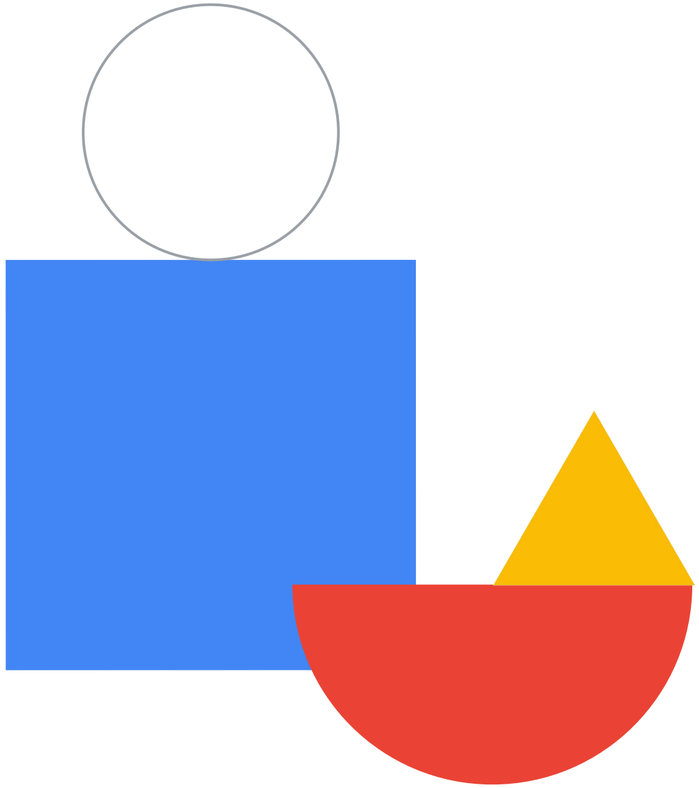
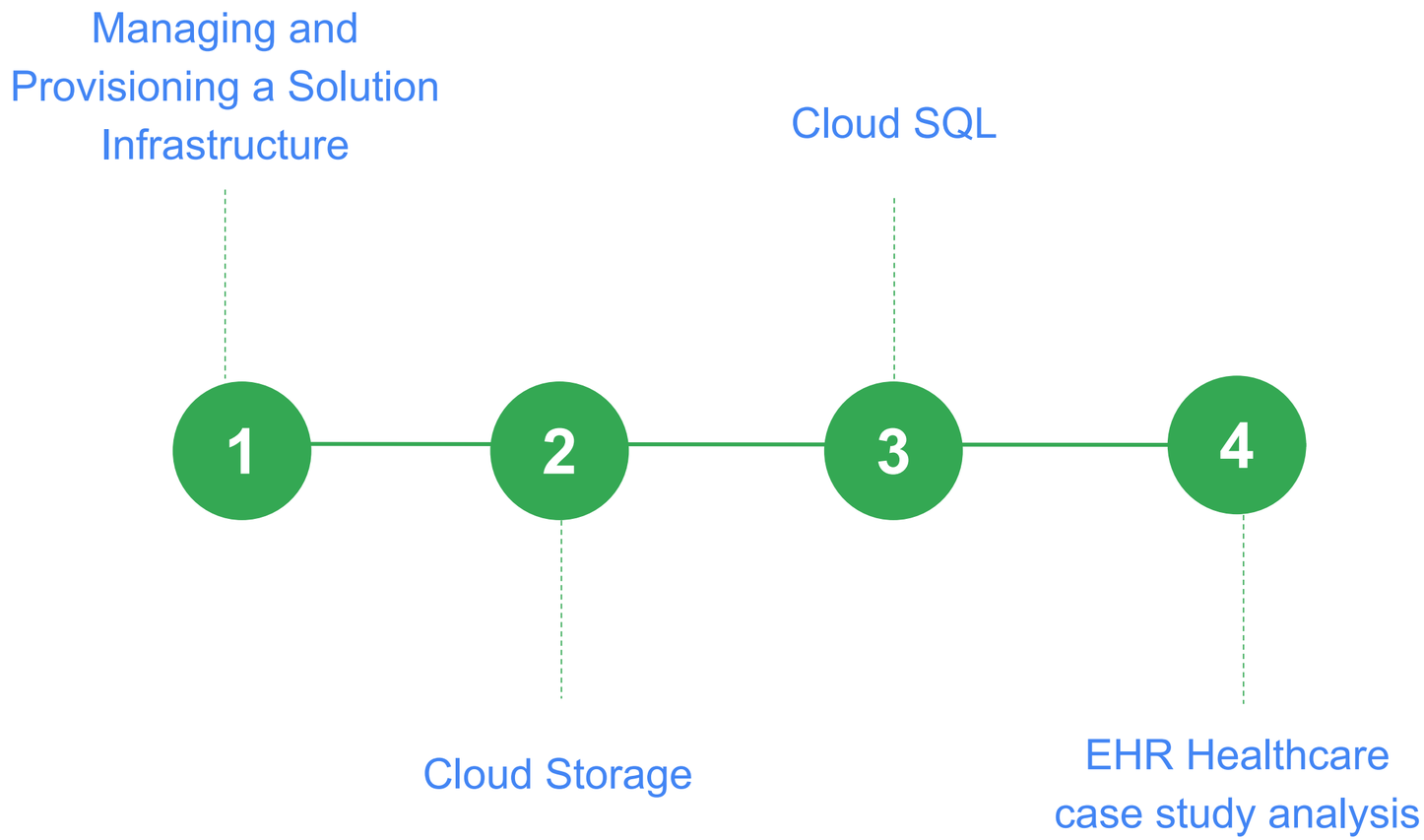
Google Cloud



