

Preparing for Your Professional Cloud Architect Journey

Module 2: Managing and Provisioning
a Solution Infrastructure

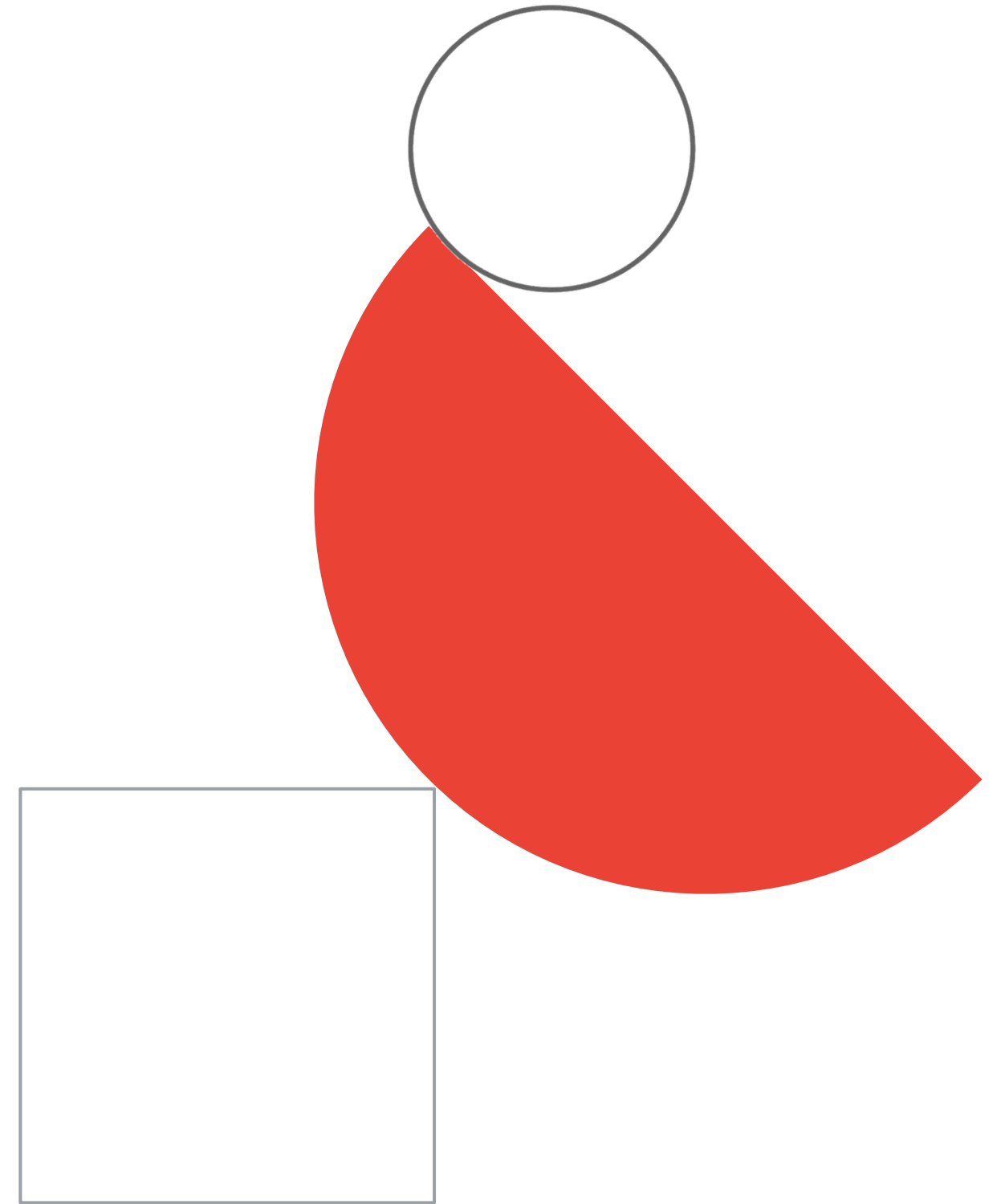


Module agenda

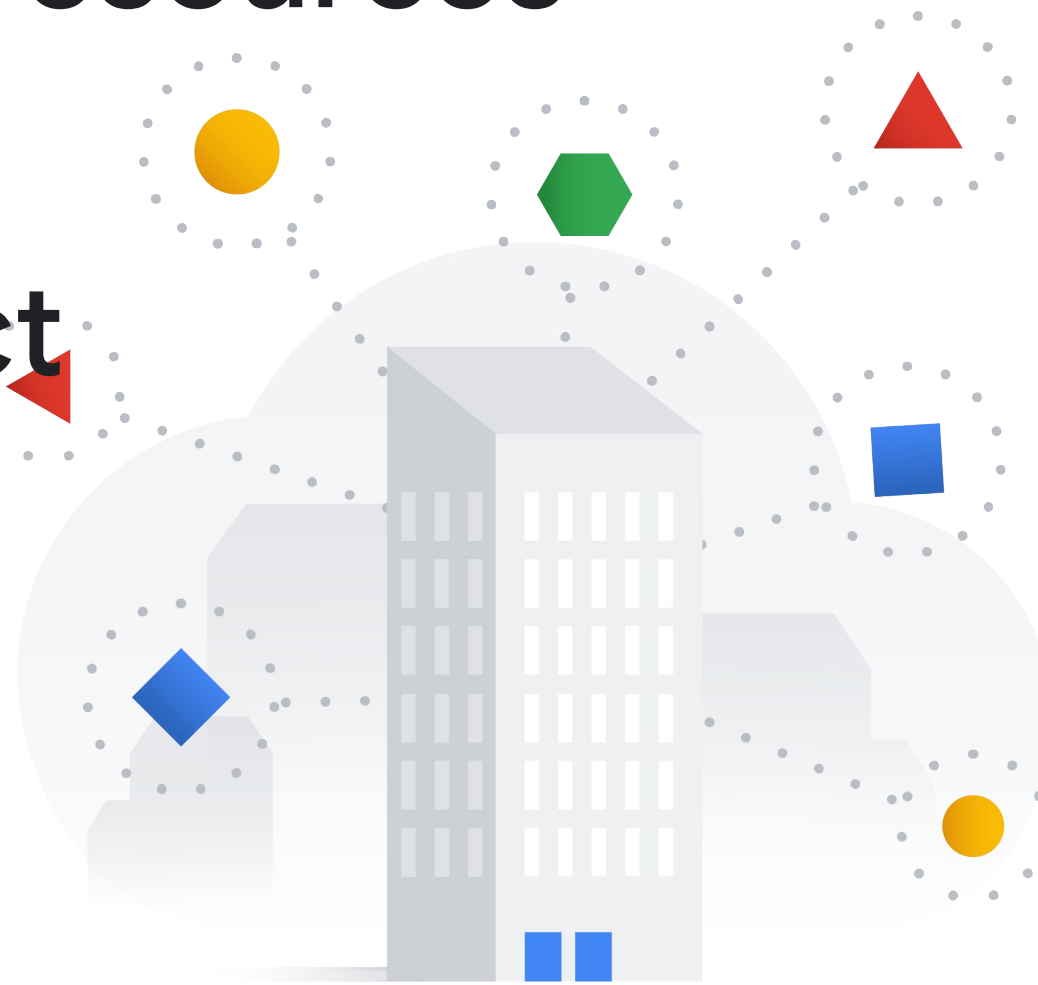
- 01 Provisioning a cloud solution to meet Cymbal Direct's requirements
- 02 Diagnostic questions
- 03 Review and study planning



Provisioning a cloud solution to meet Cymbal Direct's requirements



Your role in provisioning resources for Cymbal Direct



- Configuring network topologies
- Configuring individual storage systems
- Configuring compute systems

