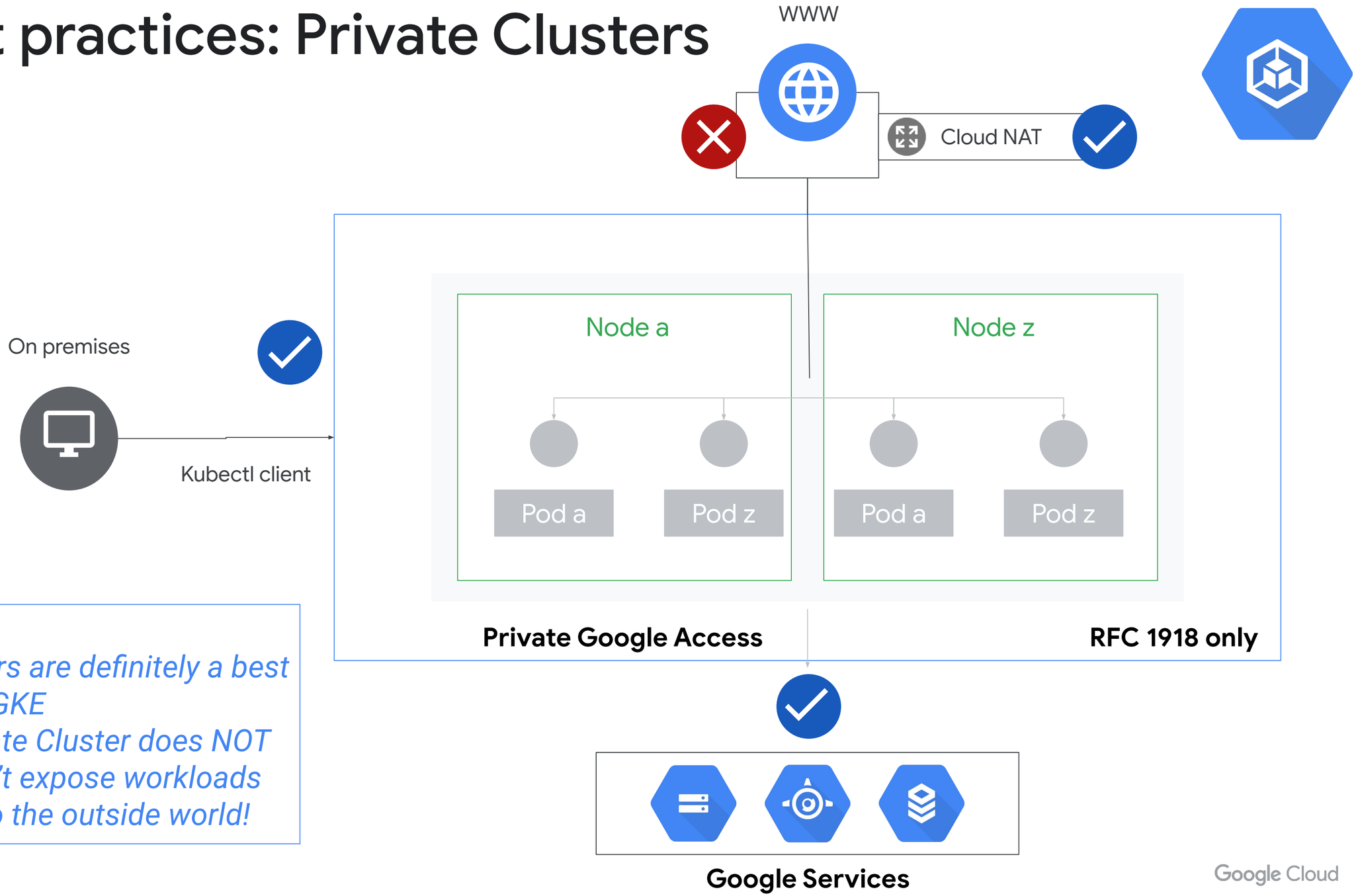
110 pods running in each node -> **4 * 110 = 440**

Twice number of IPs per pod **440 * 2 = 880**

2^{10} number of IPs for pods

*Assuming the default maximum of 110 pods per node

GKE best practices: Private Clusters



Exam Tip:

- *Private Clusters are definitely a best practice with GKE*
- *Having a Private Cluster does NOT mean you can't expose workloads via Services to the outside world!*

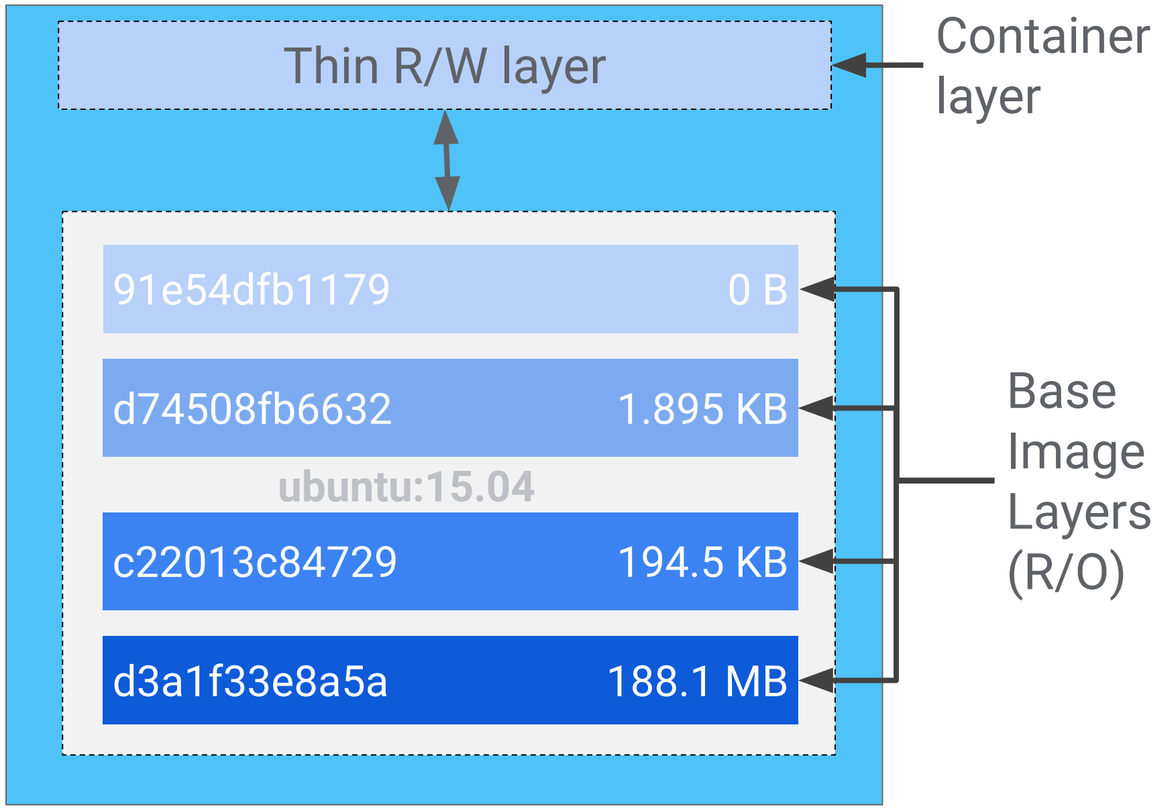
Container best practices: building images

Exam Tip: *Each instruction in a Dockerfile creates a layer.*

Dockerfile

```
FROM ubuntu:15.04
COPY . /app
RUN make /app
CMD python /app/app.py
```

Container



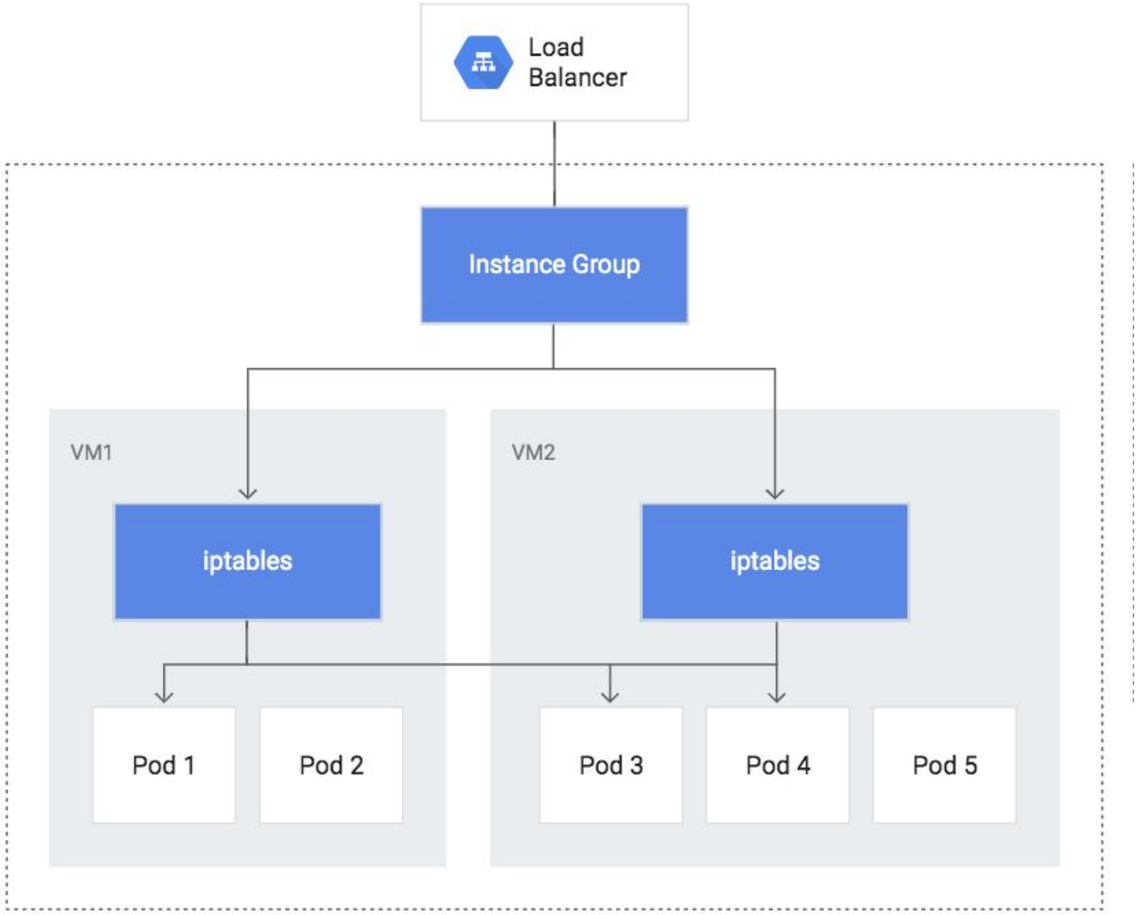
docker commands

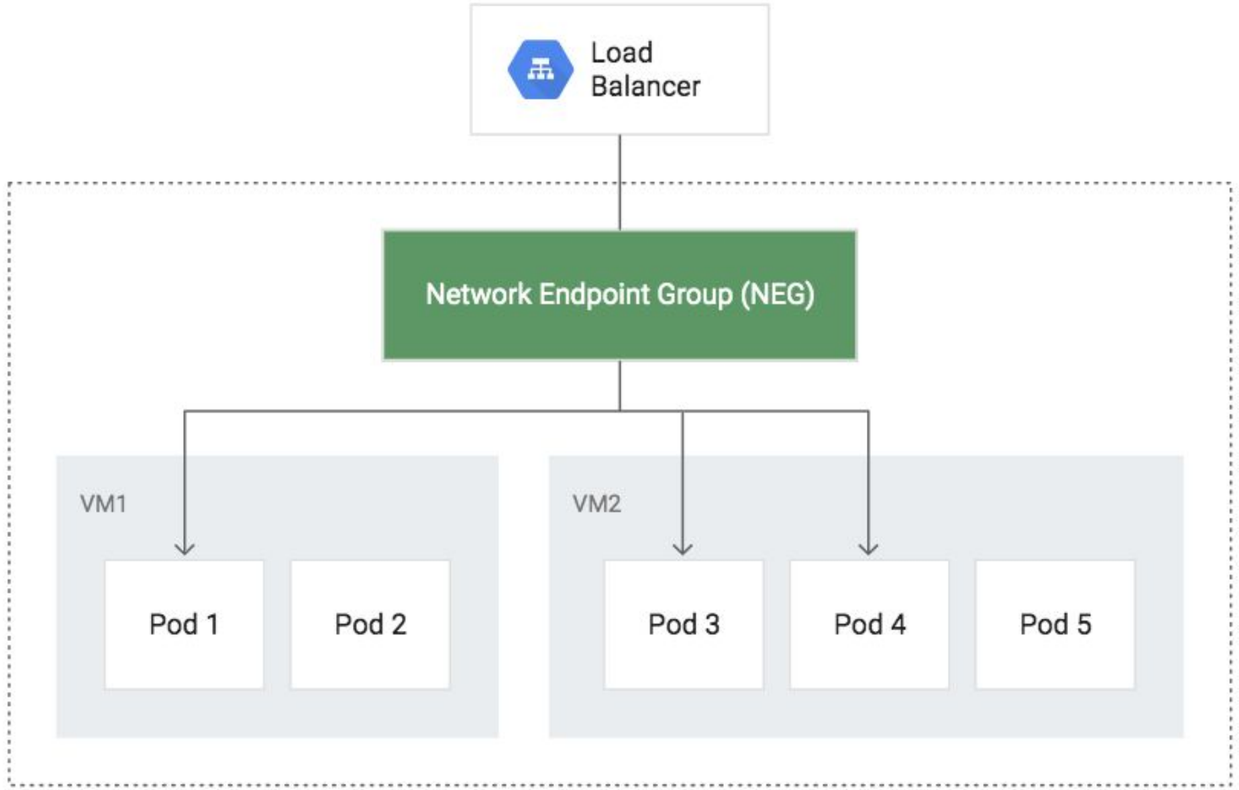
```
$> docker build -t py-web-server
.
$> docker run -d py-web-server
$> docker images
$> docker ps
$> docker logs <container id>
```

Exam Tips: *Here are best practices for building container images:*

- *Use the smallest base image possible (when new versions are rolled out, only smallest image layers are changed). Eg. use "alpine" image rather than "centos" or "ubuntu" if possible.*
- *Use multi-stage builds (app can be built in a first "build" container and the result can be used in another container)*
- *Try to create images with common layers (if a layer already exists on a cluster, it does not have to be downloaded)*