Preparing for Your Professional Cloud Architect Journey

Module 2: Managing and Provisioning a Solution Infrastructure

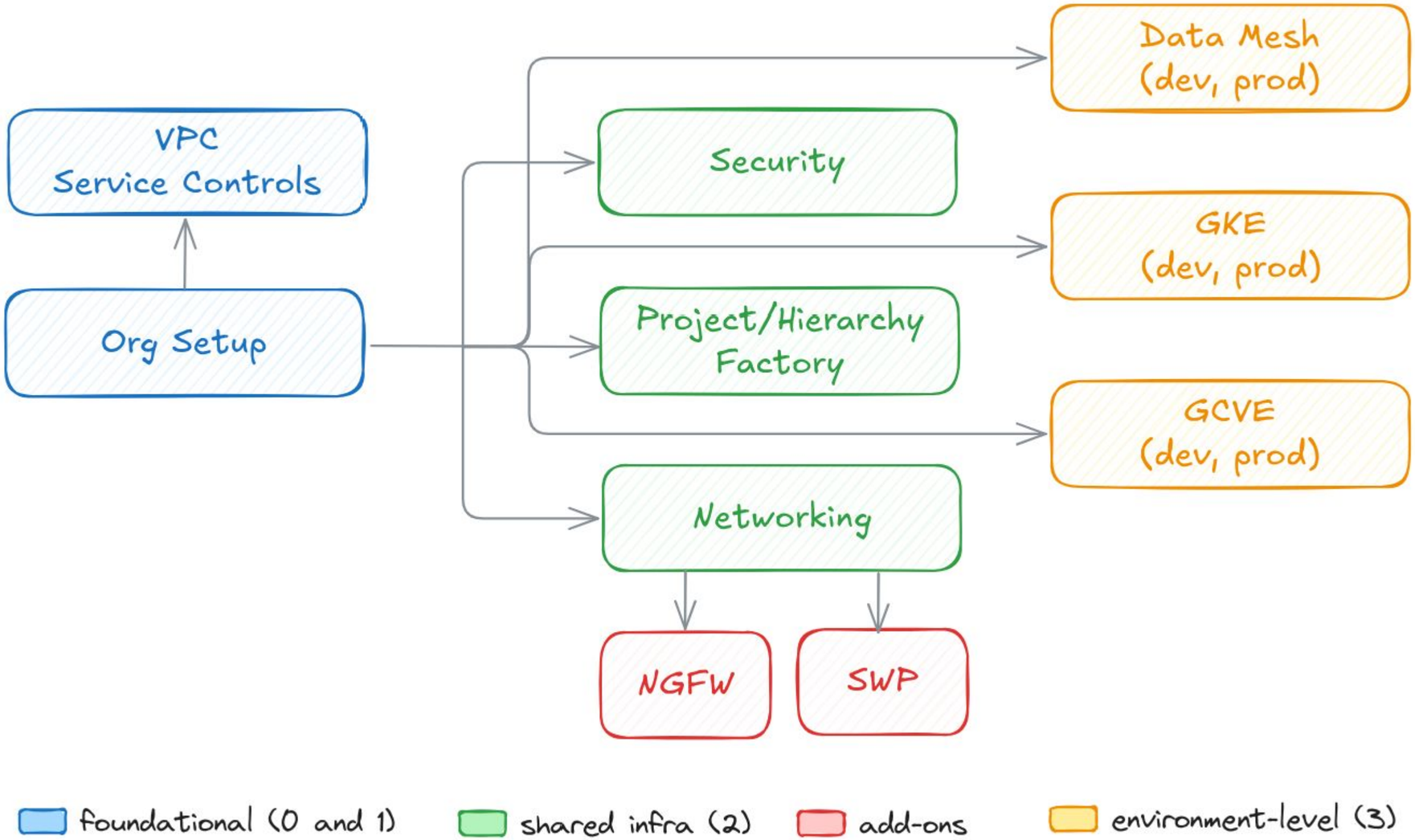