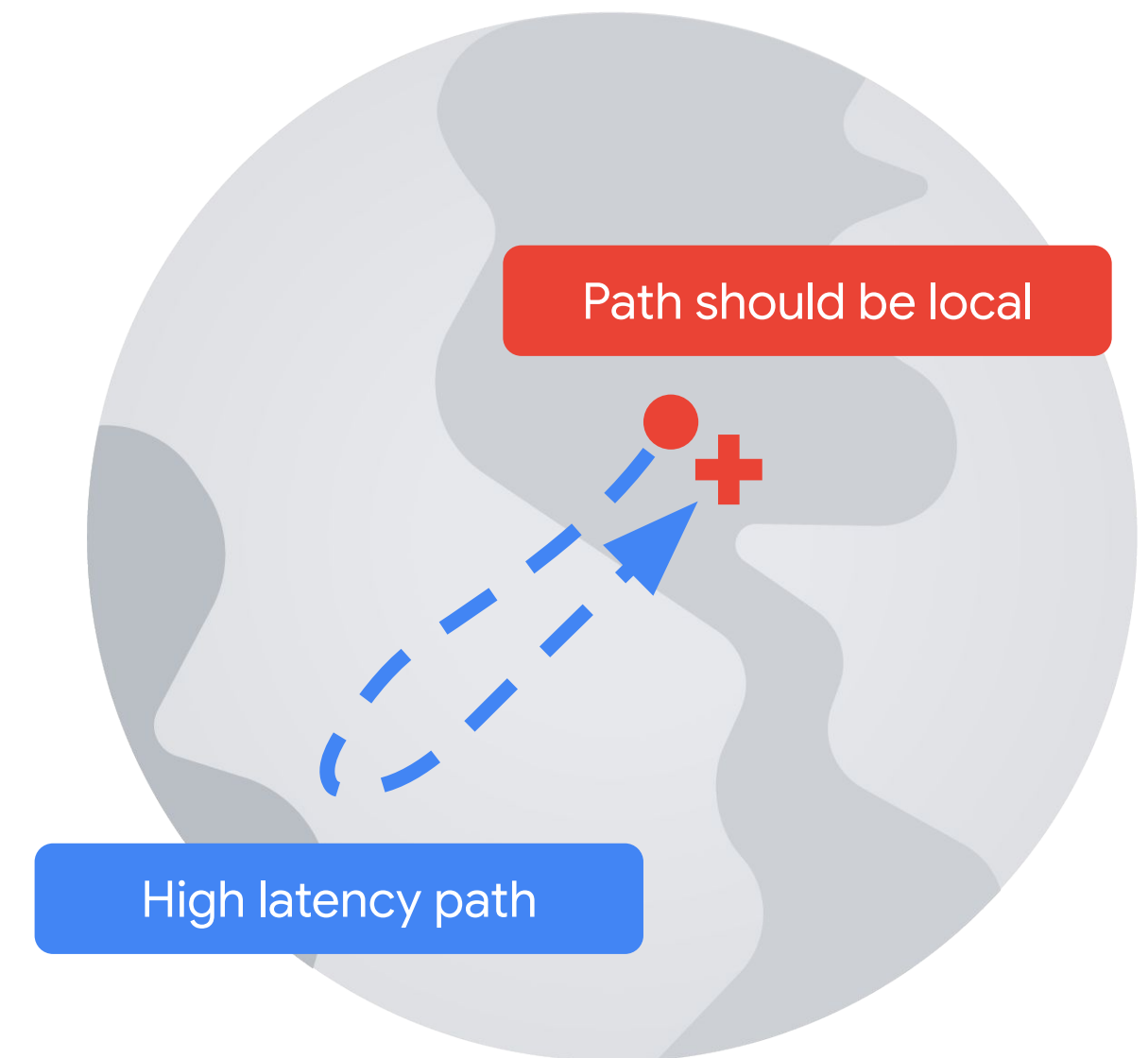




What configuration choices will you make as
a **Professional Cloud Architect**?

Issues with the Delivery by Drone Initiative

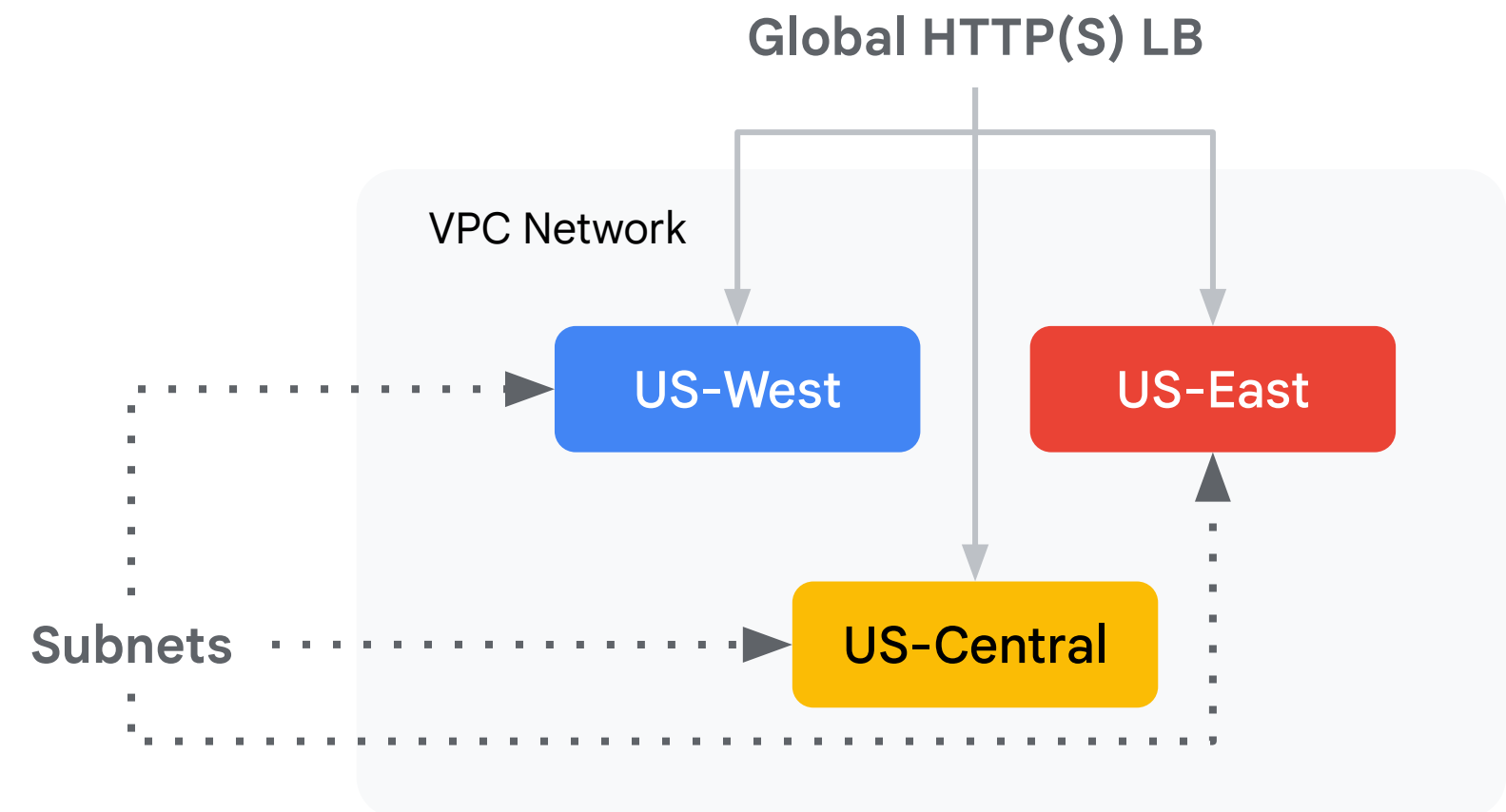
- Pilots complain about occasional unexpected latency.
- The service was initially set up using DNS load balancing.
- Some traffic is sent to resources further away.