Ingress service: standard (non-NEG) vs NEG





Exam Tip: *NEG is often preferred as a container-native load balancing type.*

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

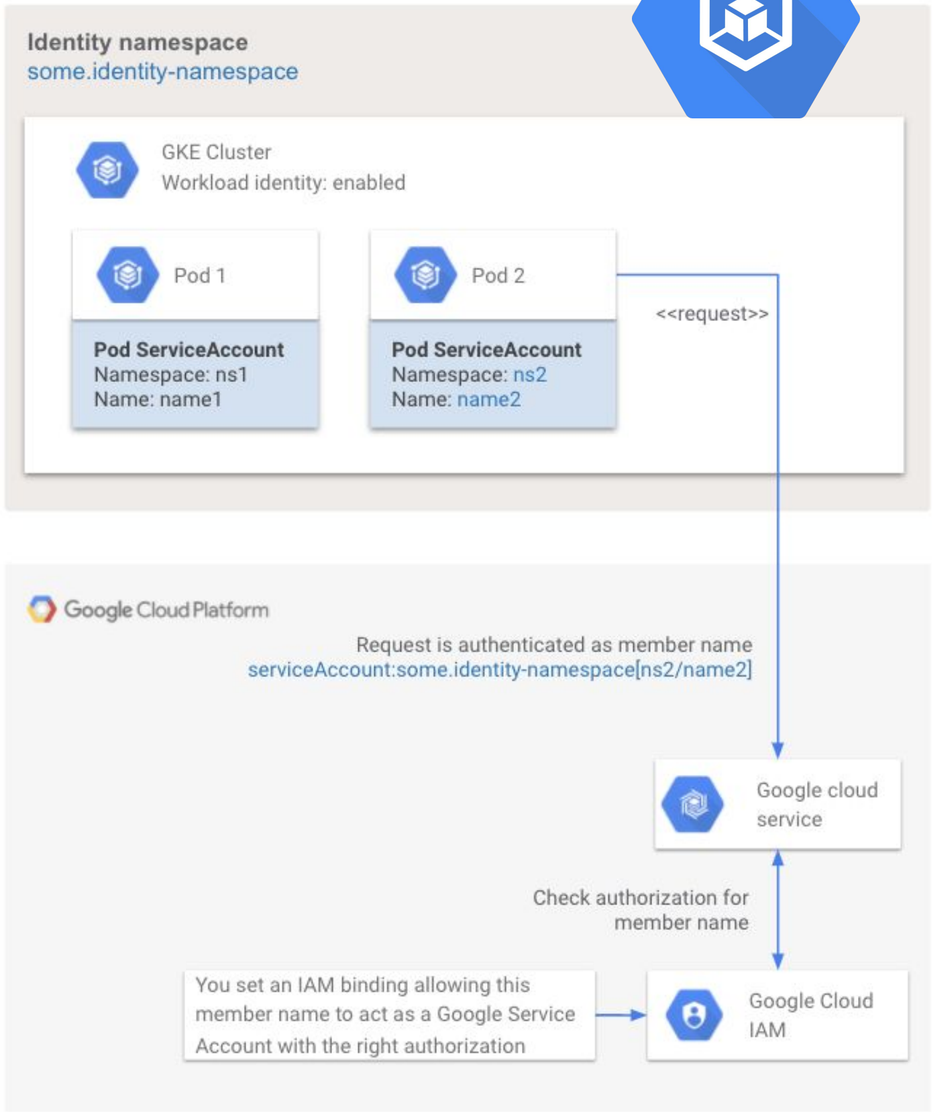
=> toilsome to setup & hard to secure

GKE API access from k8s *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

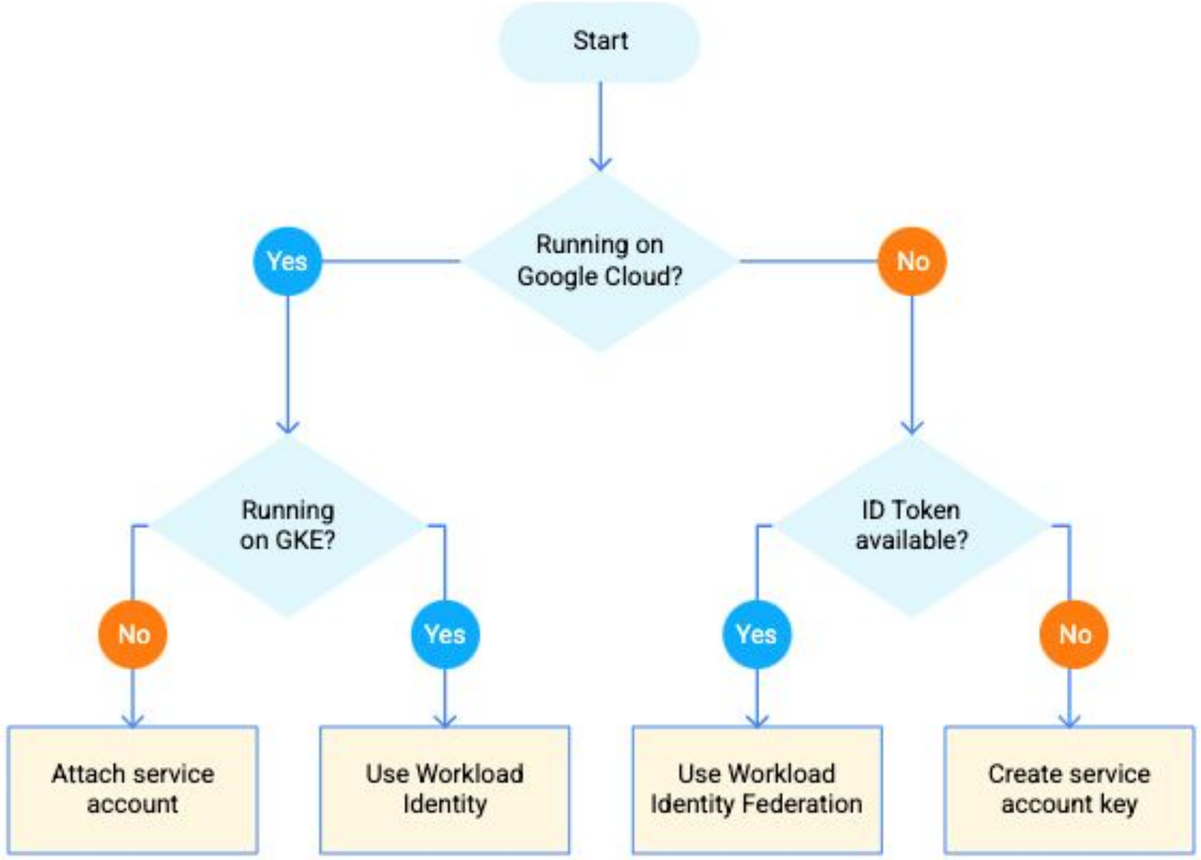
It just works!

Exam Tip: *Workload Identity is a best practice for a GKE which needs to access other GCP APIs.*



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.



How to bootstrap / change a GKE cluster

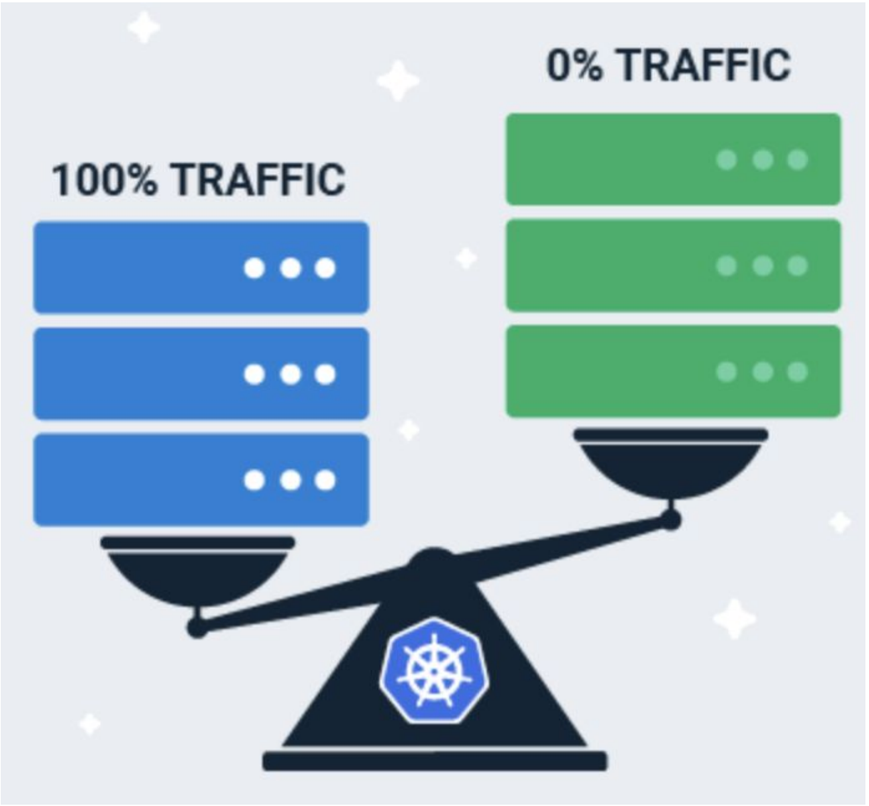
Exam Tips:

- *Make sure to differentiate:*
  - *When creating / modifying / deleting cluster (or its node pools), you should use gcloud command (since you're interacting with GCP to manage INFRASTRUCTURE for GKE). For example:*
    - *To create a cluster: 'gcloud container clusters create... '*
    - *To resize a cluster (change number of nodes): 'gcloud container clusters **resize** CLUSTER_NAME --node-pool POOL_NAME --num-nodes NUM_NODES'*
    - *To enable autoscaling on a node pool of existing cluster: 'gcloud container clusters **update** CLUSTER_NAME **--enable-autoscaling** --node-pool=POOL_NAME --min-nodes=MIN_NODES --max-nodes=MAX_NODES --region=COMPUTE_REGION'*
    - *To disable autoscaling on a node pool of existing cluster: 'gcloud container clusters update CLUSTER_NAME **--no-enable-autoscaling** --node-pool=POOL_NAME --region=COMPUTE_REGION'*
  - *When interacting with Kubernetes objects (eg. you'd like to deploy some Pods), you should use 'kubectl' command, eg:*
    - *To scale a deployment: 'kubectl autoscale deployment hello-app --cpu-percent=80 --min=1 --max=5'*

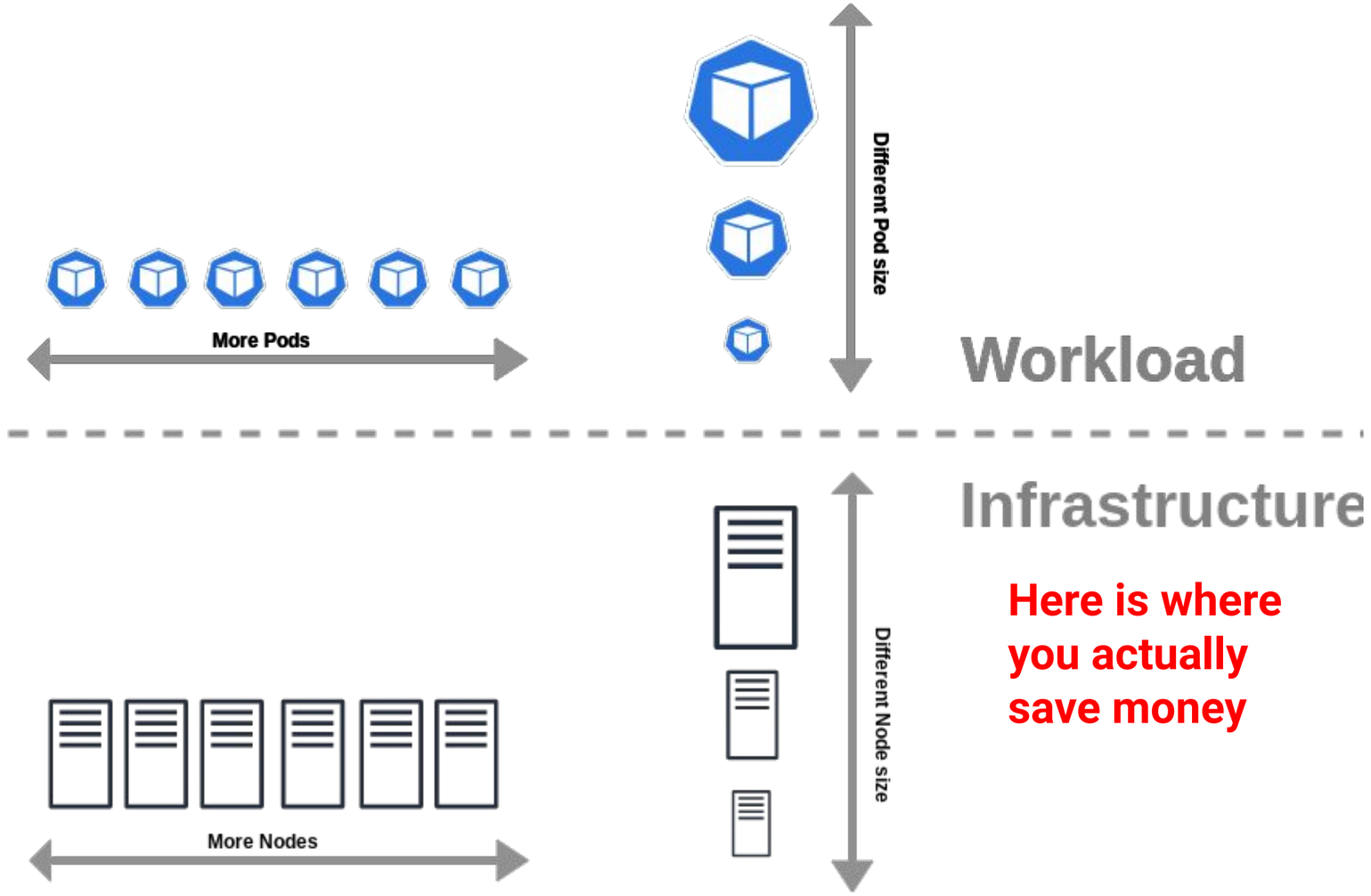
A/B testing, rolling updates, canary testing in GKE

Exam Tips:

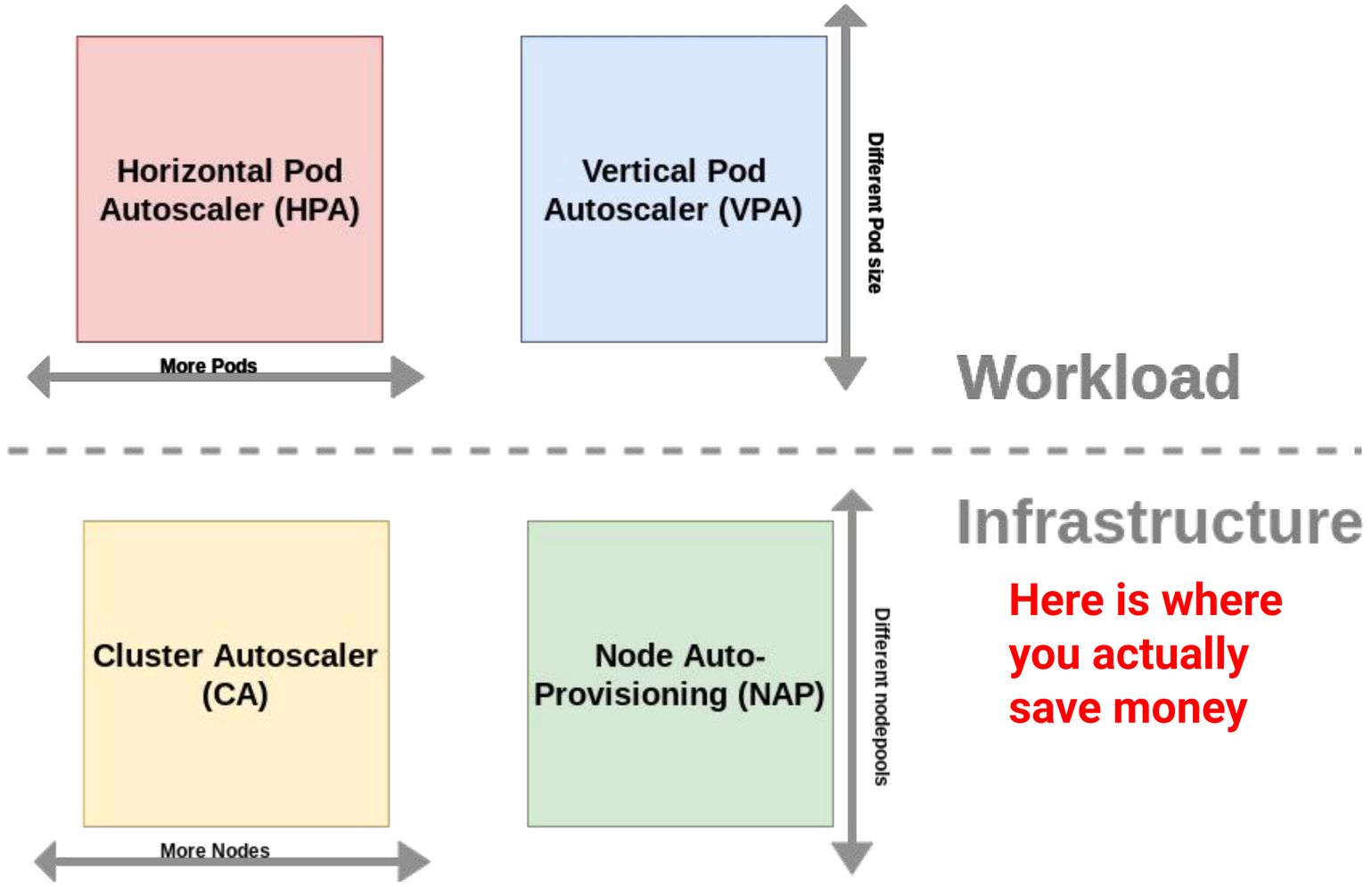
- *You should know what deployment options GKE offers and how each of them works on a high level. Here is a great resource to understand those concepts.*
- *Differentiate between deployment strategies and testing strategies.*
- *Be able to choose the right strategy under different circumstances, eg. minimal downtime, rollback duration etc.*
- *Deploying new version is important... but being able to quickly and reliably roll back to previous version is even more important!*
- *To start a rolling update of a new app in GKE:*
  - *kubectl set image deployment/hello-app hello-app=REGION-docker.pkg.dev/${PROJECT_ID}/hello-repo/hello-app:v2*



GKE: The 4 scalability dimensions

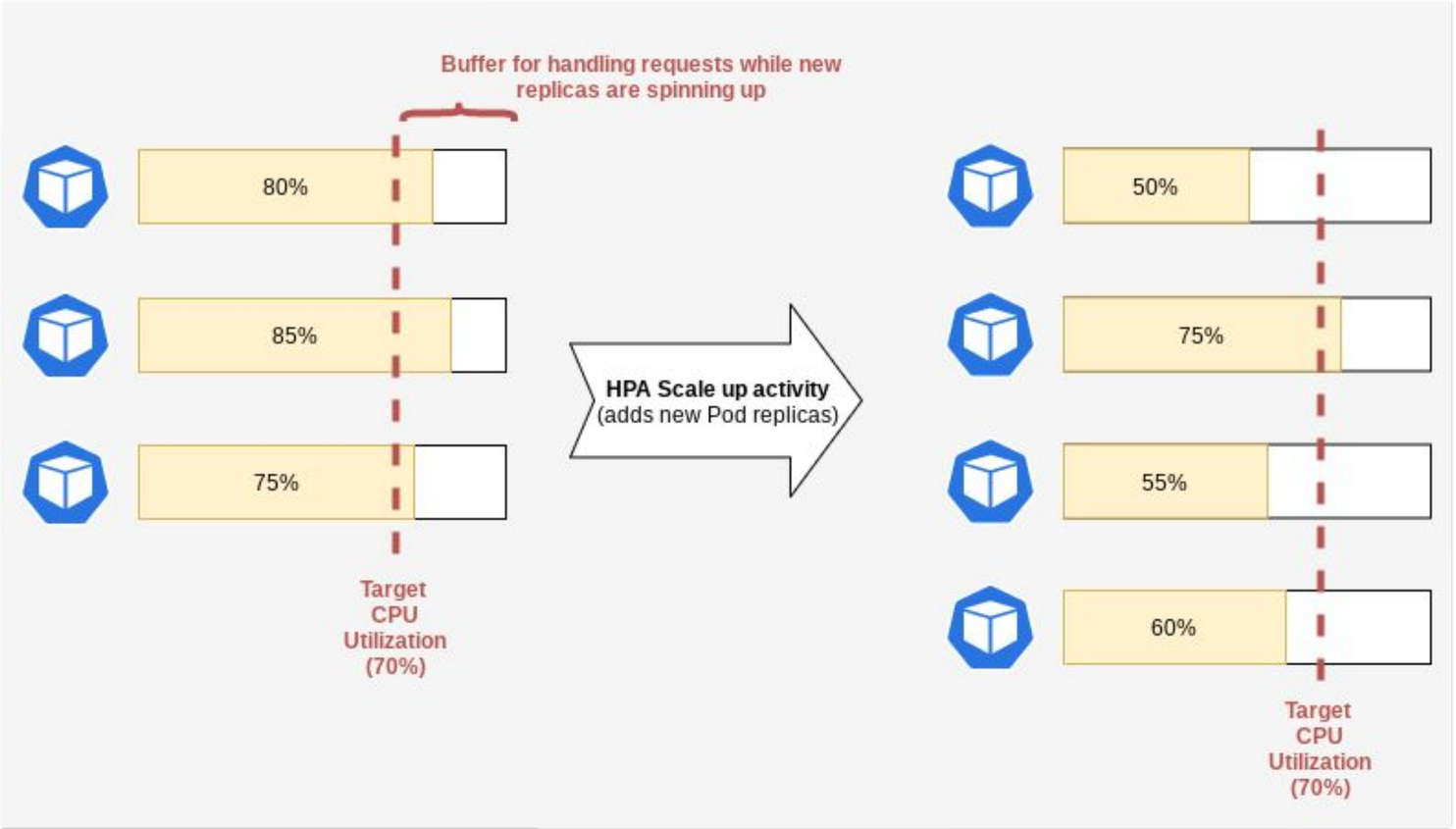


GKE supports all 4 scalability dimensions



GKE: Horizontal Pod Autoscaler (HPA)

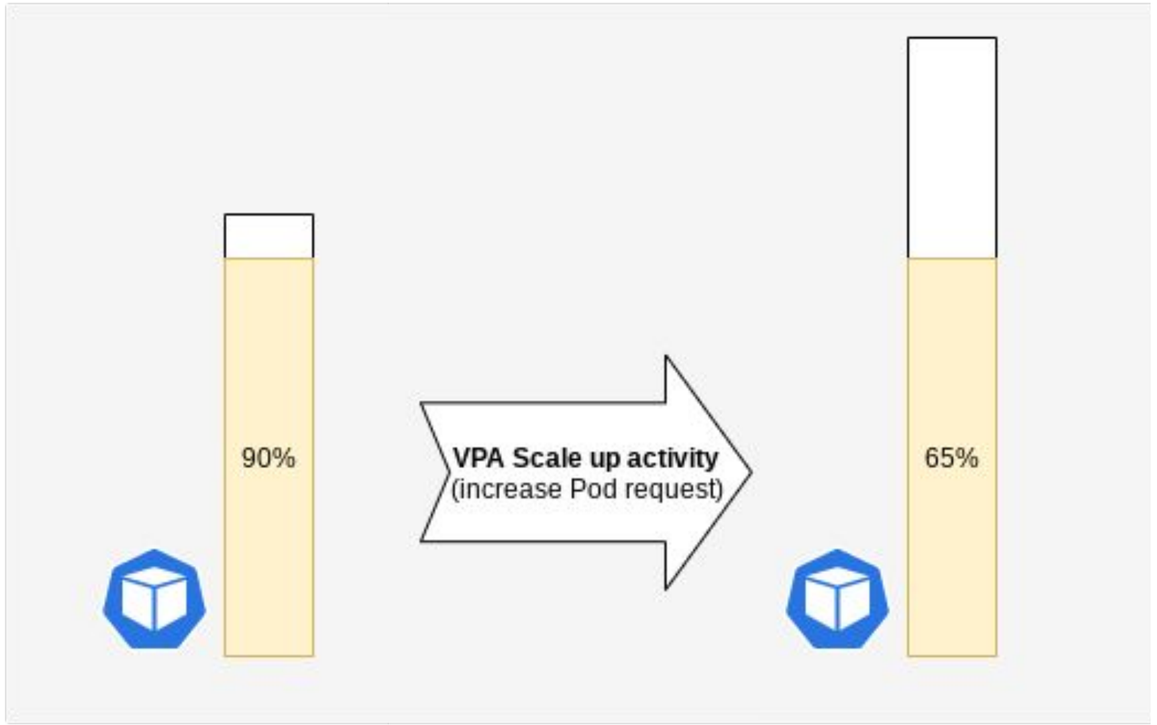
- Target Utilization: CPU or other custom metrics (eg. requests per second)
- Indicated for: stateless workers that can spin up reasonably fast
- Buffer size:
  - Small buffer prevents early scale ups, but it can overload your application during spikes.
  - Big buffer causes resource waste, increasing the cost of your bill.
  - Need to be enough for handling requests during two or three minutes in a spike.



For more information, see Configuring a Horizontal Pod Autoscaler.

GKE: Vertical Pod Autoscaler (VPA)

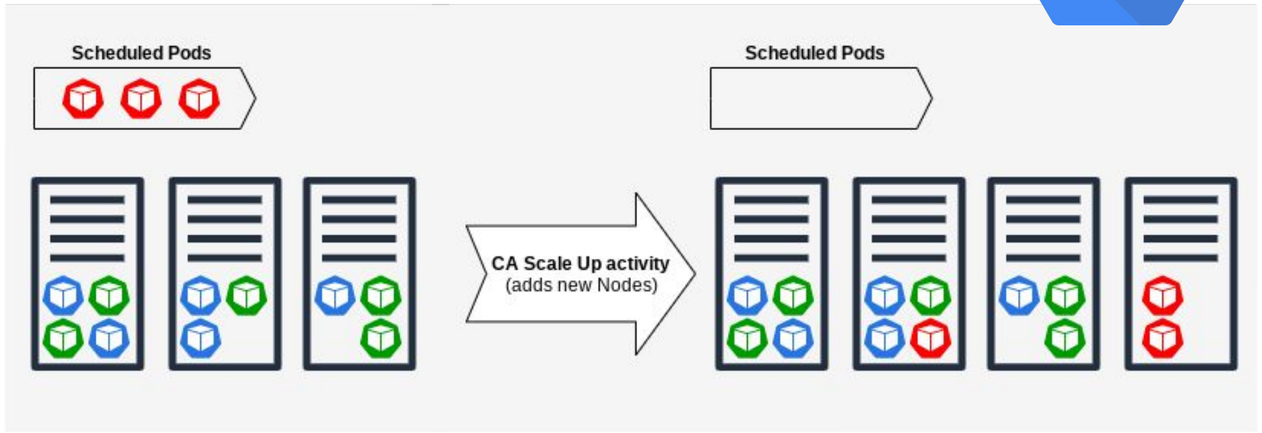
- Indicated for: stateless and stateful workloads not handled by HPA or when you don't know the proper Pod's resource requests
- Don't use VPA either Initial or Auto mode if you need to handle sudden spikes in traffic. Use HPA instead.
- Modes:
  - **Off**: recommendation
  - **Initial**: do not restart
  - **Auto**: restart
- Be careful when enabling the **Auto** Mode

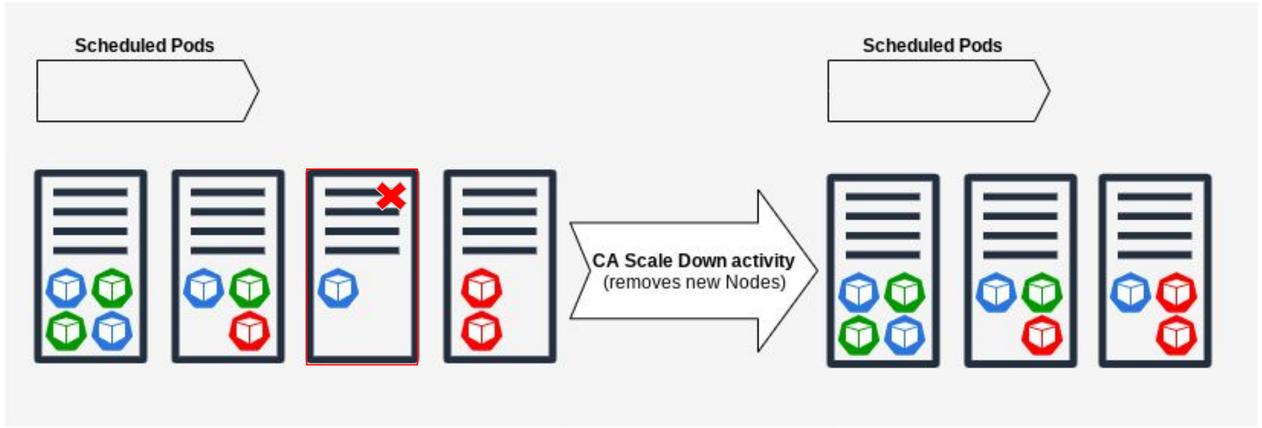


For more information, see Configuring Vertical Pod Autoscaling.