Week 3 topics



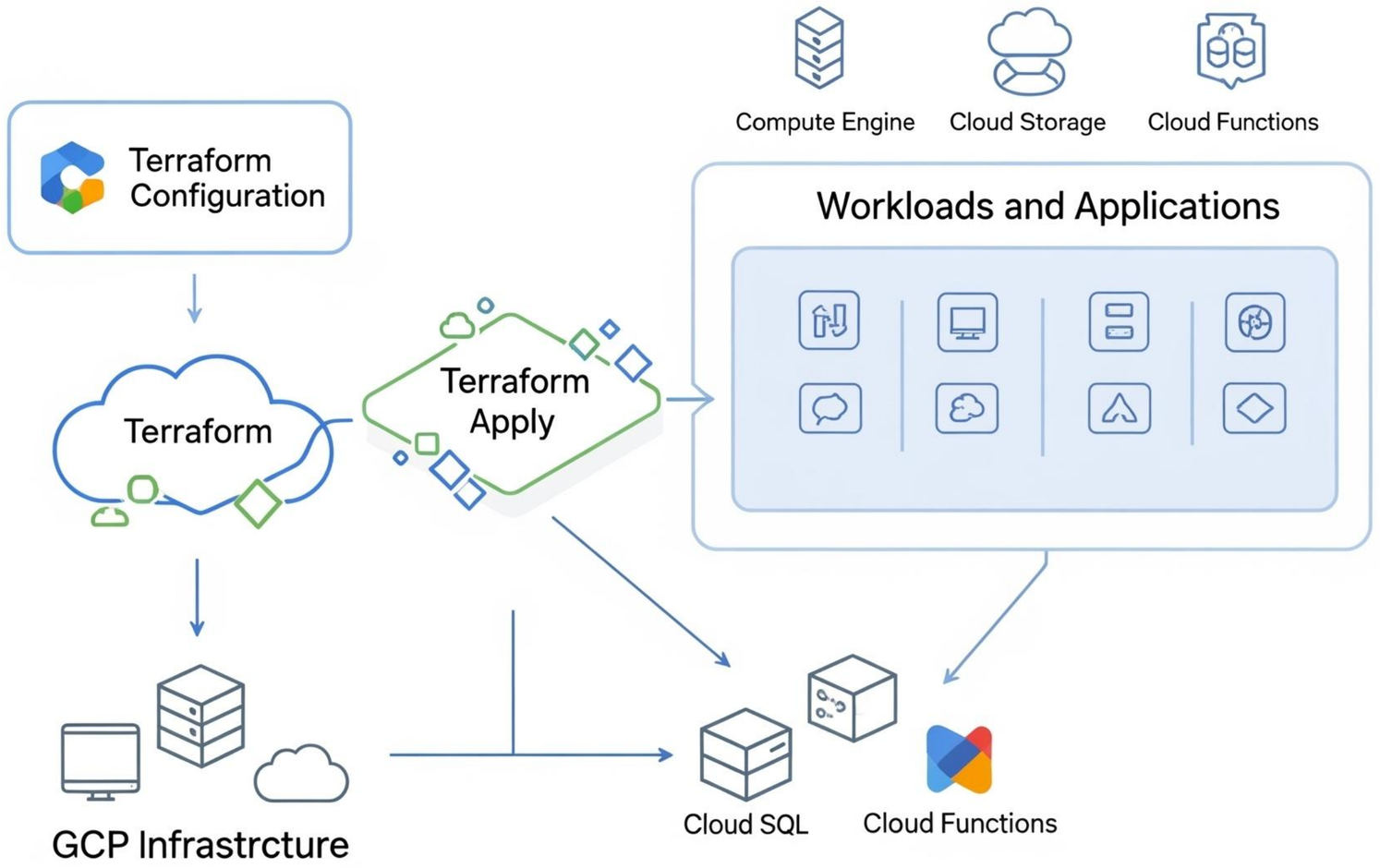
Managing and Provisioning a Solution Infrastructure

Before workload migration starts...