Provisioning networking for Delivery by Drone

You decided to:

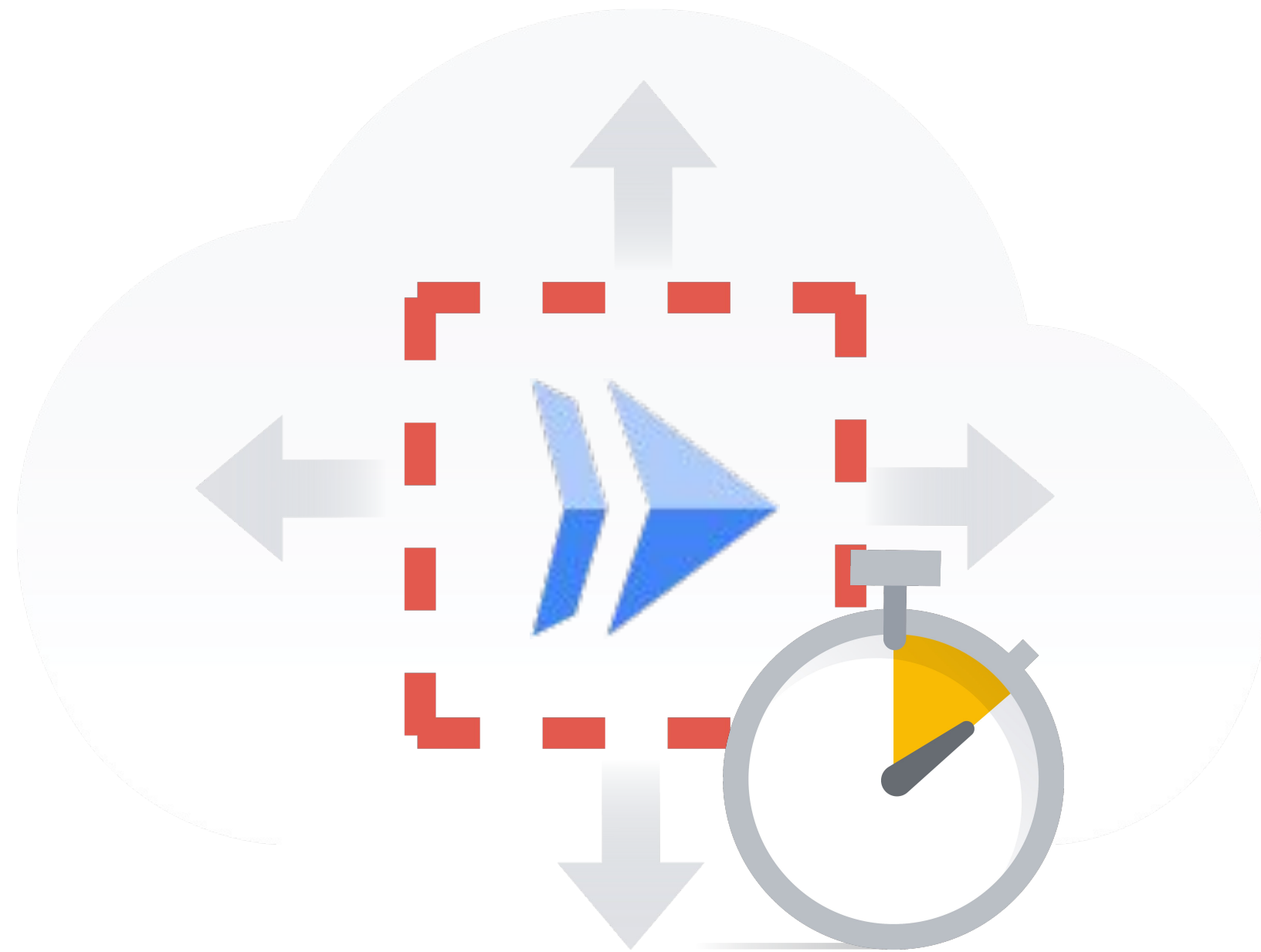
- Move to a Global HTTP(S) Load Balancer
- Use a Custom Network
- Configure subnets only in nearby regions



Configuring an organization policy constraint

[Organization policy constraints](#)
[| Resource Manager](#)
[Documentation | Google Cloud](#)

- You set `'constraints/compute.skipDefaultNetworkCreation'` to `'true'`
- You also configured `'constraints/compute.restrictSharedVpcSubnetworks'` to subnets in regions near where the drones are being deployed for beta deliveries.



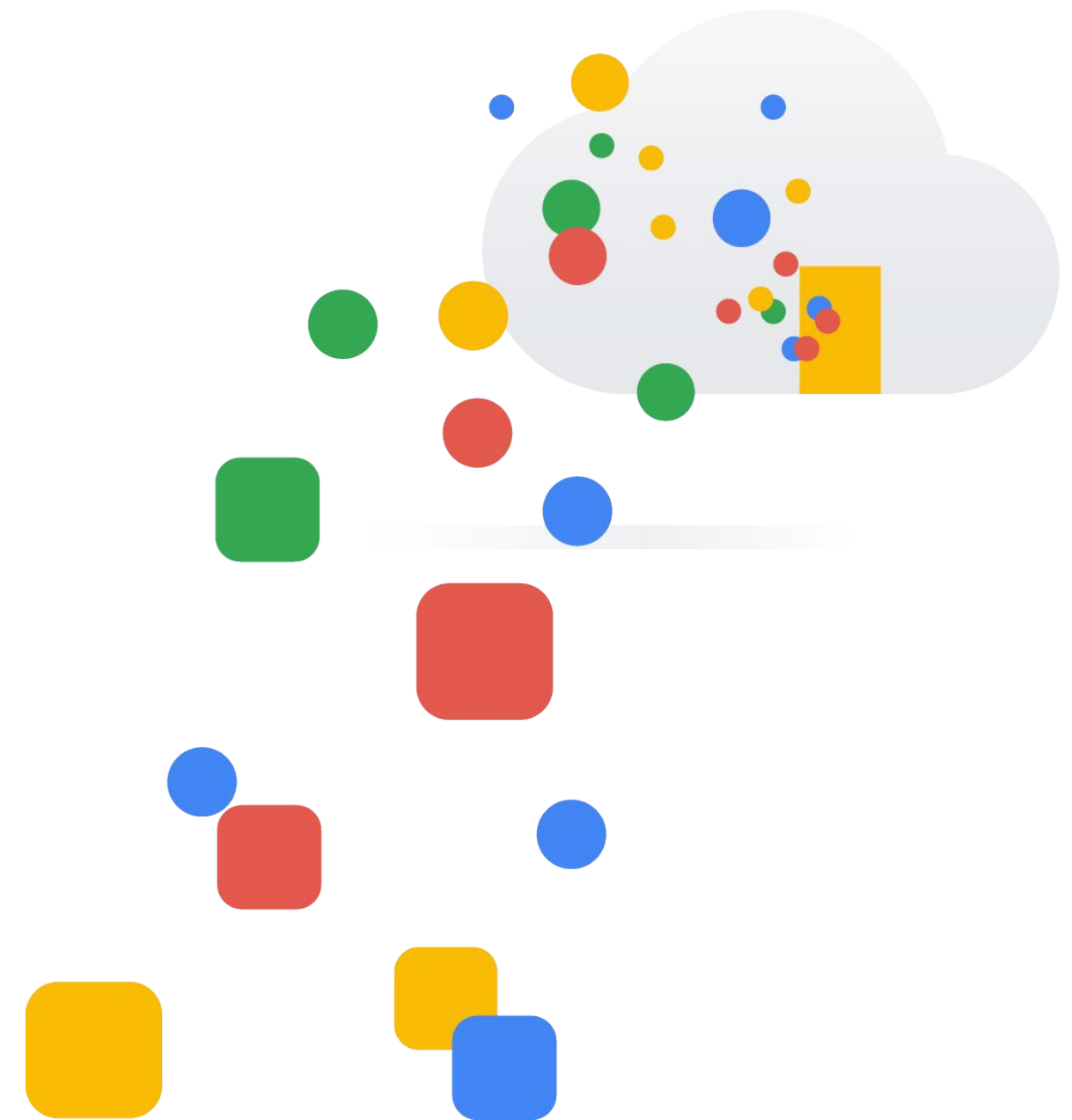
Cymbal Direct's compute configuration

Cloud Run lets you scale with minimal latency.
You configure a high number of minimum
instances to reduce cold starts.