GKE: Cluster Autoscaler (CA)

- Indicated for: whenever you are using either HPA or VPA
- Optimized for the cost of infrastructure
- It is based on scheduling simulation and declared Pod requests
- Certain Pods cannot be restarted by any autoscaler. Blocking scale down. Kube-dns is the most common one. StatefulSets usually should not be restarted as well.
- If your workloads are resilient to nodes restarting inadvertently and to capacity losses, you can further improve cost savings by creating a cluster or node pool with preemptible VMs
- Learn how to analyse Cluster Autoscaler events in the logs.

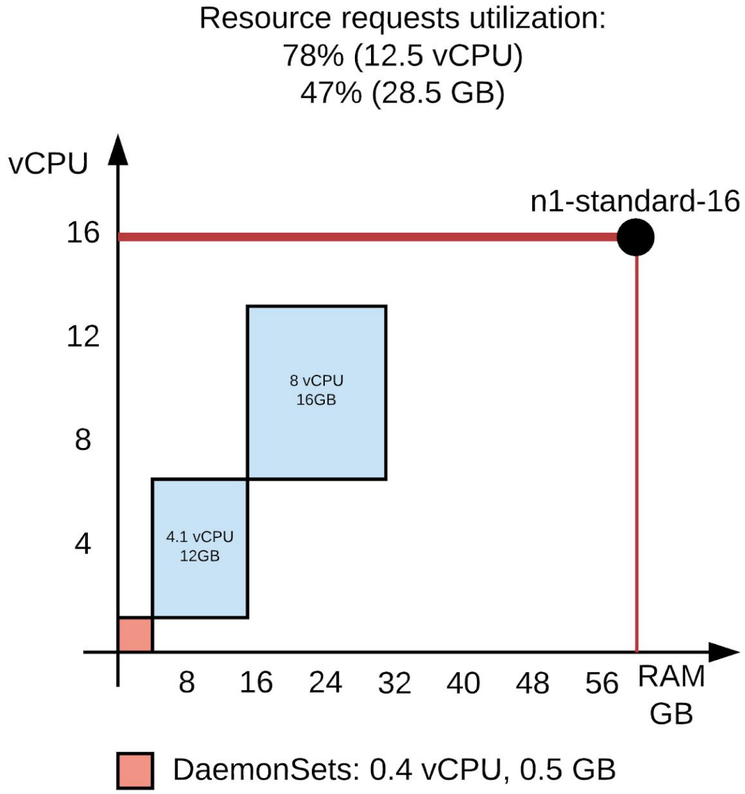


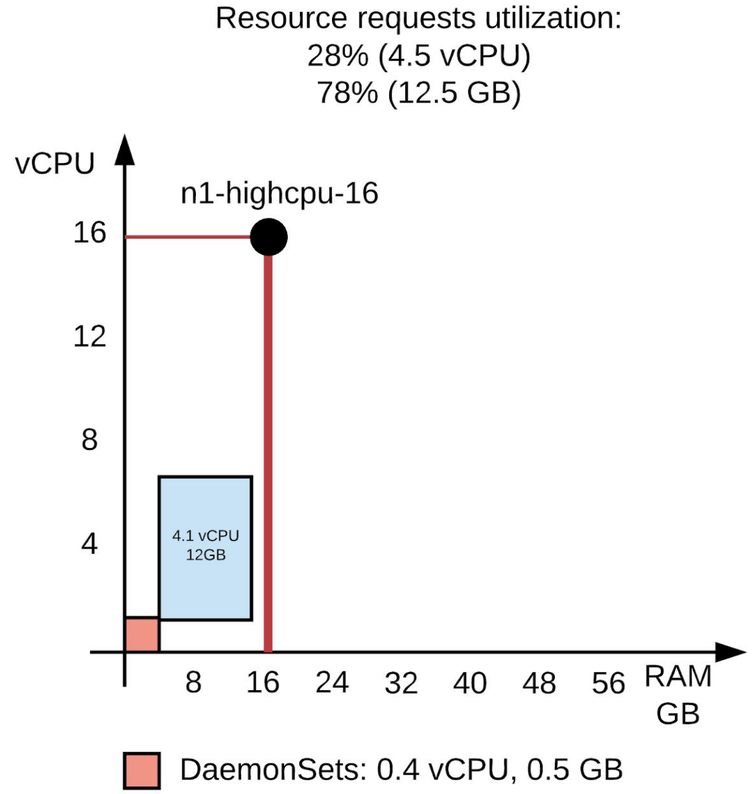


For more information, see Autoscaling a cluster.

GKE: Binpacking

- Make sure your workload fit well inside the machine size
- You can create multiple node pools and use either nodeSelector or Node Affinity to select which node your pod must run.
- Another simpler option is to configure Node auto-provisioning





GKE: Pod Placement

Requests & Limits	**Requests** specify how much resource (i.e. CPU and memory) a Container needs **Limits** specify the amount of resources the container is allowed to use
Node Selector	**Node selector** is an approach to schedule Pods to a specific set of nodes (or GKE node pools) using matching labels
Affinity & Anti-Affinity	**Affinity/anti-affinity i**s a scheduling feature to place Pods to Nodes using expressive rules against Pod and Node labels.
Taints & Tolerations	**Taints** are used to repel Pods from specific Nodes. **Tolerations** allow Pods to tolerate the taints

Pod Placement

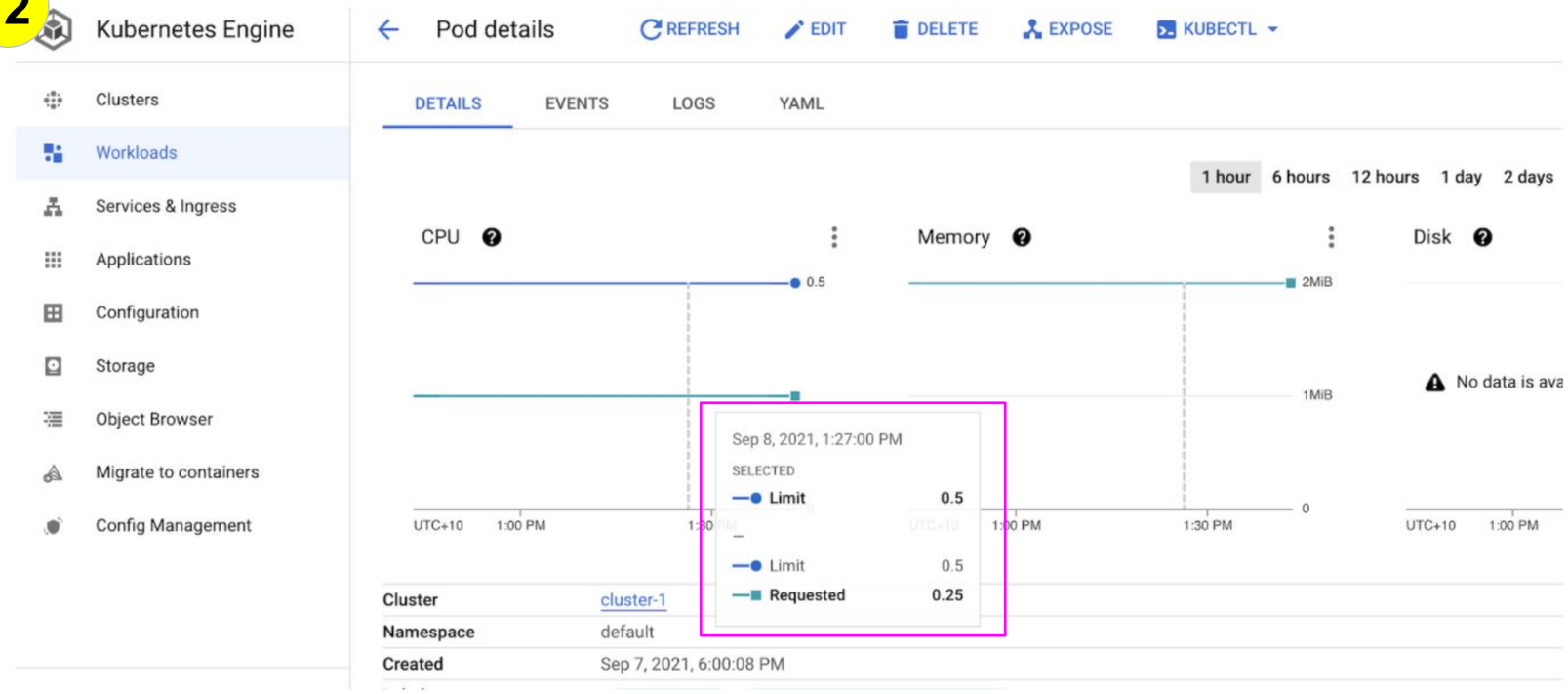
Requests & Limits

Requests specify how much resource (i.e. CPU and memory) a Container needs
Limits specify the amount of resources the container is allowed to use

1

```
apiVersion: v1
kind: Pod
metadata:
  name: frontend
spec:
  containers:
  - name: app
    image: images.my-company.example/app:v4
    resources:
      requests:
        memory: "64Mi"
        cpu: "250m"
      limits:
        memory: "128Mi"
        cpu: "500m"
  - name: log-aggregator
    image: images.my-company.example/log-aggregator:v6
    resources:
      requests:
        memory: "64Mi"
        cpu: "250m"
      limits:
        memory: "128Mi"
        cpu: "500m"
```

2



Memory cgroup out of memory: Killed process - when Container hits a memory limit

Pod Placement

Node Selector

Node selector is an approach to schedule Pods to a specific set of nodes (or GKE node pools) using matching labels

1

```
apiVersion: v1
kind: Pod
metadata:
  name: nginx
  labels:
    env: test
spec:
  containers:
  - name: nginx
    image: nginx:latest
    imagePullPolicy: IfNotPresent
  nodeSelector:
    cloud.google.com/gke-nodepool: app-pool
```

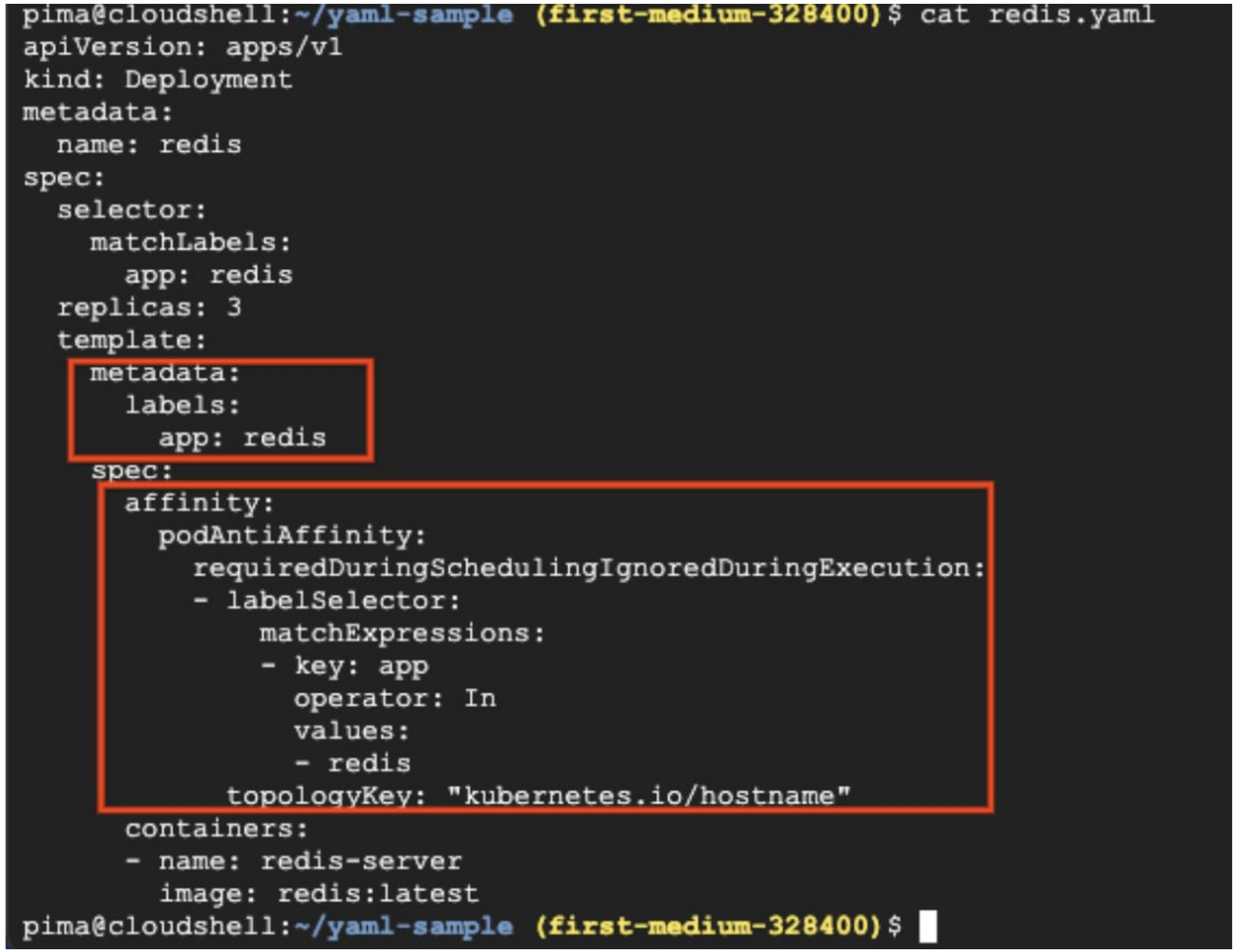
2

```
apiVersion: v1
kind: Pod
metadata:
  name: podthree
  labels:
    env: test
spec:
  containers:
  - name: nginx
    image: nginx:latest
    imagePullPolicy: IfNotPresent
  nodeSelector:
    disktype: ssd
```