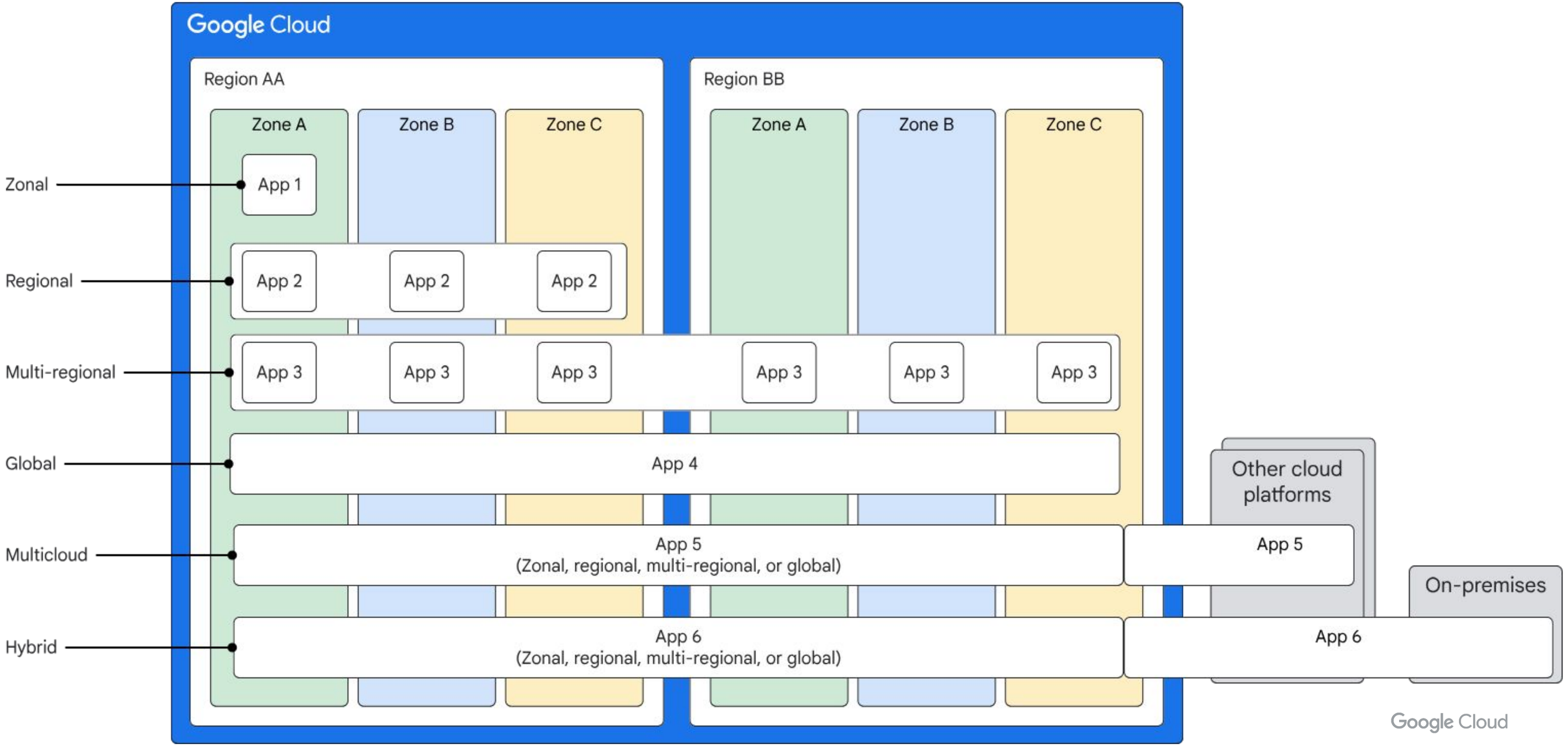
... deploy a Landing Zone



… and only then, focus on your workloads and apps.



Deployment archetypes



Google Cloud Storage (GCS)

Know these GCS features well!

- Controlling object lifecycle:
  - Retention policy (best for compliance)
  - Object Hold (prevent individual objects from being deleted)
  - Object Versioning (aka “automatic backups with retention policy; be aware of additional costs)
  - Object Lifecycle Management (aka “object TTL” / downgrade class to optimize costs)
- ACLs (read, write, full control on buckets or an object).
- Objects are immutable.
- Location constraints on buckets.
- Pub/Sub notifications for Cloud Storage
- Resumable uploads (can restart from the last successful chunk).
- Strong consistency except for cached objects.
- Storage class set at object level (fine-grained performance/cost control without moving data to different buckets).
- Cloud Storage Triggers to handle events in Cloud Functions.
- Streaming uploads to GCS.
- For data encryption, GCS supports GMEK, CMEK and CSEK (most services do not support CSEK!)

Diagnostic Question Discussion

Your company has an application that is running on multiple instances of Compute Engine. It generates 1 TB per day of logs. For compliance reasons, the logs need to be kept for at least two years. The logs need to be available for active query for 30 days. After that, they just need to be retained for audit purposes. You want to implement a storage solution that is compliant, minimizes costs, and follows Google-recommended practices.

What should you do?

A. 1. Write a daily cron job, running on all instances, that uploads logs into a Cloud Storage bucket. 2. Create a sink to export logs into a regional Cloud Storage bucket. 3. Create an Object Lifecycle rule to move files into a Coldline Cloud Storage bucket after one month

B. 1. Install a Cloud Logging agent on all instances. 2. Create a sink to export logs into a partitioned BigQuery table. 3. Set a time_partitioning_expiration of 30 days.

C. 1. Install a Cloud Logging agent on all instances. 2. Create a sink to export logs into a regional Cloud Storage bucket. 3. Create an Object Lifecycle rule to move files into a Coldline Cloud Storage bucket after one month. 4. Configure a retention policy at the bucket level using bucket lock.

D. 1. Create a daily cron job, running on all instances, that uploads logs into a partitioned BigQuery table. 2. Set a time_partitioning_expiration of 30 days.

Diagnostic Question Discussion

Your company has an application that is running on multiple instances of Compute Engine. It generates 1 TB per day of logs. For compliance reasons, the logs need to be kept for at least two years. The logs need to be available for active query for 30 days. After that, they just need to be retained for audit purposes. You want to implement a storage solution that is compliant, minimizes costs, and follows Google-recommended practices.

What should you do?

A. 1. Write a daily cron job, running on all instances, that uploads logs into a Cloud Storage bucket. 2. Create a sink to export logs into a regional Cloud Storage bucket. 3. Create an Object Lifecycle rule to move files into a Coldline Cloud Storage bucket after one month

B. 1. Install a Cloud Logging agent on all instances. 2. Create a sink to export logs into a partitioned BigQuery table. 3. Set a time_partitioning_expiration of 30 days.

C. 1. Install a Cloud Logging agent on all instances. 2. Create a sink to export logs into a regional Cloud Storage bucket. 3. Create an Object Lifecycle rule to move files into a Coldline Cloud Storage bucket after one month. 4. Configure a retention policy at the bucket level using bucket lock.

D. 1. Create a daily cron job, running on all instances, that uploads logs into a partitioned BigQuery table. 2. Set a time_partitioning_expiration of 30 days.