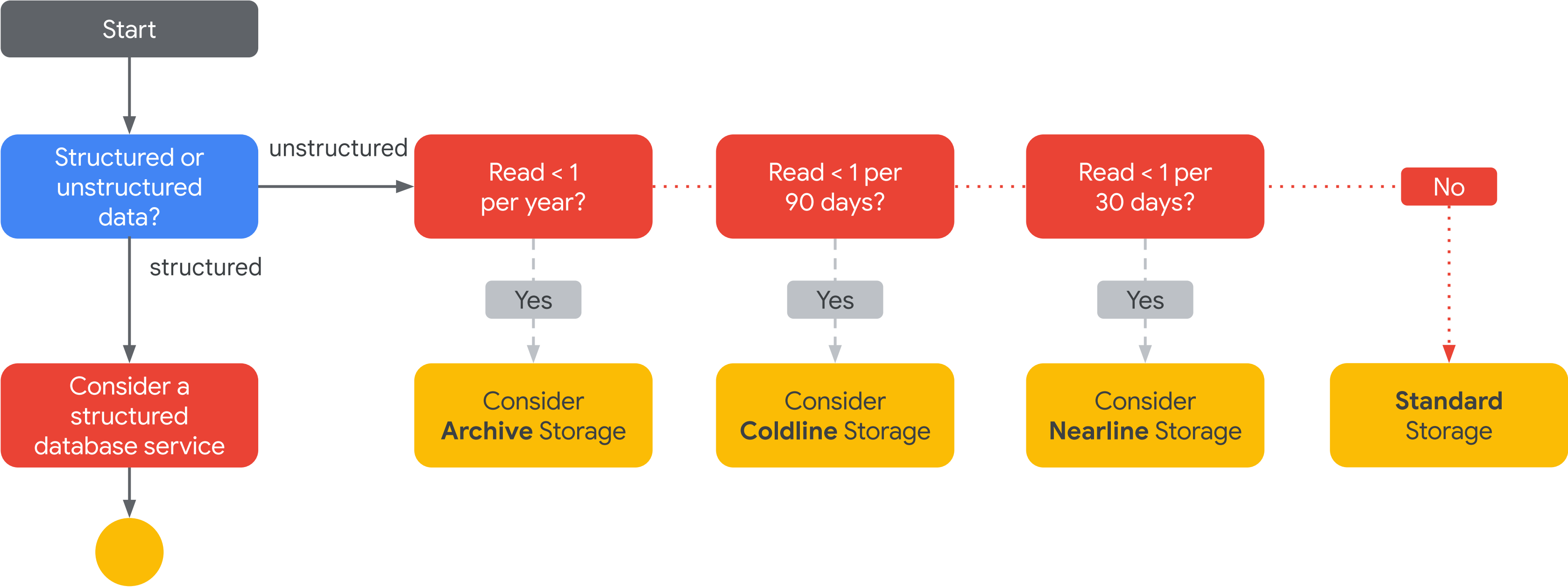
Configuration options for Cymbal Direct's other applications

For deployments that have stateful information such as databases, or where the developer prefers to preserve their existing workflow, you've chosen to leverage GKE.

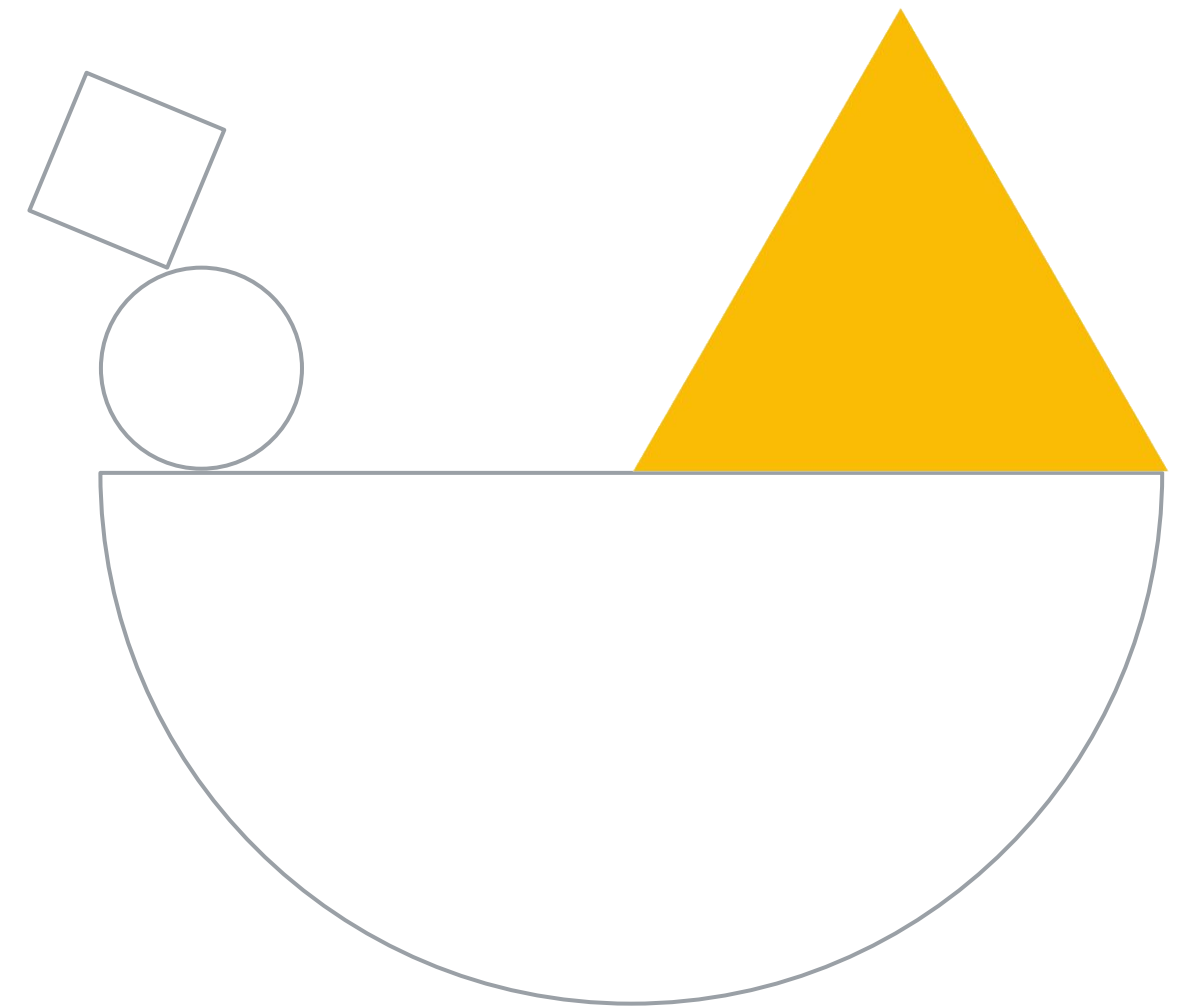
For their Compute Engine instances, you've decided to use managed instance groups with Shielded VMs.