Pod Placement

Affinity & Anti-Affinity

Affinity/anti-affinity is a scheduling feature to place Pods to Nodes using expressive rules against Pod and Node labels.



```
pima@cloudshell:~/yaml-sample (first-medium-328400)$ cat redis.yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: redis
spec:
  selector:
    matchLabels:
      app: redis
  replicas: 3
  template:
    metadata:
      labels:
        app: redis
    spec:
      affinity:
        podAntiAffinity:
          requiredDuringSchedulingIgnoredDuringExecution:
          - labelSelector:
              matchExpressions:
              - key: app
                operator: In
                values:
                - redis
            topologyKey: "kubernetes.io/hostname"
      containers:
      - name: redis-server
        image: redis:latest
pima@cloudshell:~/yaml-sample (first-medium-328400)$
```

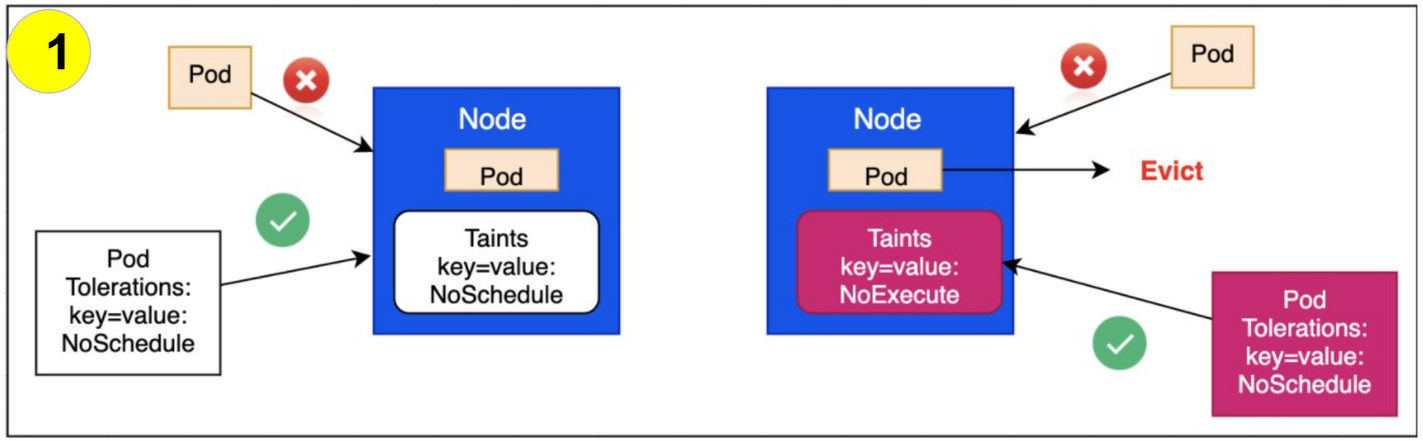
```
Error: Cannot schedule pods: node(s) didn't
match pod anti-affinity rules
```

Pod Placement

Taints & Tolerations

Taints are used to repel Pods from specific Nodes.
Tolerations allow Pods to tolerate the taints

1



2

$ kubectl taint nodes NODE_NAME key=value:effect
$ kubectl taint nodes gke-123 service=web:NoExecute

3

```
pima@cloudshell:~/yaml-sample (first-medium-328400)$ cat web.yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: web
spec:
  selector:
    matchLabels:
      app: web
  replicas: 3
  template:
    metadata:
      labels:
        app: web
    spec:
      containers:
      - name: web-app
        image: nginx:latest
      tolerations:
      - key: "service-web"
        operator: "Equal"
        value: "true"
        effect: "NoSchedule"
```

4

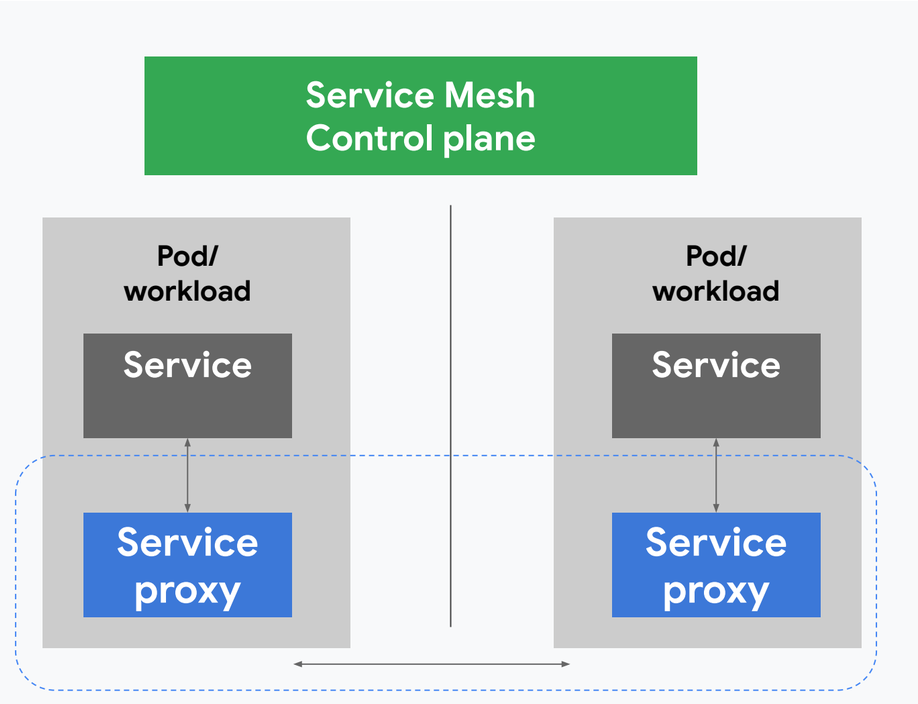
```
FailedScheduling: 0/3 nodes are available: 3 node(s) had
taint {service-web: true}, that the pod didn't tolerate
```

Service Mesh (Istio / ASM)

Used for visibility, traffic control, security, policy enforcement etc

Outbound features:

- Service authentication
- Load balancing
- Timeouts, retries and circuit breakers
- Connection pool sizing
- Fine-grained routing
- Telemetry
- Request Tracing
- Fault Injection



Data plane

Inbound features:

- Service authentication
- Authorization
- Rate limits
- Load shedding
- Telemetry
- Request Tracing
- Fault Injection

Exam Tip: *Service Mesh (Istio / Anthos Service Mesh) is often the right choice when advanced traffic management is required, eg. mutual TLS, Fault Injection, Traffic Splitting, Circuit Breaking, Connection Pooling etc. Have a look here.*

GOOGLE Kubernetes Engine

#GCPSketchnote

@PVERGADIA THECLOUDGIRL.DEV

9.07.2020

What is GKE?

Your app crashed in production!

SYS ADMIN SAM

Let's fix it once and for all with CONTAINER!

But it worked on my machine?!

DEVELOPER ERIN

CONTAINER FEATURES

- Portable
- Shareable
- Versions
- Isolation
- Introspection
- Fast Deployments
- Immutable
- Reusable

CONTAINER	VIRTUAL MACHINE	BARE-METAL SERVER
Application Code	Application Code	Application Code
Dependencies	Dependencies	Dependencies
Operating System	Operating System	Operating System
Hardware	Hardware	Hardware

But I have got lots of containers, how can I orchestrate all of them?

SAM

I have heard Kubernetes could be the answer...

It is open source platform for managing containers.

ERIN

SAM

Kubernetes is not that easy from Installation to Provisioning to Upgrades to Scaling & SLAs

How does GKE work?

SAM

User

kubectl

http://gRPC/GCP UI

Google Kubernetes Engine Container Cluster in GCP

REGIONAL CONTROL PLANE
- API Server
- Resource Controllers
- Storage
- Scheduler
- Replica in Zone B
- Replica in Zone C

NODES
- User Pod: Containers
- User Pod: Containers
- User Pod: Containers

CONNECTED GCP SERVICES
- VPC Networking
- Persistent Disk
- Load Balancer
- Cloud Monitoring

Color Legend:
- Google Kubernetes Engine provisions, maintains & operates
- Google Kubernetes Engine provisions User optionally maintains & operates

MANAGED KUBERNETES

KUBERNETES → GKE

I bet GKE is the answer with advanced cluster management!

- Easy Cluster Creation
- Load Balancing
- Auto Scaling
- Auto Upgrades
- Auto Repair
- Logging Monitoring

How do I use GKE ?

Cloud Code → Code Repository → Cloud Build → Container Registry → GKE ← Kubectl

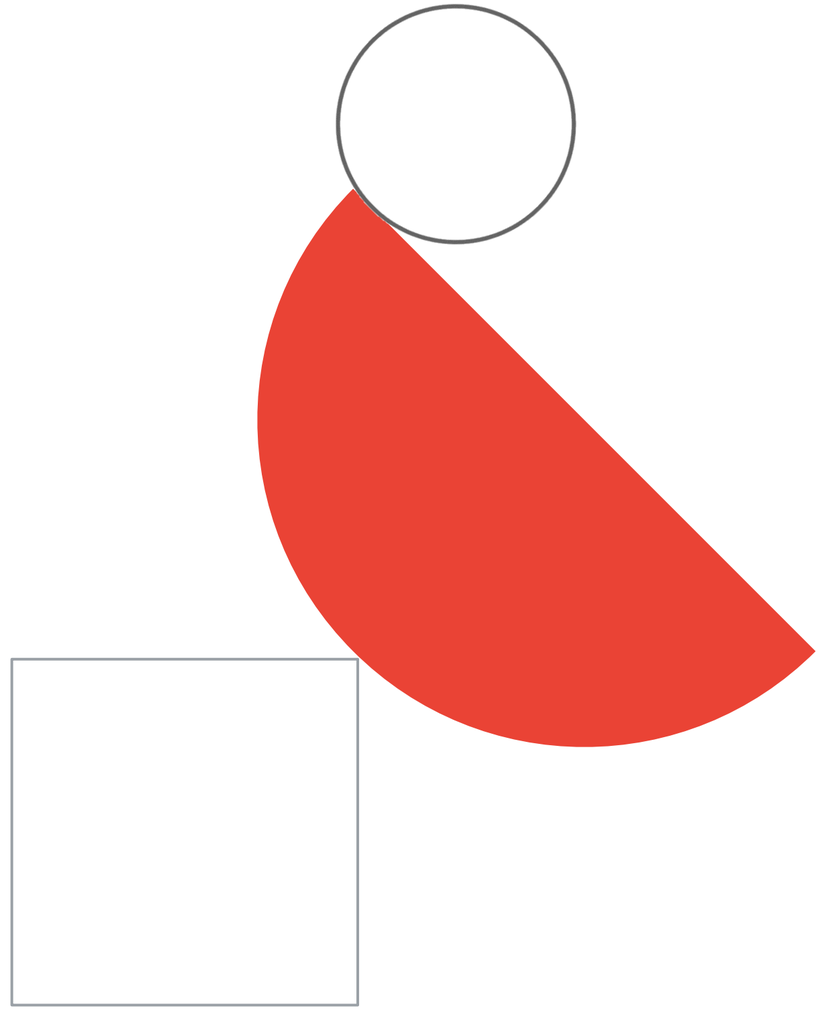
WORKLOAD		INFRASTRUCTURE	
Horizontal Pod Autoscaler (HPA)	Vertical Pod Autoscaler (VPA)	Cluster Autoscaler (CA)	Node Auto-Provisioning (NAP)
More Pods	Different Pod Sizes	More Nodes	Different Node Pools

How does it handle traffic growth?

How do I secure apps using GKE ?

SECURE APPS	TRUSTED NETWORKING	SOFTWARE SUPPLY CHAIN SECURITY
Data Encryption	Global VPC	Binary Authorization
Certified Images	Global Load Balancing	Vulnerability Scanning
Private Clusters	Cloud Armor	Managed Base Image
Idenity & Access - IAM - RBAC	Network Policy	

Cloud Run



Cloud Run

- Enables stateless containers.
- Abstracts away infrastructure management.
- Automatically scales up and down.
- Open API and runtime environment.

Exam Tip: *"Stateless" is the key here. Cloud Run is MUCH newer than App Engine (2019 vs 2008) and uses Kubernetes (App Engine uses pre-K8s and pre-Docker containers). Otherwise, use-cases for App Engine and Cloud Run are similar.*

Containers in GCP = GKE or Cloud Run

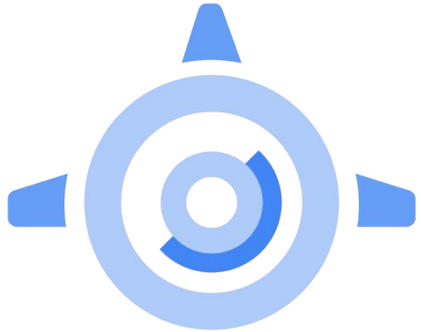
OR

Exam Tip: *How to differentiate between GKE and Cloud Run?*

- *Cloud Run is fully serverless (GKE Standard was not... but Autopilot is...)*
- *Cloud Run are best when your biggest priority is time to market (fast development, deployment, scaling) and want to remove the ops and infra management from the process, or do not have a team to orchestrate and manage containers.*
- *98% of new Cloud Run users are able to code, build, and deploy an app within 5 minutes*

AppEngine vs Cloud Run

- AppEngine was first released in *2008*, and while it still has a larger use-base and receives updates, Cloud Run offers, in most cases, a better alternative
- **Cloud Run** is the flagship product, receives updates first is container-first and compatible with open-source software
- Cloud Run covers almost all the use cases of AppEngine and has an excellent developer experience
- Cloud Run is great for serverless use-cases and event-driven automation
- See more in-depth comparison and migration info, including **performance** & **cost advantages** at go/migrate-run



App Engine

vs

Cloud Run

prefer this for new projects

Comparing the App Engine environments

	Standard environment	Flexible environment
Instance startup	Seconds	Minutes
SSH access	No	Yes (although not by default)
Write to local disk	No (some runtimes have read and write access to the /tmp directory)	Yes, ephemeral (disk initialized on each VM startup)
Support for 3rd-party binaries	For certain languages	Yes
Network access	Via App Engine services	Yes
Pricing model	After free daily use, pay per instance class, with automatic shutdown	Pay for resource allocation per hour; no automatic shutdown