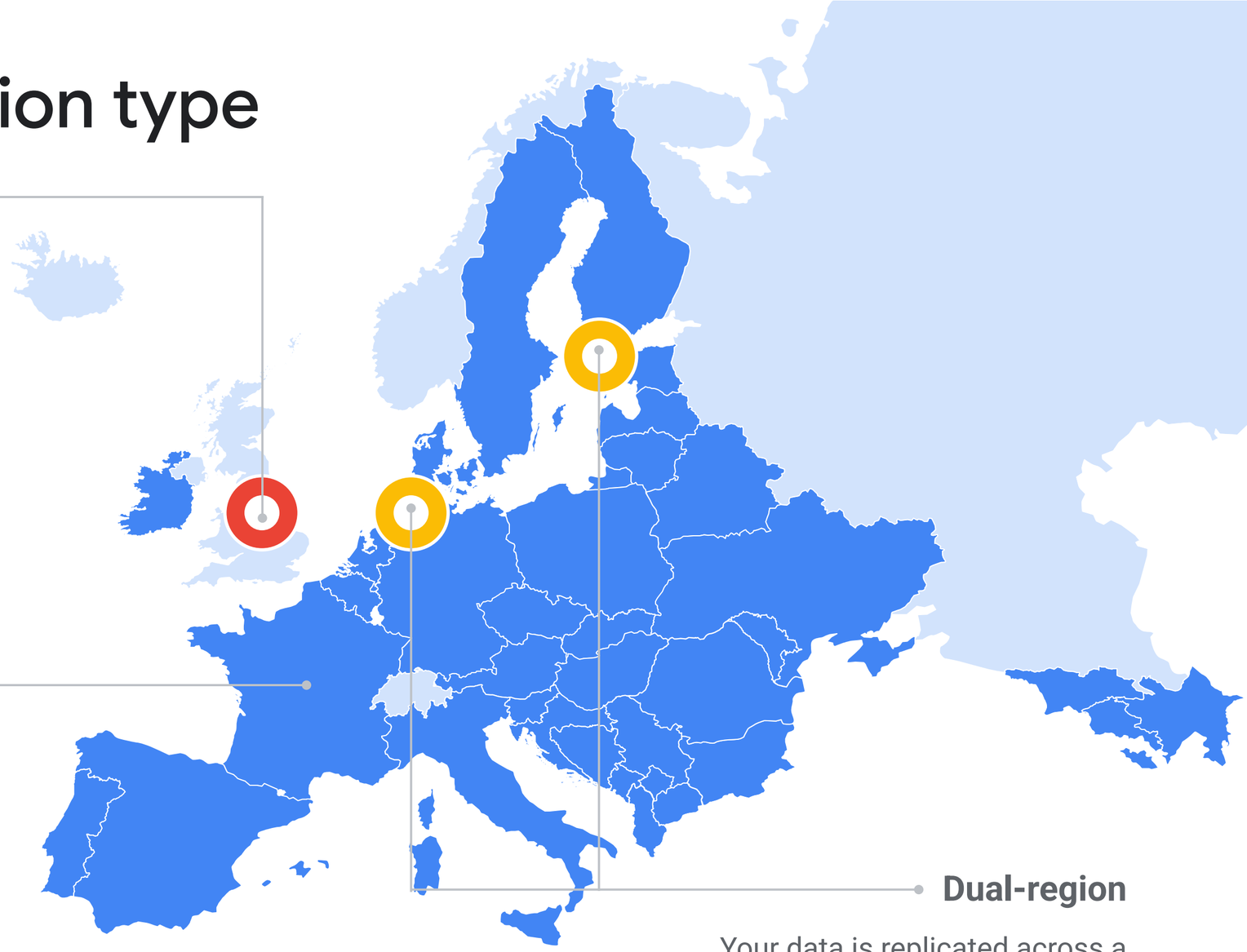
GCS: Choosing a location type

Regional

Your data is stored in a specific region with replication across availability zones in that region. Good for colocating compute and storage for high performance (eg. data analytics).

Multi-Region

Your data is distributed redundantly across US, EU, or Asia. Good for serving content to end users and when you want automatic failover.



Dual-region

Your data is replicated across a specific pair of regions. Good for when you need colocated compute and storage and automatic DR.

Exam Tip:

- *Know the use-cases for each of those choices.*
- *Dual-region buckets are only available for selected regions!*

Google Cloud

Google Cloud Storage: use-cases for each storage class

Standard		Nearline	Coldline	Archive
In multi-region locations for serving content globally.	**In regional locations for data accessed frequently or high throughput needs**	**For data access less than once a month**	**For data accessed roughly less than once a quarter**	**For long term retention**
Streaming videos	Video transcoding	Serving rarely accessed docs	Serve rarely used data	Regulatory archives
Images	Genomics	Backup	Movie archive	Tape replacement
Websites	General data analytics & compute		Disaster recovery	
Documents				

Google Cloud Storage: autoclass

Automatically transition objects to colder storage classes based on usage patterns and transition back to Standard on access.

Not too “intelligent” as of now.