Cymbal Direct's storage configuration



Diagnostic questions

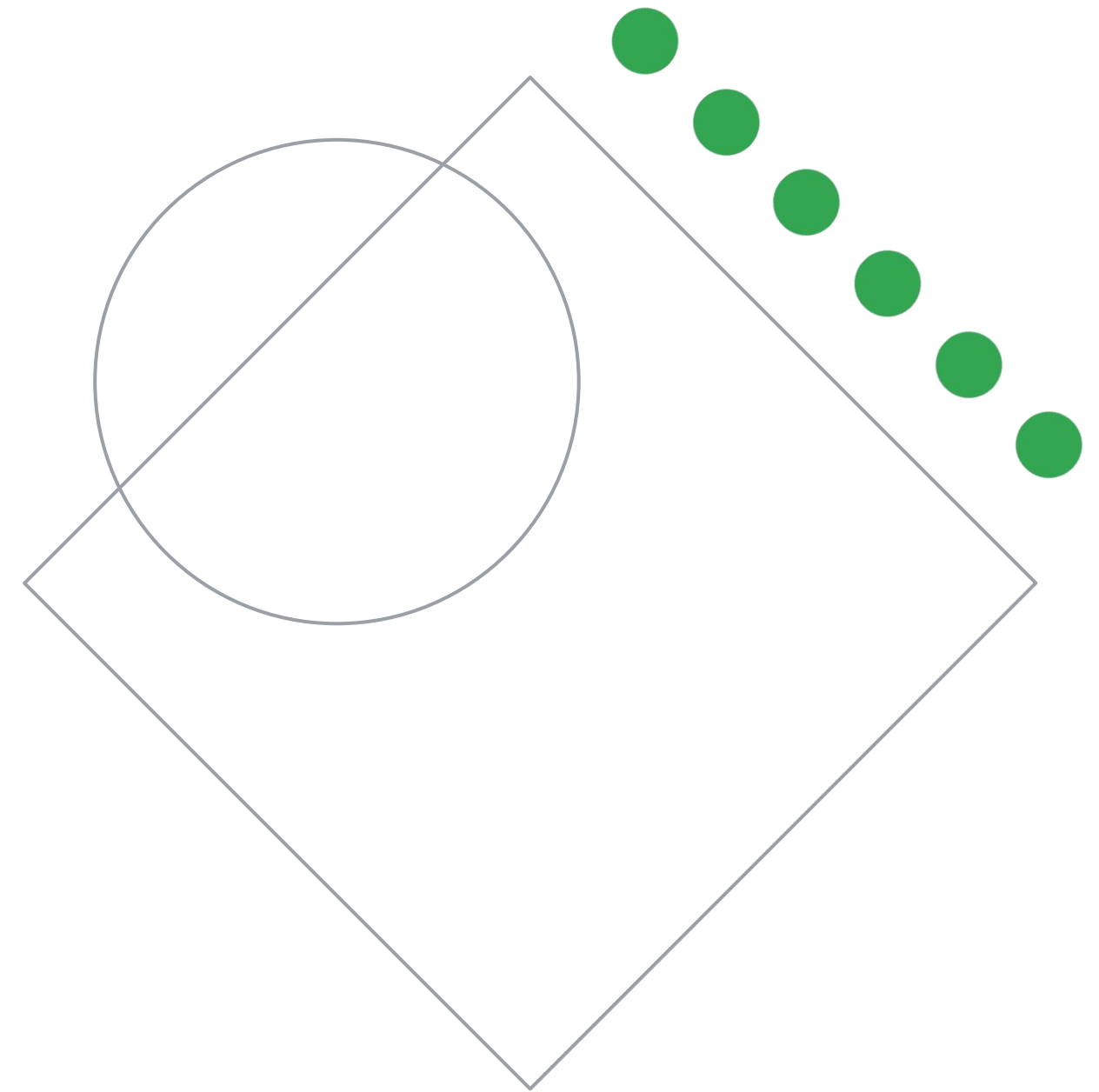


Please complete the diagnostic questions now

- Forms are provided for you to answer the diagnostic questions
- The instructor will provide you a link to the forms
- The diagnostic questions are also available in the workbook

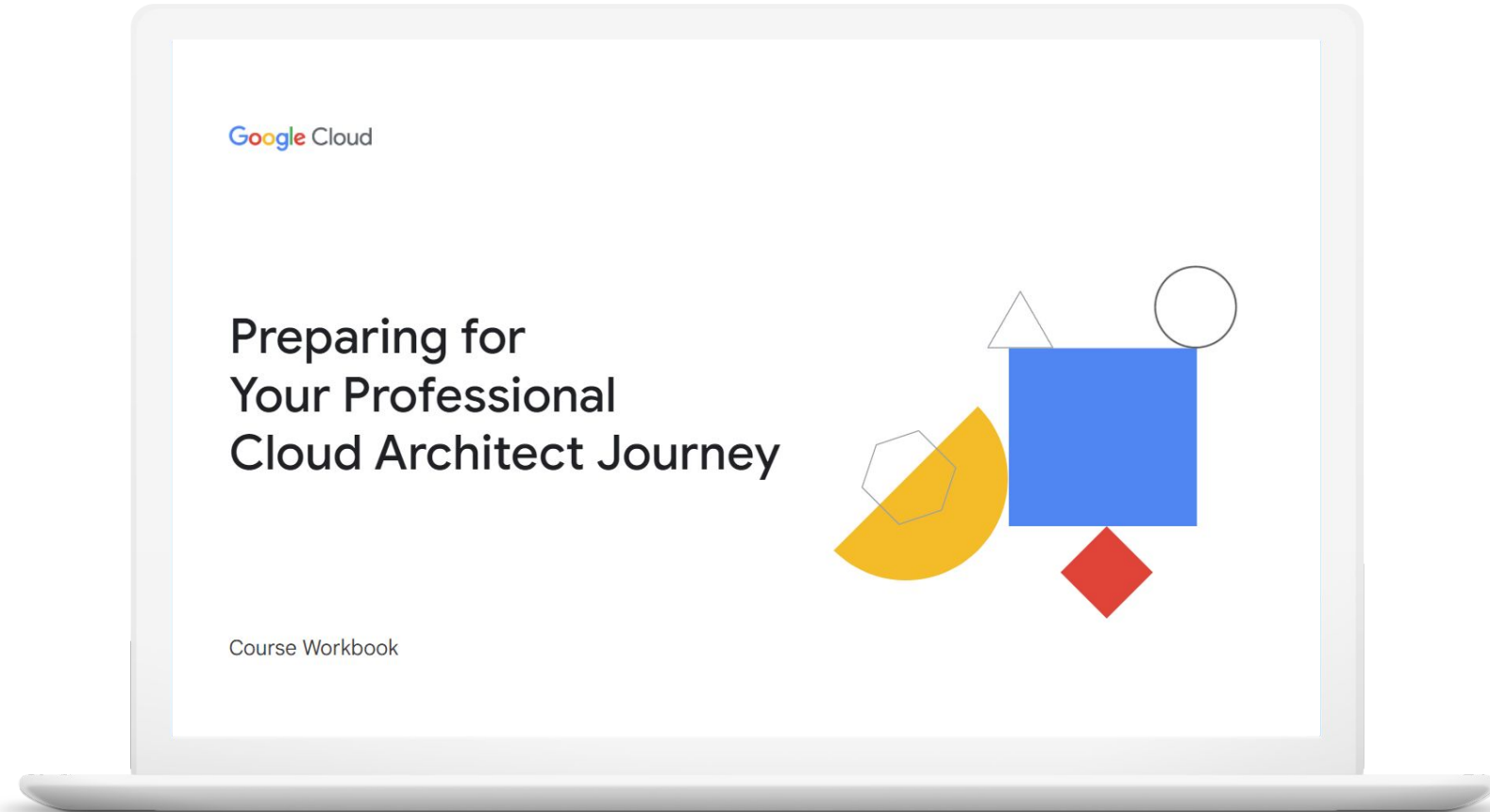


Review and study planning



Your study plan:

Managing and provisioning a solution infrastructure



2.1

Configuring network topologies

2.2

Configuring individual storage systems

2.3

Configuring compute systems

2.1 | Configuring network topologies

Considerations include:

- Extending to on-premises environments (hybrid networking)
- Extending to a multicloud environment that may include Google Cloud to Google Cloud communication
- Security protection (e.g. intrusion protection, access control, firewalls)

2.1 | Diagnostic Question 01 Discussion



Cymbal Direct must meet compliance requirements. You need to ensure that employees with valid accounts **cannot access their VPC network from locations outside of its secure corporate network**, including from home. You also want a high degree of **visibility into network traffic** for **auditing and forensics** purposes.

What should you do?

- A. Ensure that all users install **Cloud VPN**. Enable VPC Flow Logs for the networks you need to monitor.
- B. Enable **VPC Service Controls**, define a network perimeter to restrict access to authorized networks, and **enable VPC Flow Logs** for the networks you need to monitor.
- C. Enable **Identity-Aware Proxy (IAP)** to allow users to access services securely. Use Google Cloud's operations suite to view audit logs for the networks you need to monitor.
- D. Enable **VPC Service Controls**, and use **Google Cloud's operations suite** to view audit logs for the networks you need to monitor.