Google Cloud

Exam Tip: *"Know how to differentiate between App Engine Standard and Flex.*

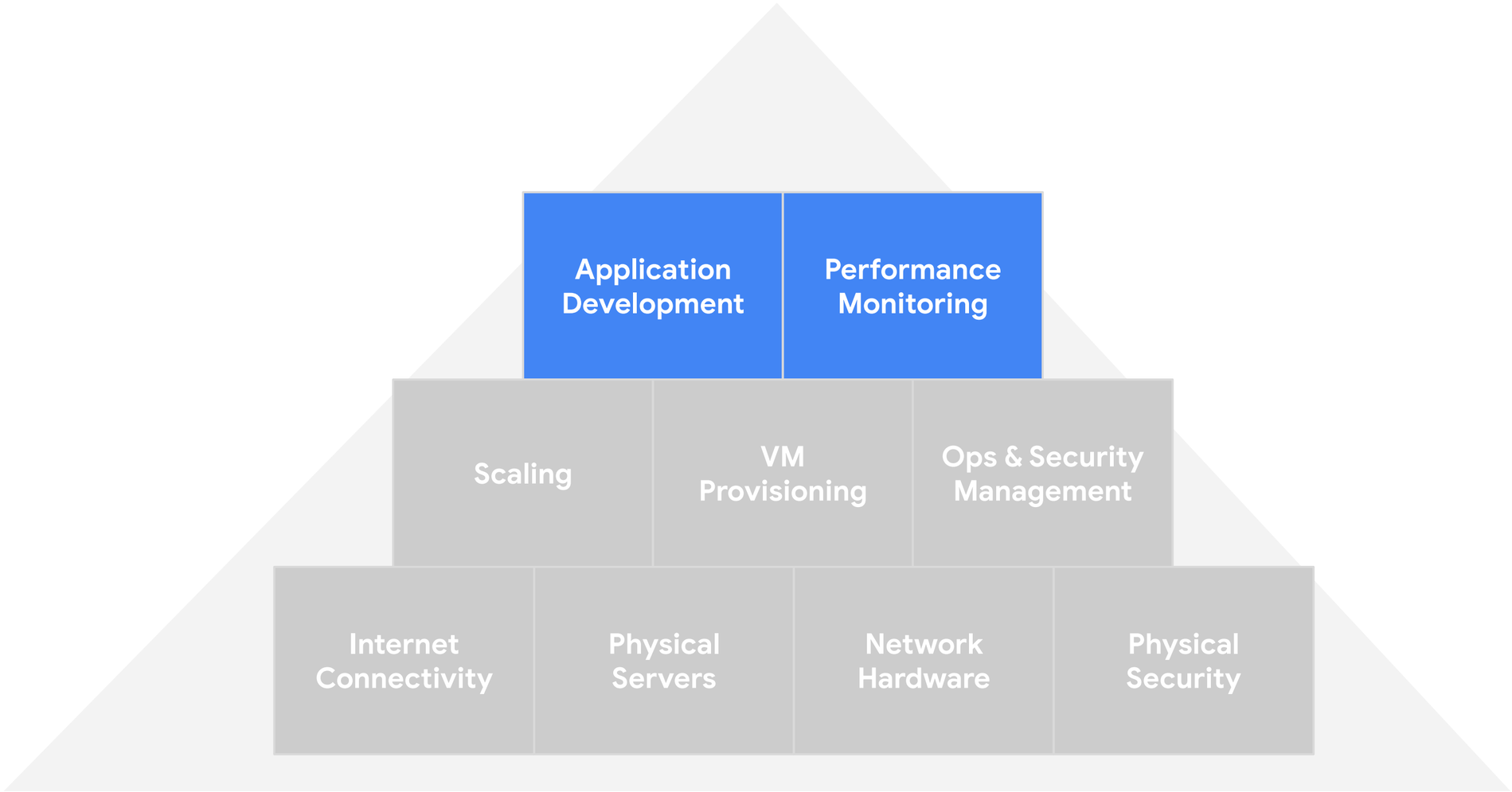
Cloud Functions

Exam Tip: *Cloud Functions (and App Engine Standard!) can scale to 0 if not being used.*

- Create single-purpose functions that respond to events without a server or runtime.
  - Event examples: New instance created, file added to Cloud Storage.
- Written in Javascript (Node.js), Python or Go; execute in managed Node.js environment on Google Cloud.

The Responsibility Pyramid

Serverless

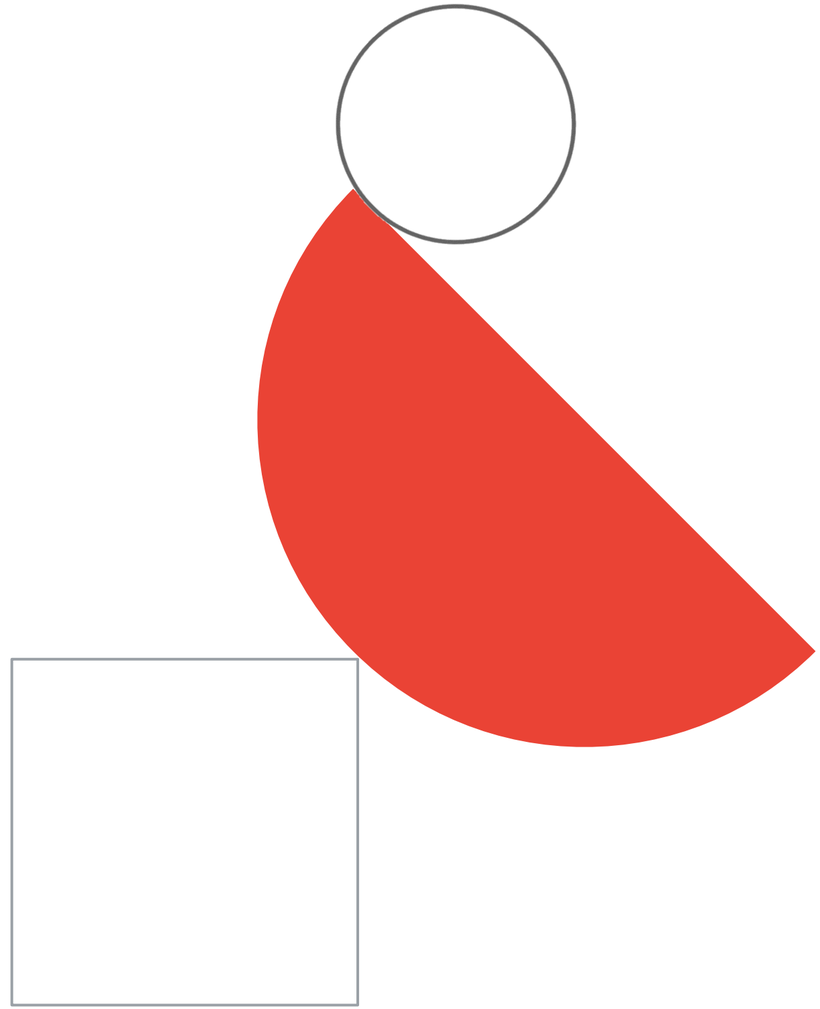


Managed by customer

Fully Managed by Google

Google Cloud

EHR case study analysis




EHR Healthcare

Proposed Technical Solutions

EHR Healthcare

- Data sensivity: HIPPA regulations, DLP, data encryption (possibly manual key management using CMEK / CSEK, KMS, HSM, EKM), least privilege approach (IAM, custom roles, IAP, ...), secure access to VMs and services, audit logs, bucket locks, Organization Policy Service.
- Kubernetes + "a group of Kubernetes clusters": GKE (possibly Autopilot mode), plus strong arguments for Anthos (“multiple, potentially different environments”)
  - consistent management, possibly from a single system: Anthos Config Management (ACM)
  - Manage traffic with Service Mesh: Fault Injection, Circuit Breaking, Request Timeouts
- MySQL + MS SQL Server -> Cloud SQL; Redis -> Memorystore; MongoDB -> MongoDB on GKE -> Firestore
- APIs for integration: Apigee (since it's integration with on-prem)
- Active Directory:
  - GCDS: Replication AD -> Cloud Identity, possibly also ADFS: AD Federation Services for AD-based single sign-on.
- Email-based alerting and Telemetry modernization: Cloud Operations Suite, uptime checks, SLIs and SLOs, dashboards and different notification channels. Alerting overview.
- Secure and high-performance connection between on-premises and GCP: Interconnect + Cloud VPN (HA) as backup
- CI/CD: (if cloud native) Cloud Source Repositories (CSR) + Cloud Build + Artifact Registry. Jenknis / Spinnaker if not GCP-native.
- Ingesting and processing data from new providers: ETL pipeline (possibly Pub/Sub -> Dataproc/Dataflow -> BigQuery)
- Dynamic provisioning of new environments: IaaC (Terraform / Deployment Manager).
- Making predictions: ML in the form of Vertex AI / AutoML / BigQuery ML / pre-built models, nothing very concrete
- Security products: Cloud Armor, Security Command Center

[EHR case study] Diagnostic Question #1

For this question, refer to the EHR Healthcare case study. You need to define the technical architecture for hybrid connectivity between EHR's on-premises systems and Google Cloud. You want to follow Google's recommended practices for production-level applications.

Considering the EHR Healthcare business and technical requirements, what should you do?

A. Configure two Partner Interconnect connections in one metro (City), and make sure the Interconnect connections are placed in different metro zones.

B. Configure two VPN connections from on-premises to Google Cloud, and make sure the VPN devices on-premises are in separate racks.

C. Configure Direct Peering between EHR Healthcare and Google Cloud, and make sure you are peering at least two Google locations.

D. Configure two Dedicated Interconnect connections in one metro (City) and two connections in another metro, and make sure the Interconnect connections are placed in different metro zones.

[EHR case study] Diagnostic Question #1

For this question, refer to the EHR Healthcare case study. You need to define the technical architecture for hybrid connectivity between EHR's on-premises systems and Google Cloud. You want to follow Google's recommended practices for production-level applications.

Considering the EHR Healthcare business and technical requirements, what should you do?

A. Configure two Partner Interconnect connections in one metro (City), and make sure the Interconnect connections are placed in different metro zones.

B. Configure two VPN connections from on-premises to Google Cloud, and make sure the VPN devices on-premises are in separate racks.

C. Configure Direct Peering between EHR Healthcare and Google Cloud, and make sure you are peering at least two Google locations.

D. Configure two Dedicated Interconnect connections in one metro (City) and two connections in another metro, and make sure the Interconnect connections are placed in different metro zones.

[EHR case study] Diagnostic Question #2

For this question, refer to the EHR Healthcare case study. In the past, configuration errors put public IP addresses on backend servers that should not have been accessible from the Internet. You need to ensure that no one can put external IP addresses on backend Compute Engine instances and that external IP addresses can only be configured on frontend Compute Engine instances.

What should you do?

A. Create an Organizational Policy with a constraint to allow external IP addresses only on the frontend Compute Engine instances.

B. Revoke the compute.networkAdmin role from all users in the project with front end instances.

C. Create an Identity and Access Management (IAM) policy that maps the IT staff to the compute.networkAdmin role for the organization.

D. Create a custom Identity and Access Management (IAM) role named GCE_FRONTEND with the compute.addresses.create permission.

[EHR case study] Diagnostic Question #2

For this question, refer to the EHR Healthcare case study. In the past, configuration errors put public IP addresses on backend servers that should not have been accessible from the Internet. You need to ensure that no one can put external IP addresses on backend Compute Engine instances and that external IP addresses can only be configured on frontend Compute Engine instances.

What should you do?

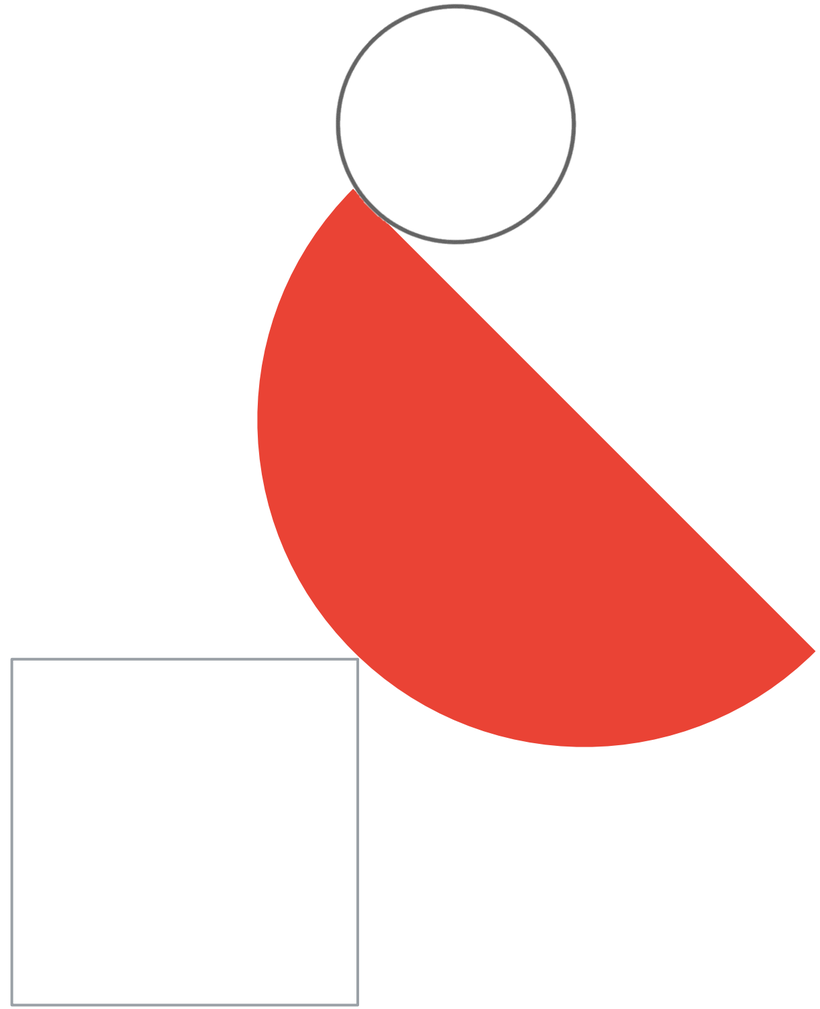
A. Create an Organizational Policy with a constraint to allow external IP addresses only on the frontend Compute Engine instances.

B. Revoke the compute.networkAdmin role from all users in the project with front end instances.

C. Create an Identity and Access Management (IAM) policy that maps the IT staff to the compute.networkAdmin role for the organization.

D. Create a custom Identity and Access Management (IAM) role named GCE_FRONTEND with the compute.addresses.create permission.