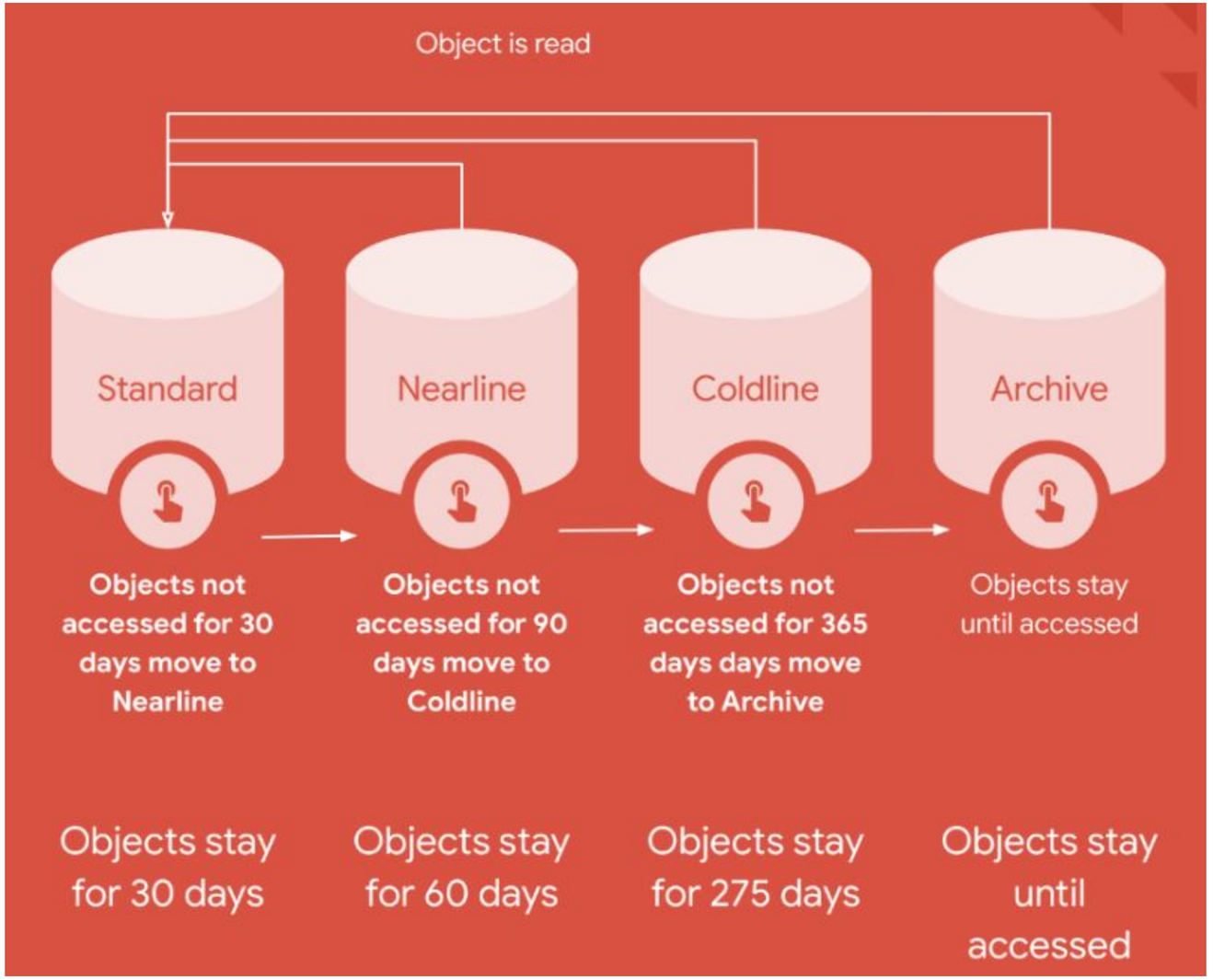
- **Choose a storage class for your data**

  A storage class sets costs for storage, retrieval, and operations, with minimal differences in uptime. Choose if you want objects to be managed automatically or specify a default storage class based on how long you plan to store your data and your workload or use case. Learn more

  (•) Autoclass
  Automatically transitions each object to hotter or colder storage based on object-level activity, to optimize for cost and latency. Recommended if usage frequency may be unpredictable. Can be changed to a default class at any time. Pricing details

  ( ) Set a default class
  Applies to all objects in your bucket unless you manually modify the class per object or set object lifecycle rules. Best when your usage is highly predictable. Can't be changed to Autoclass once the bucket is created.

  - ( ) Standard
    Best for short-term storage and frequently accessed data
  - ( ) Nearline
    Best for backups and data accessed less than once a month
  - ( ) Coldline
    Best for disaster recovery and data accessed less than once a quarter
  - ( ) Archive
    Best for long-term digital preservation of data accessed less than once a year



Best Practices on Storage Class Selection

Consider retention period and access frequency

Retention Period

Access Frequency	<1 mo	1–3 mo	3–12 mo	>12 mo
>12/yr	Standard	Standard	Standard	Standard
4–12/yr	Standard	Nearline	Nearline	Nearline
1–4/yr	Standard	Nearline	Coldline	Coldline
<1/yr	Standard	Nearline	Coldline	Archive

Exam Tips:

- *Each storage class has so-called "minimum storage duration", so when optimizing costs, you also need to validate if you'll need to keep your objects for at least this amount of time.*

