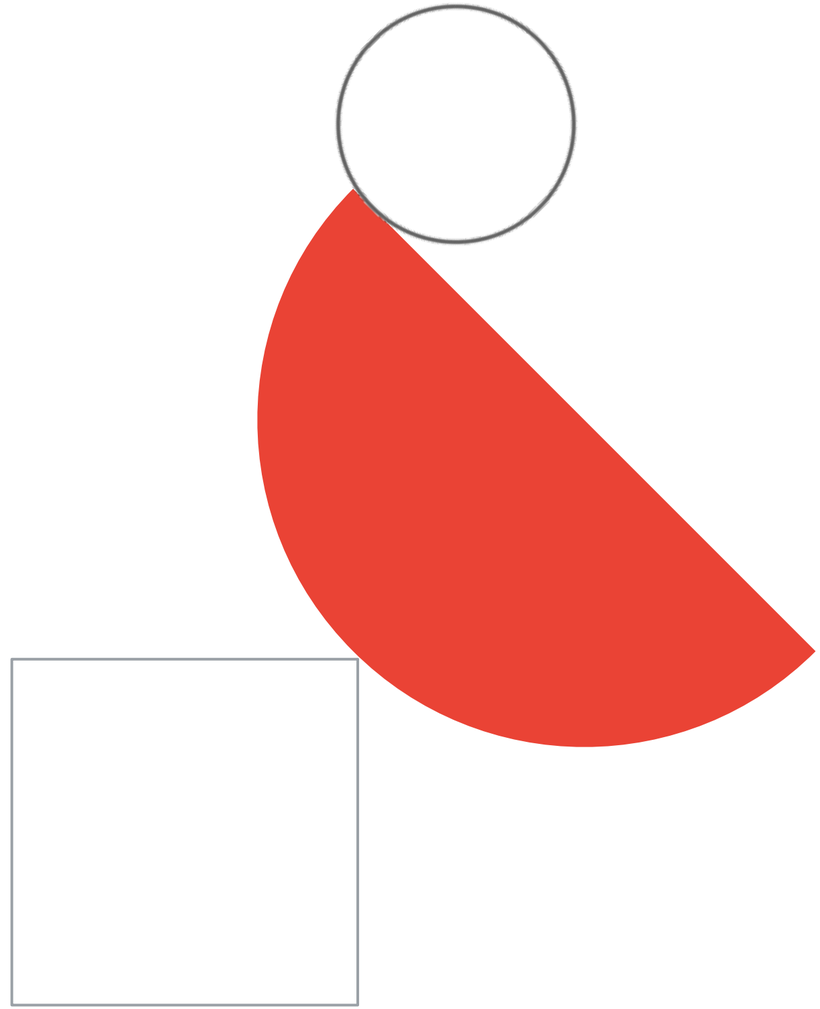
EHR case study analysis




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.

[EHR case study] Diagnostic Question #3

For this question, refer to the EHR Healthcare case study. You are responsible for ensuring that EHR's use of Google Cloud will pass an upcoming privacy compliance audit.

What should you do? (Choose two.)

A. Verify EHR's product usage against the list of compliant products on the Google Cloud compliance page.

B. Advise EHR to execute a Business Associate Agreement (BAA) with Google Cloud.

C. Use Firebase Authentication for EHR's user facing applications.

D. Implement Prometheus to detect and prevent security breaches on EHR's web-based applications.

E. Use GKE private clusters for all Kubernetes workloads.

[EHR case study] Diagnostic Question #3

For this question, refer to the EHR Healthcare case study. You are responsible for ensuring that EHR's use of Google Cloud will pass an upcoming privacy compliance audit.

What should you do? (Choose two.)

A. Verify EHR's product usage against the list of compliant products on the Google Cloud compliance page.

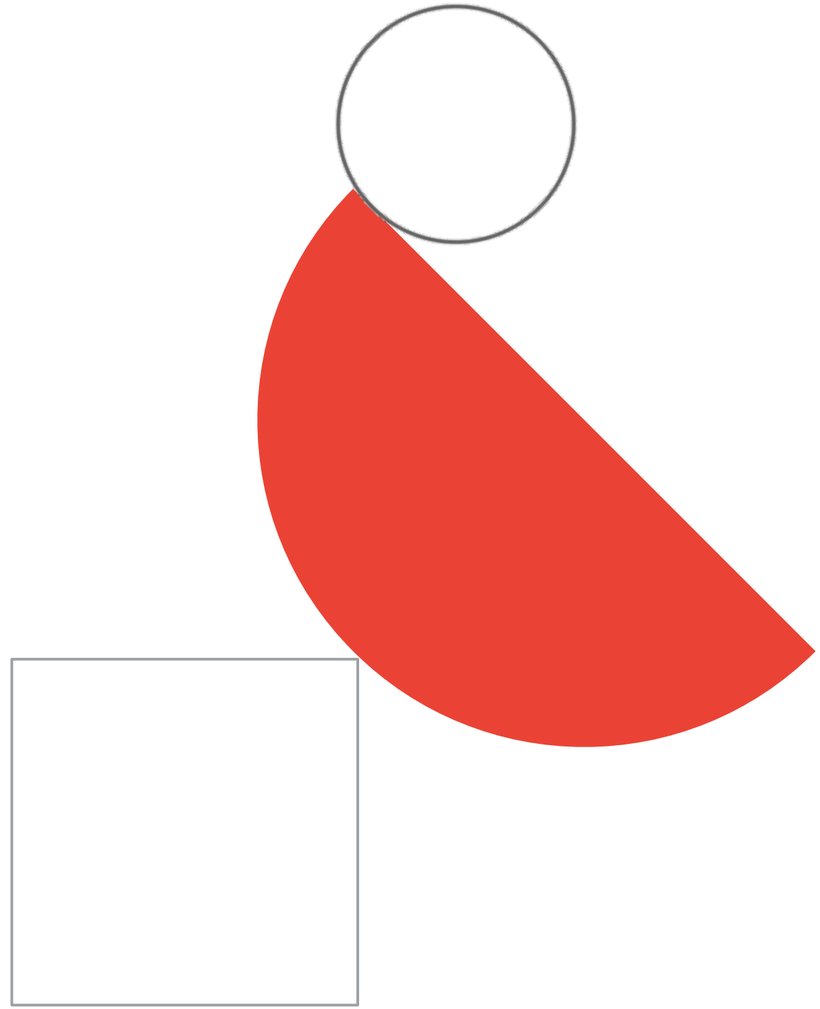
B. Advise EHR to execute a Business Associate Agreement (BAA) with Google Cloud.

C. Use Firebase Authentication for EHR's user facing applications.

D. Implement Prometheus to detect and prevent security breaches on EHR's web-based applications.

E. Use GKE private clusters for all Kubernetes workloads.

[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.