[optional] Links to useful materials



Optional materials 1

[READING]

- Get a feeling of different migration approaches to GCP.
- What is Binary Authorization (relevant to Kubernetes).
- Application deployment and testing strategies | Cloud Architecture Center
- Container-native load balancing through standalone zonal NEGs | Google Kubernetes Engine (GKE)
- Implementing deployment and testing strategies on GKE | Cloud Architecture Center

[VIDEOS]

- How is data encrypted? How does encryption work at Google's data centers?
- Data Encryption and KMS: Data Encryption and Managed Encryption Keys
- What is Kubernetes?
- [demo] Creating a GKE Cluster with a detailed explanation of the options: Creating a GKE cluster (demo)
- Cloud Run intro: Say hello to serverless containers with Cloud Run
- VERY nice Cloud Run deep-dive session: How to run your container without servers
- Examples of Cloud Run usage: Can Cloud Run handle these 9 workloads?
- Cloud Functions vs Cloud Run: https://www.youtube.com/watch?v=zRjOSxTpC3A
- Where should I run my code?:
  a. Shorter version: Choosing the right compute option in GCP: a decision tree
  b. Longer version (HIGHLY recommended!): Where should I run my stuff? Choosing compute options

Optional materials 2

- Observing container environments with Cloud Operations Suite: Observing container environments with Cloud Operations
- How to run containers on Kubernetes
- Building Small Containers
- Kubernetes architecture: Nodes and control plane
- Kubernetes networking:
  a. Short version (5 min): Introduction to GKE cluster networking
  b. Slightly longer (11 min) one, with additional info: GKE: Concepts of Networking
- Introduction to GKE Autoscaling
- Introducing Autopilot in Google Kubernetes Engine
- Secure access to GKE workloads with Workload Identity
- Top 3 ways to run your containers on Google Cloud
- What is Anthos?
  a. Super-short version: What is Anthos? #GCPSketchnote
  b. Short version: What is Anthos?
  c. Longer version: An introduction to Anthos (Google Cloud Community Day '19)
- All you need to know about Migrate for Anthos: Introducing Migrate for Anthos and GKE

Optional materials 3

- BeyondCorp and IAP (Identity-Aware Proxy): Getting started with BeyondCorp: A deeper look into IAP
- Security Command Center overview: The three-step overview
- Data Loss Prevention (DLP) overview: Getting started with Data Loss Prevention on Security Command Center
- Secret Manager: Manage your Cloud Run secrets securely with Secret Manager

[PODCASTS]

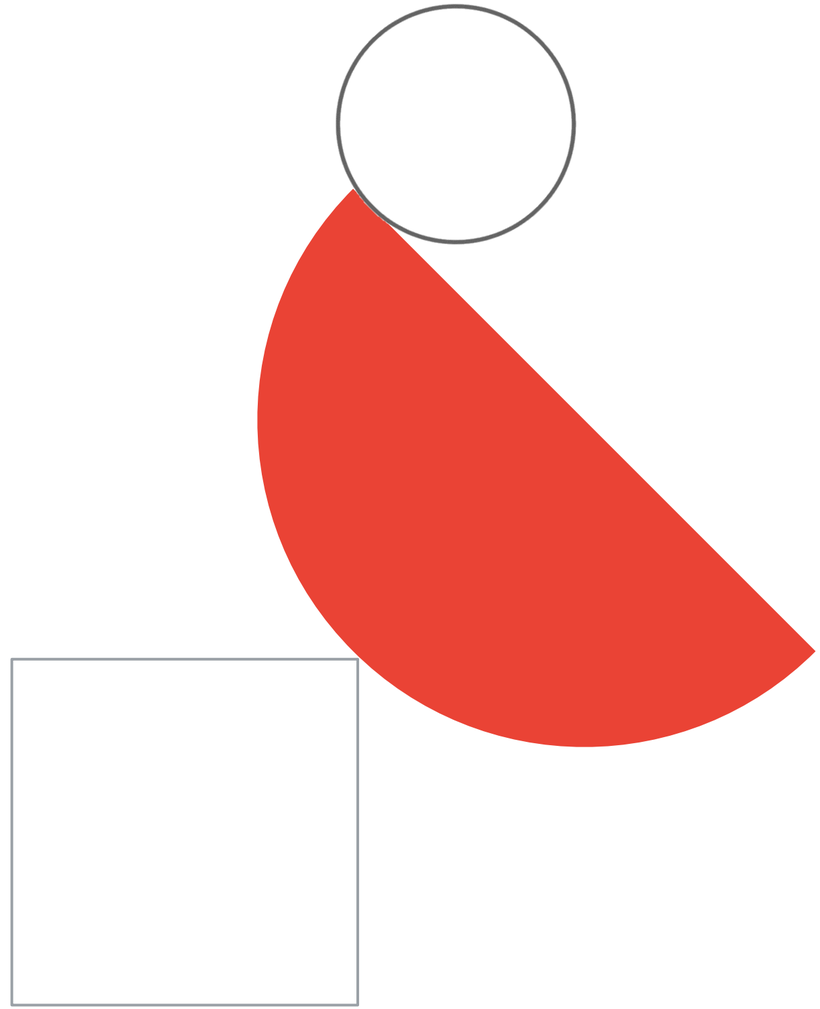
- GKE Autopilot
- Cloud Run and Anthos
- Cloud Run

[DEEP DIVES]

- [video] Kubernetes Q&A: Answering your Kubernetes Questions | AMA with Eric Brewer
- [video] Terraform, serverless, and Cloud Run in practice: Terraform, serverless, and Cloud Run in practice
- [video] [super interesting documentary] [not technical] [for k8s geeks] :) Kubernetes: The Documentary: Part 1, Part 2.

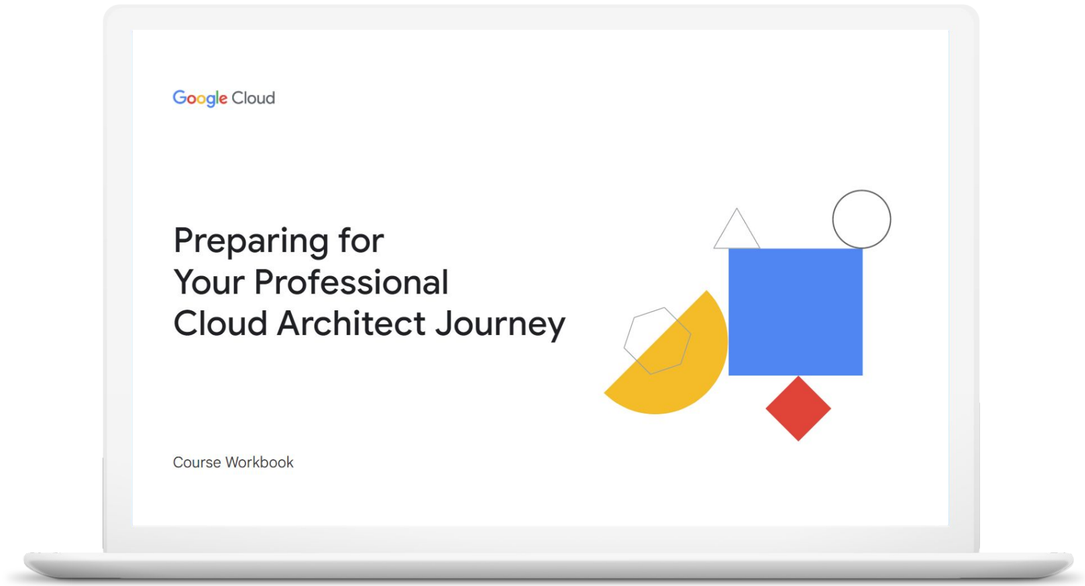
Diagnostic Questions

for Exam Guide Section 3: Designing for security and compliance



PCA Exam Guide Section 3:

Designing for security and compliance



3.1 Designing for security

3.2 Designing for compliance

3.1 Designing for security

Considerations include:

- Identity and access management (IAM)
- Resource hierarchy (organizations, folders, projects)
- Data security (key management, encryption, secret management)
- Separation of duties (SoD)
- Security controls (e.g., auditing, VPC Service Controls, context aware access, organization policy)
- Managing customer-managed encryption keys with Cloud Key Management Service
- Remote access

3.1 Diagnostic Question 01 Discussion

Your client created an Identity and Access Management (IAM) resource hierarchy with Google Cloud when the company was a startup. Your client has grown and now has **multiple departments and teams**. You want to recommend a resource hierarchy that follows Google-recommended practices.

What should you do?

A. Keep all resources in **one project**, and use a **flat resource hierarchy** to reduce complexity and simplify management.

B. Keep all resources in **one project,** but **change the resource hierarchy** to reflect company organization.

C. Use a **flat resource hierarchy** and **multiple projects** with established trust boundaries.

D. Use **multiple projects** with established trust boundaries, and **change the resource hierarchy** to reflect company organization.

3.1 Diagnostic Question 01 Discussion

Your client created an Identity and Access Management (IAM) resource hierarchy with Google Cloud when the company was a startup. Your client has grown and now has **multiple departments and teams**. You want to recommend a resource hierarchy that follows Google-recommended practices.

What should you do?

A. Keep all resources in **one project**, and use a **flat resource hierarchy** to reduce complexity and simplify management.

B. Keep all resources in **one project,** but **change the resource hierarchy** to reflect company organization.

C. Use a **flat resource hierarchy** and **multiple projects** with established trust boundaries.

D. Use **multiple projects** with established trust boundaries, and **change the resource hierarchy** to reflect company organization.

3.1 Diagnostic Question 02 Discussion

Cymbal Direct's social media app must run in a **separate project** from its APIs and web store. You want to use **Identity and Access Management (IAM)** to ensure a **secure environment.**

How should you set up IAM?

A. Use **separate** service accounts for each component (social media app, APIs, and web store) with **basic** roles to grant access.

B. Use **one** service account for all components (social media app, APIs, and web store) with **basic** roles to grant access.

C. Use **separate** service accounts for each component (social media app, APIs, and web store) with **predefined or custom** roles to grant access.

D. Use **one** service account for all components (social media app, APIs, and web store) with **predefined or custom** roles to grant access.

3.1 Diagnostic Question 02 Discussion

Cymbal Direct's social media app must run in a **separate project** from its APIs and web store. You want to use **Identity and Access Management (IAM)** to ensure a **secure environment.**

How should you set up IAM?

A. Use **separate** service accounts for each component (social media app, APIs, and web store) with **basic** roles to grant access.

B. Use **one** service account for all components (social media app, APIs, and web store) with **basic** roles to grant access.

C. Use **separate** service accounts for each component (social media app, APIs, and web store) with **predefined or custom** roles to grant access.

D. Use **one** service account for all components (social media app, APIs, and web store) with **predefined or custom** roles to grant access.

3.1 Diagnostic Question 03 Discussion

Michael is the owner/operator of “Zneeks,” a retail shoe store that caters to sneaker aficionados. He regularly works with customers who order small batches of custom shoes. Michael is interested in **using Cymbal Direct to manufacture and ship custom batches of shoes to these customers**. Reasonably tech-savvy but not a developer, Michael likes using Cymbal Direct's **partner purchase portal but wants the process to be easy**.

What is an example of a user story that could describe Michael’s persona?

A. As a shoe retailer, Michael wants to **send Cymbal Direct custom purchase orders so that batches of custom shoes are sent to his customers.**

B. Michael is a **tech-savvy owner/operator** of a small business.

C. Zneeks is a **retail shoe store** that **caters to sneaker aficionados**.

D. Michael is reasonably tech-savvy but **needs Cymbal Direct's partner purchase portal to be easy.**

3.1 Diagnostic Question 03 Discussion

Michael is the owner/operator of “Zneeks,” a retail shoe store that caters to sneaker aficionados. He regularly works with customers who order small batches of custom shoes. Michael is interested in **using Cymbal Direct to manufacture and ship custom batches of shoes to these customers**. Reasonably tech-savvy but not a developer, Michael likes using Cymbal Direct's **partner purchase portal but wants the process to be easy**.

What is an example of a user story that could describe Michael’s persona?

A. As a shoe retailer, Michael wants to **send Cymbal Direct custom purchase orders so that batches of custom shoes are sent to his customers.**

B. Michael is a **tech-savvy owner/operator** of a small business.

C. Zneeks is a **retail shoe store** that **caters to sneaker aficionados**.

D. Michael is reasonably tech-savvy but **needs Cymbal Direct's partner purchase portal to be easy.**

3.1 Diagnostic Question 04 Discussion

Cymbal Direct has an application running on a Compute Engine instance. You need to g**ive the application access** to several Google Cloud services. You **do not want to keep any credentials on the VM** instance itself.

What should you do?

A. Create a service account **for each of the services** the VM needs to access. Associate the service accounts with the Compute Engine instance.

B. Create a service account and **assign it the project owner role**, which enables access to any needed service.

C. Create a service account for the instance. Use **Access scopes** to enable access to the required services.

D. Create a service account with one or more **predefined or custom roles**, which give access to the required services.

3.1 Diagnostic Question 04 Discussion

Cymbal Direct has an application running on a Compute Engine instance. You need to g**ive the application access** to several Google Cloud services. You **do not want to keep any credentials on the VM** instance itself.

What should you do?

A. Create a service account **for each of the services** the VM needs to access. Associate the service accounts with the Compute Engine instance.

B. Create a service account and **assign it the project owner role**, which enables access to any needed service.

C. Create a service account for the instance. Use **Access scopes** to enable access to the required services.

D. Create a service account with one or more **predefined or custom roles**, which give access to the required services.

3.1 Diagnostic Question 05 Discussion

Cymbal Direct wants to use Identity and Access Management (IAM) to allow employees to have **access to Google Cloud resources and services based on their job roles**. **Several employees are project managers and want to have some level of access** to see what has been deployed. The security team wants to ensure that securing the environment and managing resources is simple so that it will **scale.**

What approach should you use?

A. Grant access by assigning **custom** roles to groups. Use multiple groups for better control. Give access as low in the hierarchy as possible to prevent the inheritance of too many abilities from a higher level.

B. Grant access by assigning **predefined roles to groups.** Use multiple groups for better control. Give access as **low in the hierarchy as possible** to prevent the inheritance of too many abilities from a higher level.

C. Give access directly to each **individual** for more granular control. Give access as low in the hierarchy as possible to prevent the inheritance of too many abilities from a higher level.

D. Grant access by assigning **predefined roles to groups**. Use multiple groups for better control. Make sure you **give out access to all the children** in a hierarchy under the level needed, because child resources will not automatically inherit abilities.