2.1 | Diagnostic Question 01 Discussion



Cymbal Direct must meet compliance requirements. You need to ensure that employees with valid accounts **cannot access their VPC network from locations outside of its secure corporate network**, including from home. You also want a high degree of **visibility into network traffic** for **auditing and forensics** purposes.

What should you do?

- A. Ensure that all users install **Cloud VPN**. Enable VPC Flow Logs for the networks you need to monitor.
- B. Enable **VPC Service Controls**, define a network perimeter to restrict access to authorized networks, and **enable VPC Flow Logs** for the networks you need to monitor.
- C. Enable **Identity-Aware Proxy (IAP)** to allow users to access services securely. Use Google Cloud's operations suite to view audit logs for the networks you need to monitor.
- D. Enable **VPC Service Controls**, and use **Google Cloud's operations suite** to view audit logs for the networks you need to monitor.

2.1 | Configuring network topologies

Resources to start your journey

[VPC network overview | Google Cloud](#)

[Choosing a Network Connectivity product | Google Cloud](#)

[Cloud VPN overview](#)

[Best practices | Cloud Interconnect](#)

[Options for connecting to multiple VPC networks | Cloud Interconnect Best practices for enterprise organizations |](#)

[Documentation | Google Cloud](#)



2.2 | Configuring individual storage systems

Considerations include:

- Data storage allocation
- Data processing/compute provisioning
- Security and access management
- Network configuration for data transfer and latency
- Data retention and data life cycle management
- Data growth planning

2.2 | Diagnostic Question 03 Discussion



Cymbal Direct's user account management app allows users to delete their accounts whenever they like. Cymbal Direct also has a very generous **60-day return policy** for users. The customer service team wants to make sure that they can still refund or replace items for a customer **even if the customer's account has been deleted**.

What can you do to ensure that the customer service team has **access to relevant account information**?

- A. **Temporarily disable the account for 30 days.** Export account information to Cloud Storage, and enable lifecycle management to **delete the data in 60 days**.
- B. Ensure that the user clearly understands that after they delete their account, **all their information will also be deleted**. Remind them to download a copy of their order history and account information before deleting their account. Have the support agent copy any open or recent orders to a shared spreadsheet.
- C. **Restore a previous copy** of the user information database from a snapshot. Have a database administrator capture needed information about the customer.
- D. **Disable the account.** Export account information to Cloud Storage. Have the customer service team permanently **delete the data after 30 days**.

2.2 | Diagnostic Question 03 Discussion



Cymbal Direct's user account management app allows users to delete their accounts whenever they like. Cymbal Direct also has a very generous **60-day return policy** for users. The customer service team wants to make sure that they can still refund or replace items for a customer **even if the customer's account has been deleted**.

What can you do to ensure that the customer service team has **access to relevant account information**?

- A. **Temporarily disable the account for 30 days.** Export account information to Cloud Storage, and enable lifecycle management to **delete the data in 60 days**.
- B. Ensure that the user clearly understands that after they delete their account, **all their information will also be deleted**. Remind them to download a copy of their order history and account information before deleting their account. Have the support agent copy any open or recent orders to a shared spreadsheet.
- C. **Restore a previous copy** of the user information database from a snapshot. Have a database administrator capture needed information about the customer.
- D. **Disable the account.** Export account information to Cloud Storage. Have the customer service team permanently **delete the data after 30 days**.

2.2 | Configuring individual storage systems

Resources to start your journey

[Select and implement a storage strategy | Architecture Framework | Google Cloud](#)

[Best practices for Cloud Storage](#)

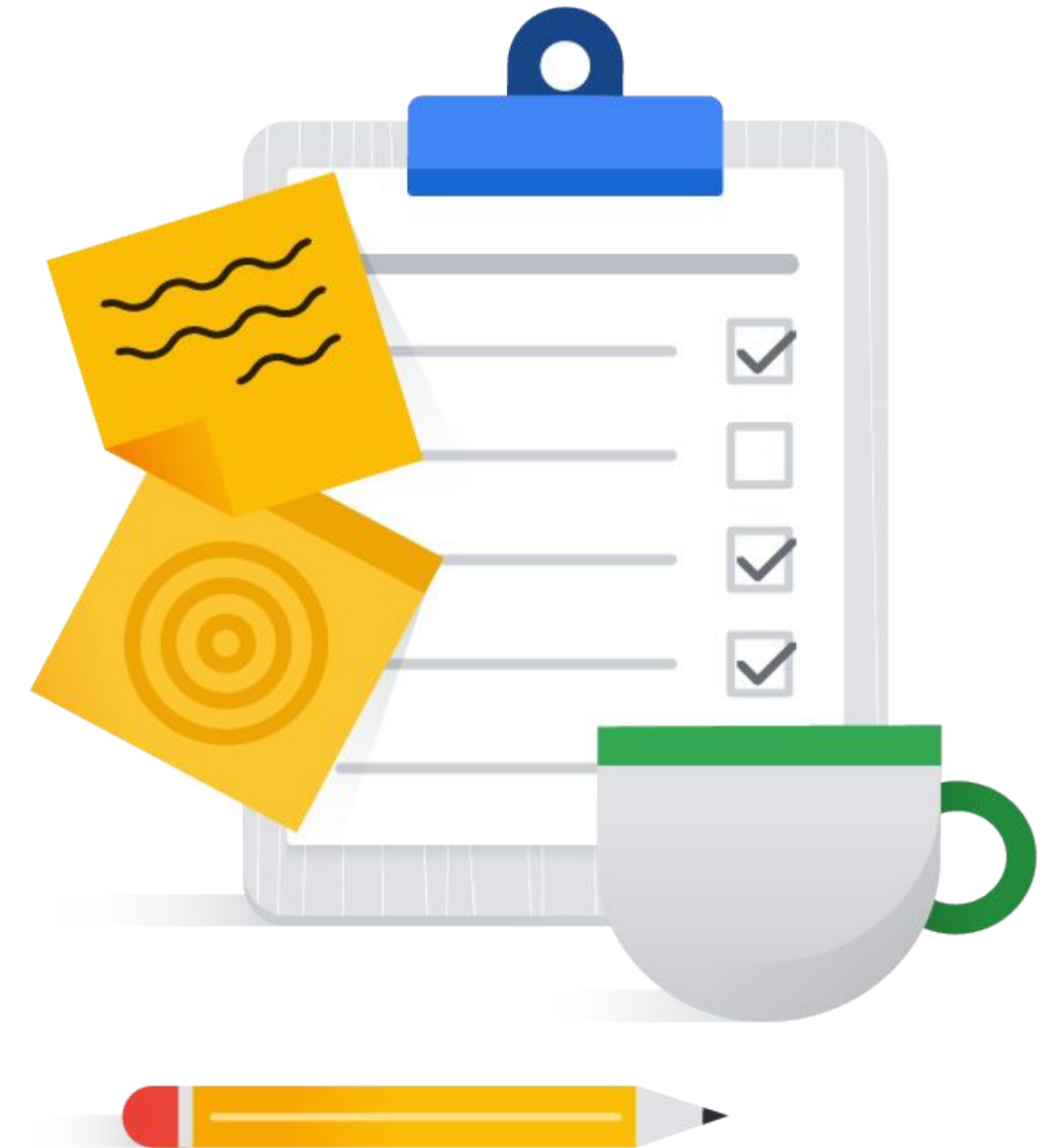
[Enterprise tier | Filestore | Google Cloud](#)

[Design an optimal storage strategy for your cloud workload](#)

[Storage options | Compute Engine Documentation | Google Cloud](#)

[Cloud Storage Options | Google Cloud](#)

[Object storage vs block storage vs file storage: which should you choose? | Google Cloud Blog](#)



2.3 | Configuring compute systems

Considerations include:

- Compute resource provisioning
- Compute volatility configuration (preemptible vs. standard)
- Network configuration for compute resources (Google Compute Engine, Google Kubernetes Engine, serverless networking)
- Infrastructure orchestration, resource configuration, and patch management
- Container orchestration

2.3 | Diagnostic Question 04 Discussion



Cymbal Direct wants to create a **pipeline to automate the building of new application releases**.