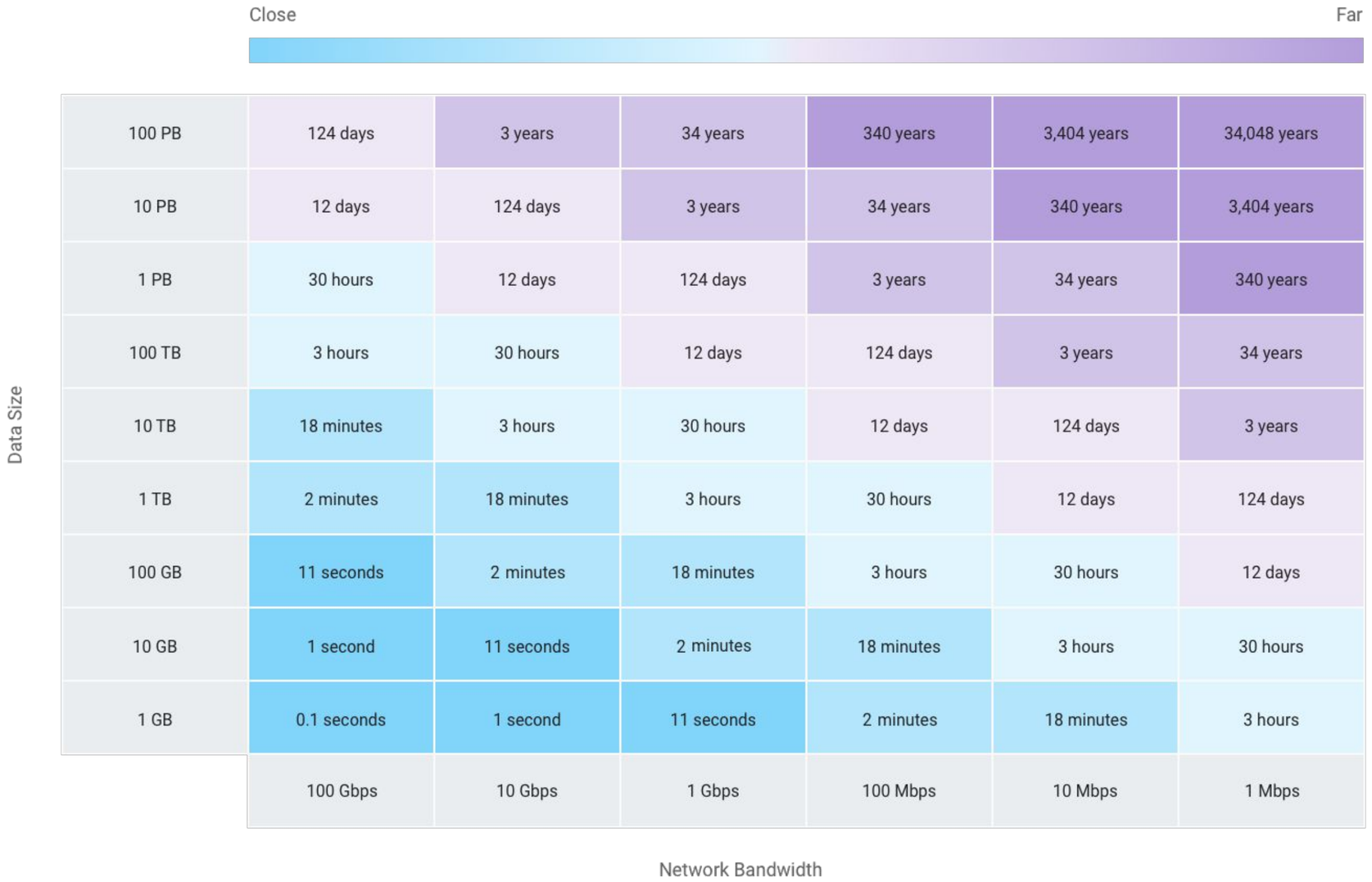
Choose the right tool to move data to GCS!

Where you're moving data from	Scenario	Suggested products
Another cloud provider (for example, Amazon Web Services or Microsoft Azure) to Google Cloud	—	Storage Transfer Service
Cloud Storage to Cloud Storage (two different buckets)	—	Storage Transfer Service
Your private data center to Google Cloud	Enough bandwidth to meet your project deadline for less than 1 TB of data	gsutil
Your private data center to Google Cloud	Enough bandwidth to meet your project deadline for more than 1 TB of data	Storage Transfer Service for on-premises data
Your private data center to Google Cloud	Not enough bandwidth to meet your project deadline	Transfer Appliance

Exam Tips:

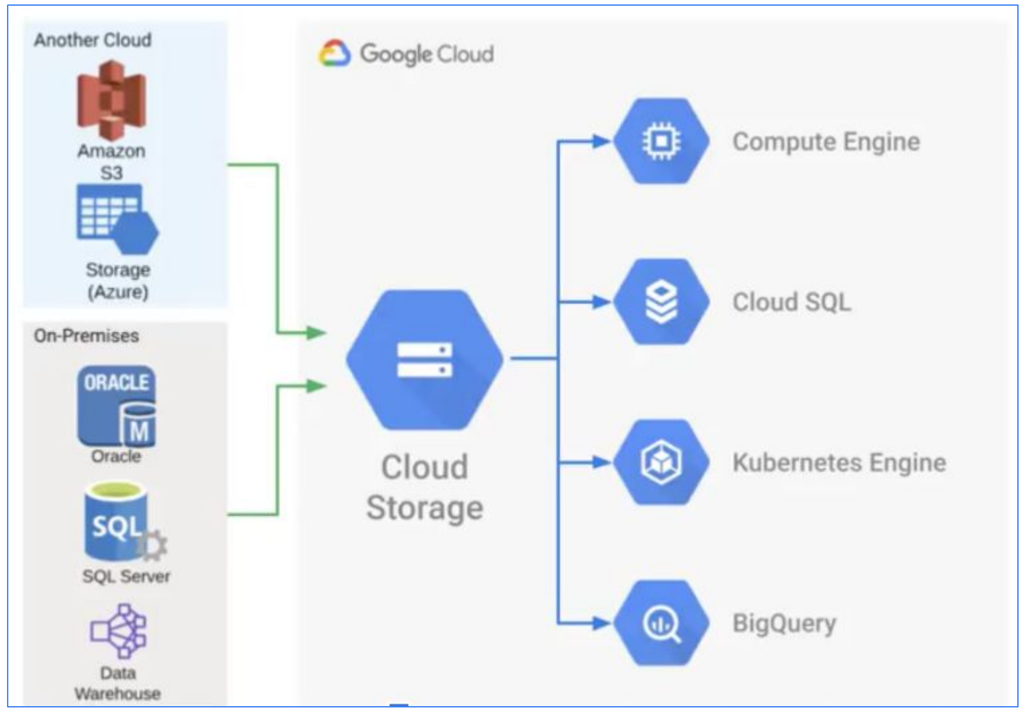
- *Depending on size and throughput, use gsutil / Transfer Service (low cost) / Transfer Appliance*
- ***When using Transfer Appliance, you need to execute so-called "rehydration" process** which will decrypt and uncompress before it's put to a destination bucket.*