3.1 Diagnostic Question 05 Discussion

Cymbal Direct wants to use Identity and Access Management (IAM) to allow employees to have **access to Google Cloud resources and services based on their job roles**. **Several employees are project managers and want to have some level of access** to see what has been deployed. The security team wants to ensure that securing the environment and managing resources is simple so that it will **scale.**

What approach should you use?

A. Grant access by assigning **custom** roles to groups. Use multiple groups for better control. Give access as low in the hierarchy as possible to prevent the inheritance of too many abilities from a higher level.

B. Grant access by assigning **predefined roles to groups.** Use multiple groups for better control. Give access as **low in the hierarchy as possible** to prevent the inheritance of too many abilities from a higher level.

C. Give access directly to each **individual** for more granular control. Give access as low in the hierarchy as possible to prevent the inheritance of too many abilities from a higher level.

D. Grant access by assigning **predefined roles to groups**. Use multiple groups for better control. Make sure you **give out access to all the children** in a hierarchy under the level needed, because child resources will not automatically inherit abilities.

3.1 Diagnostic Question 06 Discussion

You have several Compute Engine instances running NGINX and Tomcat for a web application. In your web server logs, **many login failures come from a single IP address,** which looks like a brute force attack.

How can you block this traffic?

A. **Edit the Compute Engine instances** running your web application, and **enable Google Cloud Armor.** Create a Google Cloud Armor policy with a default rule action of "Allow." Add a new rule that specifies the IP address causing the login failures as the Condition, with an action of "Deny" and a deny status of "403," and accept the default priority (1000).

B. Ensure that an HTTP(S) load balancer is configured to send traffic to the backend Compute Engine instances running your web server. Create a Google Cloud Armor policy with a **default rule action of "Deny."** Add a new rule that specifies the IP address causing the login failures as the Condition, with an action of "Deny" and a deny status of "403," and accept the default priority (1000). Add the load balancer backend service's HTTP-backend as the target.

C. Ensure that an HTTP(S) load balancer is configured to send traffic to the backend Compute Engine instances running your web server. Create a Google Cloud Armor policy with a default rule action of "Allow." **Add a new rule that specifies the IP address causing the login failures** as the Condition, with an action of "Deny" and a deny status of "403," and accept the default priority (1000). Add the load balancer backend service's HTTP-backend as the target.

D. Ensure that an HTTP(S) load balancer is configured to send traffic to your backend Compute Engine instances running your web server. Create a Google Cloud Armor policy **using the instance's local firewall** with a default rule action of "Allow." **Add a new local firewall rule** that specifies the IP address causing the login failures as the Condition, with an action of "Deny" and a deny status of "403," and accept the default priority (1000).

3.1 Diagnostic Question 06 Discussion

You have several Compute Engine instances running NGINX and Tomcat for a web application. In your web server logs, **many login failures come from a single IP address,** which looks like a brute force attack.

How can you block this traffic?

A. **Edit the Compute Engine instances** running your web application, and **enable Google Cloud Armor.** Create a Google Cloud Armor policy with a default rule action of "Allow." Add a new rule that specifies the IP address causing the login failures as the Condition, with an action of "Deny" and a deny status of "403," and accept the default priority (1000).

B. Ensure that an HTTP(S) load balancer is configured to send traffic to the backend Compute Engine instances running your web server. Create a Google Cloud Armor policy with a **default rule action of "Deny."** Add a new rule that specifies the IP address causing the login failures as the Condition, with an action of "Deny" and a deny status of "403," and accept the default priority (1000). Add the load balancer backend service's HTTP-backend as the target.

C. Ensure that an HTTP(S) load balancer is configured to send traffic to the backend Compute Engine instances running your web server. Create a Google Cloud Armor policy with a default rule action of "Allow." **Add a new rule that specifies the IP address causing the login failures** as the Condition, with an action of "Deny" and a deny status of "403," and accept the default priority (1000). Add the load balancer backend service's HTTP-backend as the target.

D. Ensure that an HTTP(S) load balancer is configured to send traffic to your backend Compute Engine instances running your web server. Create a Google Cloud Armor policy **using the instance's local firewall** with a default rule action of "Allow." **Add a new local firewall rule** that specifies the IP address causing the login failures as the Condition, with an action of "Deny" and a deny status of "403," and accept the default priority (1000).

3.1 Diagnostic Question 07 Discussion

Cymbal Direct needs to make sure its new social media integration service **can't be accessed directly from the public internet.** You want to **allow access only through the web frontend store**.

How can you prevent access to the social media integration service from the outside world, but still **allow access to the APIs** of social media services?

A. **Remove external IP addresses** from the VM instances running the social media service and place them in a private VPC behind **Cloud NAT**. Any SSH connection for management should be done with **Identity-Aware Proxy (IAP)** or a **bastion host (jump box)** after allowing SSH access from IAP or a corporate network.

B. **Limit access to the external IP addresses** of the VM instances using firewall rules and place them in a private VPC behind Cloud NAT. Any SSH connection for management should be done with Identity-Aware Proxy (IAP) or a bastion host (jump box) after allowing SSH access from IAP or a corporate network.

C. **Limit access to the external IP addresses** of the VM instances using a firewall rule to block all outbound traffic. Any SSH connection for management should be done with Identity-Aware Proxy (IAP) or a bastion host (jump box) after allowing SSH access from IAP or a corporate network.

D. **Remove external IP addresses** from the VM instances running the social media service and place them in a private VPC behind **Cloud NAT**. Any SSH connection for management should be restricted to corporate network IP addresses by Google Cloud Armor.

3.1 Diagnostic Question 07 Discussion

Cymbal Direct needs to make sure its new social media integration service **can't be accessed directly from the public internet.** You want to **allow access only through the web frontend store**.

How can you prevent access to the social media integration service from the outside world, but still **allow access to the APIs** of social media services?

A. **Remove external IP addresses** from the VM instances running the social media service and place them in a private VPC behind **Cloud NAT**. Any SSH connection for management should be done with **Identity-Aware Proxy (IAP)** or a **bastion host (jump box)** after allowing SSH access from IAP or a corporate network.

B. **Limit access to the external IP addresses** of the VM instances using firewall rules and place them in a private VPC behind Cloud NAT. Any SSH connection for management should be done with Identity-Aware Proxy (IAP) or a bastion host (jump box) after allowing SSH access from IAP or a corporate network.

C. **Limit access to the external IP addresses** of the VM instances using a firewall rule to block all outbound traffic. Any SSH connection for management should be done with Identity-Aware Proxy (IAP) or a bastion host (jump box) after allowing SSH access from IAP or a corporate network.

D. **Remove external IP addresses** from the VM instances running the social media service and place them in a private VPC behind **Cloud NAT**. Any SSH connection for management should be restricted to corporate network IP addresses by Google Cloud Armor.

3.1 Diagnostic Question 08 Discussion

Cymbal Direct is experiencing success using Google Cloud and you want to leverage tools to make your solutions more efficient. Erik, one of the original web developers, currently adds new products to your application manually. Erik has many responsibilities and requires a long lead time to add new products. You need to create a Cloud Functions application to **let Cymbal Direct employees add new products** instead of waiting for Erik. However, you want to make sure that **only authorized employees** can use the application.

What should you do?

A. Set up Cloud VPN between the corporate network and the Google Cloud project's VPC network. Allow **users** to connect to the Cloud Functions instance.

B. Use Google Cloud Armor to restrict access to the corporate network's external IP address. Configure firewall rules to allow only HTTP(S) access.

C. Create a **Google group** and add authorized employees to it. Configure Identity-Aware Proxy (IAP) to the Cloud Functions application as a HTTP-resource. Add the group as a principle with the role **"Project Owner."**

D. Create a **Google group** and add authorized employees to it. Configure Identity-Aware Proxy (IAP) to the Cloud Functions application as a HTTP-resource. Add the group as a principle with the role **"IAP-secured Web App User."**

3.1 Diagnostic Question 08 Discussion

Cymbal Direct is experiencing success using Google Cloud and you want to leverage tools to make your solutions more efficient. Erik, one of the original web developers, currently adds new products to your application manually. Erik has many responsibilities and requires a long lead time to add new products. You need to create a Cloud Functions application to **let Cymbal Direct employees add new products** instead of waiting for Erik. However, you want to make sure that **only authorized employees** can use the application.

What should you do?

A. Set up Cloud VPN between the corporate network and the Google Cloud project's VPC network. Allow **users** to connect to the Cloud Functions instance.

B. Use Google Cloud Armor to restrict access to the corporate network's external IP address. Configure firewall rules to allow only HTTP(S) access.

C. Create a **Google group** and add authorized employees to it. Configure Identity-Aware Proxy (IAP) to the Cloud Functions application as a HTTP-resource. Add the group as a principle with the role **"Project Owner."**

D. Create a **Google group** and add authorized employees to it. Configure Identity-Aware Proxy (IAP) to the Cloud Functions application as a HTTP-resource. Add the group as a principle with the role **"IAP-secured Web App User."**

3.1 Designing for security

Resources to start your journey

Google Cloud Architecture Framework: Security, privacy, and compliance

IAM best practice guides available now | Google Cloud Blog

Using resource hierarchy for access control | IAM Documentation | Google Cloud

Chapter 18 - SRE Engagement Model

Service accounts | Compute Engine Documentation | Google Cloud

Google Cloud Armor overview

Private clusters | Kubernetes Engine Documentation | Google Cloud

Understanding IAM custom roles | IAM Documentation | Google Cloud

3.2 Designing for compliance

Considerations include:

- Legislation (e.g., health record privacy, children's privacy, data privacy, and ownership)
- Commercial (e.g., sensitive data such as credit card information handling, personally identifiable information [PII])
- Industry certifications (e.g., SOC 2)
- Audits (including logs)

3.1 Diagnostic Question 09 Discussion

You've recently created an internal Cloud Run application for developers in your organization. The application lets **developers clone production Cloud SQL databases into a project specifically created to test code and deployments**. Your previous process was to export a database to a Cloud Storage bucket, and then import the SQL dump into a legacy on-premises testing environment database with connectivity to Google Cloud via Cloud VPN. Management wants to **incentivize using the new process with Cloud SQL** for rapid testing and track how frequently rapid testing occurs.

How can you ensure that the developers use the new process?

A. **Use an ACL on the Cloud Storage bucket.** Create a read-only group that only has viewer privileges, and ensure that the developers are in that group.

B. Leave the ACLs on the Cloud Storage bucket as-is. **Disable Cloud VPN**, and have developers use Identity-Aware Proxy (IAP) to connect. Create an organization policy to enforce public access protection.

C. Use **predefined roles to restrict access** to what the developers are allowed to do. Create a group for the developers, and associate the group with the Cloud SQL Viewer role. Remove the "cloudsql.instances.export" ability from the role.

D. Create a **custom role to restrict access** to what developers are allowed to do. Create a group for the developers, and associate the group with your custom role. Ensure that the custom role does not have "cloudsql.instances.export."

3.1 Diagnostic Question 09 Discussion

You've recently created an internal Cloud Run application for developers in your organization. The application lets **developers clone production Cloud SQL databases into a project specifically created to test code and deployments**. Your previous process was to export a database to a Cloud Storage bucket, and then import the SQL dump into a legacy on-premises testing environment database with connectivity to Google Cloud via Cloud VPN. Management wants to **incentivize using the new process with Cloud SQL** for rapid testing and track how frequently rapid testing occurs.

How can you ensure that the developers use the new process?

A. **Use an ACL on the Cloud Storage bucket.** Create a read-only group that only has viewer privileges, and ensure that the developers are in that group.

B. Leave the ACLs on the Cloud Storage bucket as-is. **Disable Cloud VPN**, and have developers use Identity-Aware Proxy (IAP) to connect. Create an organization policy to enforce public access protection.

C. Use **predefined roles to restrict access** to what the developers are allowed to do. Create a group for the developers, and associate the group with the Cloud SQL Viewer role. Remove the "cloudsql.instances.export" ability from the role.

D. Create a **custom role to restrict access** to what developers are allowed to do. Create a group for the developers, and associate the group with your custom role. Ensure that the custom role does not have "cloudsql.instances.export."

3.2 Diagnostic Question 10 Discussion

Your client is legally required to comply with the Payment Card Industry Data Security Standard (PCI-DSS). The client has formal audits already, but the audits are only done periodically. The client needs to **monitor for common violations** to meet those requirements more easily. The client does not want to replace audits but wants to engage in **continuous compliance** and catch violations early.

What would you recommend that this client do?

A. Enable the Security Command Center (SCC) dashboard, asset discovery, and Security Health Analytics in the **Premium tier**. Export or view the PCI-DSS Report from the SCC dashboard's **Compliance tab**.

B. Enable the Security Command Center (SCC) dashboard, asset discovery, and Security Health Analytics in the **Standard tier.** Export or view the PCI-DSS Report from the SCC dashboard's **Compliance tab.**

C. Enable the Security Command Center (SCC) dashboard, asset discovery, and Security Health Analytics in the **Premium tier.** Export or view the PCI-DSS Report from the SCC dashboard's **Vulnerabilities tab**.

D. Enable the Security Command Center (SCC) dashboard, asset discovery, and Security Health Analytics in the **Standard tier.** Export or view the PCI-DSS Report from the SCC dashboard's **Vulnerabilities tab.**

3.2 Diagnostic Question 10 Discussion

Your client is legally required to comply with the Payment Card Industry Data Security Standard (PCI-DSS). The client has formal audits already, but the audits are only done periodically. The client needs to **monitor for common violations** to meet those requirements more easily. The client does not want to replace audits but wants to engage in **continuous compliance** and catch violations early.

What would you recommend that this client do?

A. Enable the Security Command Center (SCC) dashboard, asset discovery, and Security Health Analytics in the **Premium tier**. Export or view the PCI-DSS Report from the SCC dashboard's **Compliance tab**.

B. Enable the Security Command Center (SCC) dashboard, asset discovery, and Security Health Analytics in the **Standard tier.** Export or view the PCI-DSS Report from the SCC dashboard's **Compliance tab.**

C. Enable the Security Command Center (SCC) dashboard, asset discovery, and Security Health Analytics in the **Premium tier.** Export or view the PCI-DSS Report from the SCC dashboard's **Vulnerabilities tab**.

D. Enable the Security Command Center (SCC) dashboard, asset discovery, and Security Health Analytics in the **Standard tier.** Export or view the PCI-DSS Report from the SCC dashboard's **Vulnerabilities tab.**

32 Designing for compliance

Resources to start your journey

[Manage compliance obligations | Architecture Framework | Google Cloud]

[Cloud Compliance & Regulations Resources]

[Assuring Compliance in the Cloud]

[Security Command Center | Google Cloud]

Make sure to...

Enjoy the journey as much as the destination!