What sequence of steps should you use?

- A. Set up a source code repository. **Run unit tests.** Check in code. Deploy. Build a Docker container.
- B. **Check in code.** Set up a source code repository. Run unit tests. Deploy. Build a Docker container.
- C. **Set up a source code repository. Check in code. Run unit tests. Build a Docker container. Deploy.**
- D. **Run unit tests.** Deploy. Build a Docker container. Check in code. Set up a source code repository.

2.3 | Diagnostic Question 04 Discussion



Cymbal Direct wants to create a **pipeline to automate the building of new application releases**.

What sequence of steps should you use?

- A. Set up a source code repository. **Run unit tests.** Check in code. Deploy. Build a Docker container.
- B. **Check in code.** Set up a source code repository. Run unit tests. Deploy. Build a Docker container.
- C. **Set up a source code repository. Check in code. Run unit tests. Build a Docker container. Deploy.**
- D. **Run unit tests.** Deploy. Build a Docker container. Check in code. Set up a source code repository.

2.3 | Diagnostic Question 08 Discussion



Cymbal Direct wants a **layered approach** to security when setting up Compute Engine instances.

What are some options you could use to **make your Compute Engine instances more secure**?

- A. Use **labels** to allow traffic only from certain sources and ports. Turn on Secure boot and vTPM.
- B. Use **labels** to allow traffic only from certain sources and ports. Use a Compute Engine service account.
- C. Use **network tags** to allow traffic only from certain sources and ports. Turn on **Secure boot and vTPM**.
- D. Use **network tags** to allow traffic only from certain sources and ports. Use a **Compute Engine service account**.

2.3 | Diagnostic Question 08 Discussion



Cymbal Direct wants a **layered approach** to security when setting up Compute Engine instances.

What are some options you could use to **make your Compute Engine instances more secure**?

- A. Use **labels** to allow traffic only from certain sources and ports. Turn on Secure boot and vTPM.
- B. Use **labels** to allow traffic only from certain sources and ports. Use a Compute Engine service account.
- C. Use **network tags** to allow traffic only from certain sources and ports. Turn on **Secure boot and vTPM**.
- D. Use **network tags** to allow traffic only from certain sources and ports. Use a **Compute Engine service account**.

2.3 Diagnostic Question 10 Discussion



You need to deploy a **load balancer for a web-based application with multiple backends in different regions.**

You want to direct traffic to the backend closest to the end user, but also to different backends **based on the URL the user is accessing.**

Which of the following could be used to implement this?

- A. The request is **received by the global external HTTP(S) load balancer.** A global forwarding rule sends the request to a target proxy, which checks the URL map and selects the backend service. The backend service sends the request to Compute Engine instance groups in multiple regions.
- B. The request is **matched by a URL map** and then sent to a **global external HTTP(S) load balancer.** A global forwarding rule sends the request to a target proxy, which selects a backend service. The backend service sends the request to Compute Engine instance groups in multiple regions.
- C. The request is **received by the SSL proxy load balancer,** which uses a global forwarding rule to check the URL map, then sends the request to a backend service. The request is processed by Compute Engine instance groups in multiple regions.
- D. The request is **matched by a URL map** and then sent to a **SSL proxy load balancer.** A global forwarding rule sends the request to a target proxy, which selects a backend service and sends the request to Compute Engine instance groups in multiple regions.

2.3 | Diagnostic Question 10 Discussion



You need to deploy a **load balancer for a web-based application with multiple backends in different regions.**

You want to direct traffic to the backend closest to the end user, but also to different backends **based on the URL the user is accessing.**

Which of the following could be used to implement this?

- A. The request is **received by the global external HTTP(S) load balancer.** A global forwarding rule sends the request to a target proxy, which checks the URL map and selects the backend service. The backend service sends the request to Compute Engine instance groups in multiple regions.
- B. The request is **matched by a URL map** and then sent to a **global external HTTP(S) load balancer.** A global forwarding rule sends the request to a target proxy, which selects a backend service. The backend service sends the request to Compute Engine instance groups in multiple regions.
- C. The request is **received by the SSL proxy load balancer,** which uses a global forwarding rule to check the URL map, then sends the request to a backend service. The request is processed by Compute Engine instance groups in multiple regions.
- D. The request is **matched by a URL map** and then sent to a **SSL proxy load balancer.** A global forwarding rule sends the request to a target proxy, which selects a backend service and sends the request to Compute Engine instance groups in multiple regions.

2.3 | Configuring compute systems

Resources to start your journey

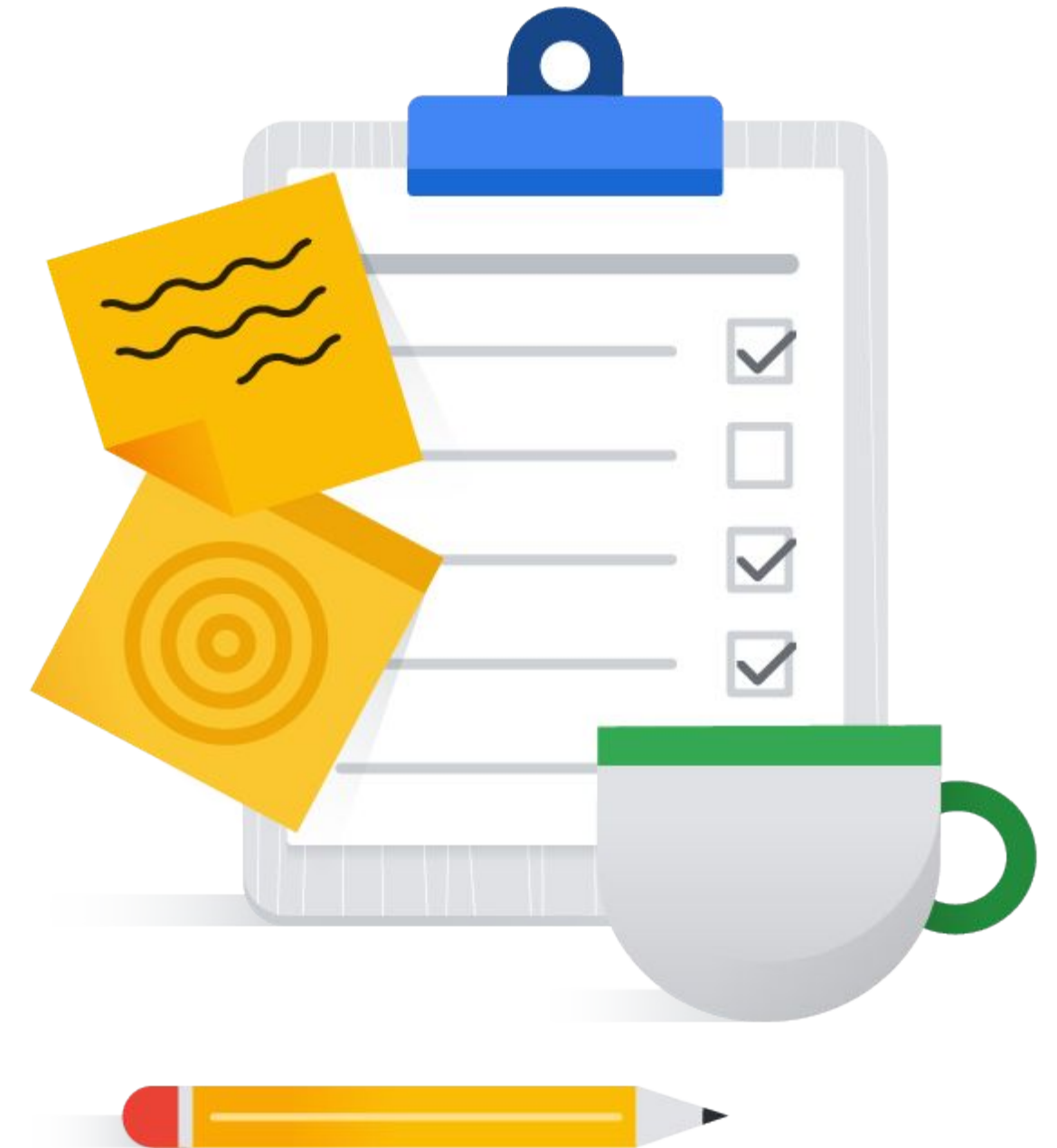
[Choose a Compute Engine deployment strategy for your workload](#)

[Google Kubernetes Engine documentation](#)

[General development tips | Cloud Run Documentation](#)

[Choosing the right compute option in GCP: a decision tree | Google Cloud Blog](#)

[Google Kubernetes Engine vs Cloud Run: Which should you use?](#)



Knowledge Check 1

Which Storage Class should you use for data that is going to be accessed at least once every two weeks?

- A. Standard
- B. Nearline
- C. Coldline
- D. Archive



Knowledge Check 1

Which Storage Class should you use for data that is going to be accessed at least once every two weeks?

A. Standard

B. Nearline

C. Coldline

D. Archive



Knowledge Check 2

Which network configuration would ensure low latency for Chicago based drone pilots?

- A. Only deploy resources to Regions in Europe
- B. Only deploy resources to Regions in Asia
- C. Only deploy resources to Regions in the US
- D. Deploy resources globally



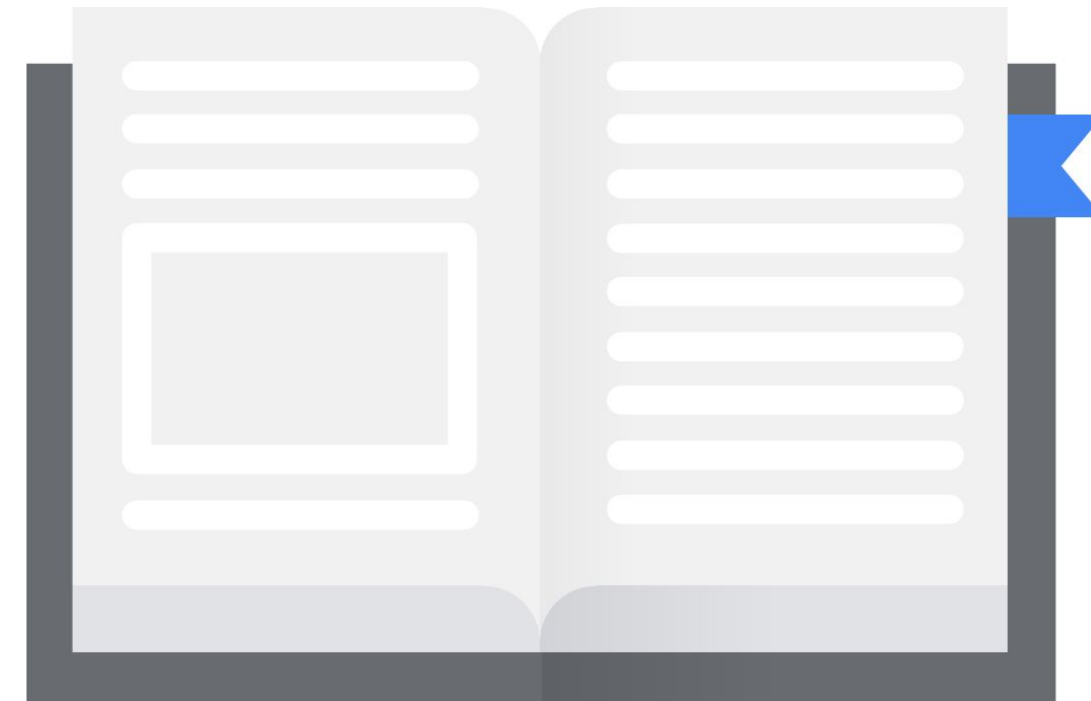
Knowledge Check 2

Which network configuration would ensure low latency for Chicago based drone pilots?

- A. Only deploy resources to Regions in Europe
- B. Only deploy resources to Regions in Asia
- C. Only deploy resources to Regions in the US
- D. Deploy resources globally



Appendix



2.1 | Diagnostic Question 02 Discussion

You are working with a client who has built a secure messaging application. The application is open source and consists of two components. The first component is a **web app, written in Go, which is used to register an account and authorize the user's IP address.** The second is an **encrypted chat protocol that uses TCP to talk to the backend chat servers running Debian. If the client's IP address doesn't match the registered IP address, the application is designed to terminate their session.** The number of clients using the service varies greatly based on time of day, and the client wants to be able to **easily scale** as needed.

What should you do?

- A. Deploy the web application using the **App Engine standard environment** using a global external HTTP(S) load balancer and a network endpoint group. **Use an unmanaged instance group** for the backend chat servers. Use an **external network load balancer to load-balance traffic** across the backend chat servers.
- B. Deploy the web application using the **App Engine flexible environment** using a global external HTTP(S) load balancer and a network endpoint group. **Use an unmanaged instance group** for the backend chat servers. Use an **external network load balancer to load-balance traffic** across the backend chat servers.
- C. Deploy the web application using the **App Engine standard environment** using a global external HTTP(S) load balancer and a network endpoint group. **Use a managed instance group** for the backend chat servers. **Use a global SSL proxy load balancer to load-balance traffic** across the backend chat servers.
- D. Deploy the web application using the **App Engine standard environment** with a global external HTTP(S) load balancer and a network endpoint group. **Use a managed instance group** for the backend chat servers. Use an **external network load balancer to load-balance traffic** across the backend chat servers.



2.3 | Diagnostic Question 05 Discussion



Your existing application runs on **Ubuntu Linux VMs** in an **on-premises hypervisor**. You want to deploy the application to Google Cloud with **minimal refactoring**.

What should you do?

- A. Set up a **Google Kubernetes Engine (GKE) cluster**, and then create a deployment with an autoscaler.
- B. Isolate the core features that the application provides. Use **Cloud Run** to deploy each feature independently as a microservice.
- C. Use X or Partner Interconnect to **connect the on-premises network where your application is running to your VPC**. Configure an endpoint for a global external HTTP(S) load balancer that connects to the existing VMs.
- D. Write Terraform scripts to deploy the application as **Compute Engine instances**.

2.3 | Diagnostic Question 06 Discussion



Cymbal Direct needs to use a **tool to deploy its infrastructure**. You want something that allows for **repeatable deployment processes, uses a declarative language, and allows parallel deployment**. You also want to deploy **infrastructure as code** on Google Cloud and other cloud providers.

- A. Automate the deployment with **Terraform scripts**.
- B. Automate the deployment using scripts containing **gcloud commands**.
- C. Use **Google Kubernetes Engine (GKE)** to create deployments and manifests for your applications.
- D. Develop in **Docker containers** for portability and ease of deployment.

What should you do?

2.3 | Diagnostic Question 07 Discussion



Cymbal Direct wants to allow partners to **make orders programmatically**, without having to speak on the phone with an agent.

What should you consider when **designing the API**?

- A. The API backend should be **loosely** coupled. Clients should not be required to know too many details of the services they use. REST APIs using **gRPC** should be used for all external APIs.
- B. The API backend should be **tightly** coupled. Clients should know a significant amount about the services they use. REST APIs using **gRPC** should be used for all external APIs.
- C. The API backend should be **loosely** coupled. Clients should not be required to know too many details of the services they use. For REST APIs, **HTTP(S)** is the most common protocol.
- D. The API backend should be **tightly** coupled. Clients should know a significant amount about the services they use. For REST APIs, **HTTP(S)** is the most common protocol used.

2.3 | Diagnostic Question 09 Discussion



You have deployed your frontend web application in Kubernetes. Based on historical use, you need **three pods to handle normal demand**. Occasionally your load will roughly **double**. A load balancer is already in place.

How could you configure your environment to efficiently meet that demand?

- A. Edit your **pod's configuration file** and change the number of replicas to six.
- B. Edit your **deployment's configuration file** and change the number of replicas to six.
- C. Use the "**kubectl autoscale**" command to change the **pod's** maximum number of instances to six.
- D. Use the "**kubectl autoscale**" command to change the **deployment's** maximum number of instances to six.