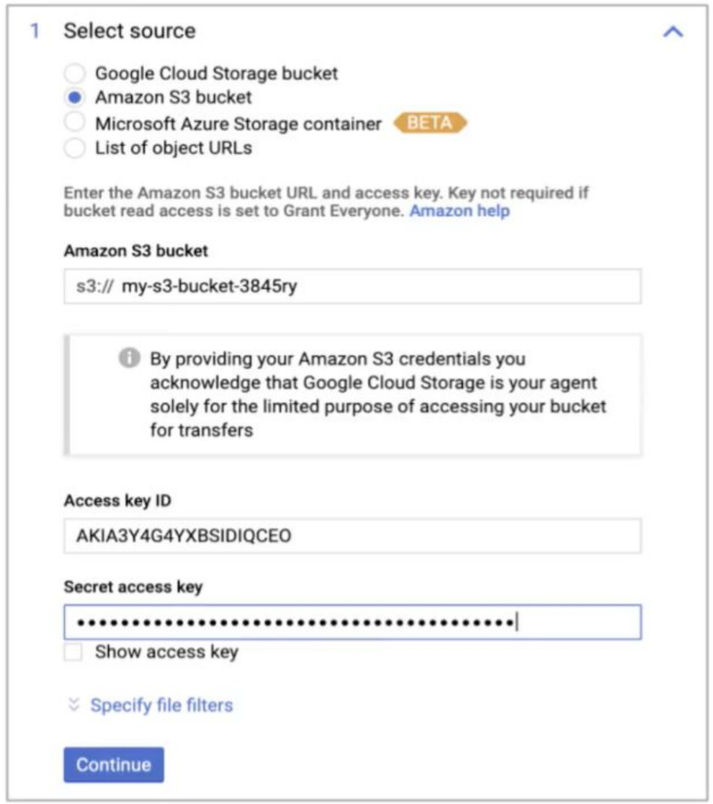
Transferring large datasets TO GCP

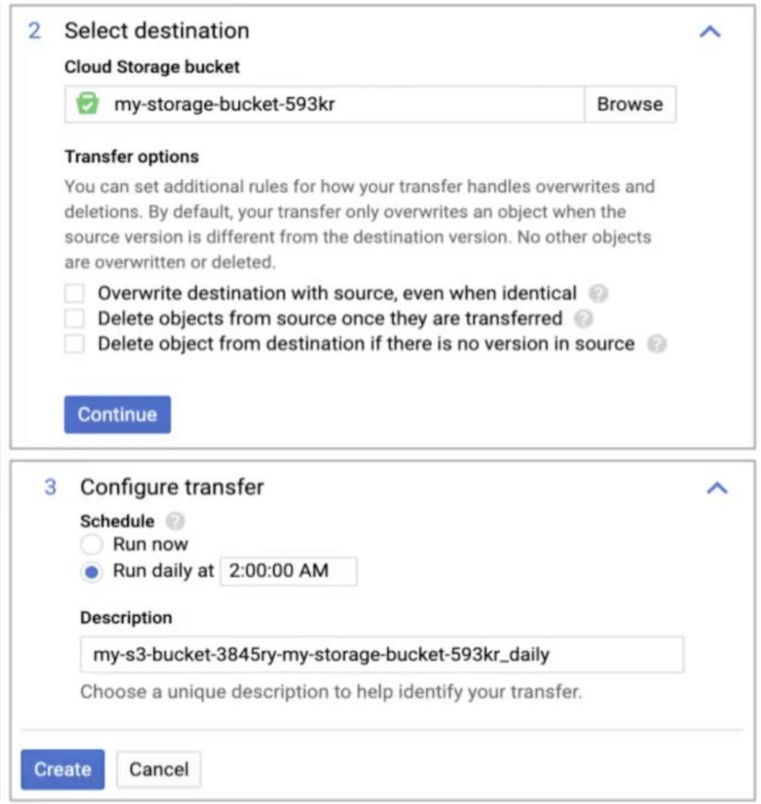


Data Size	100 Gbps	10 Gbps	1 Gbps	100 Mbps	10 Mbps	1 Mbps
100 PB	124 days	3 years	34 years	340 years	3,404 years	34,048 years
10 PB	12 days	124 days	3 years	34 years	340 years	3,404 years
1 PB	30 hours	12 days	124 days	3 years	34 years	340 years
100 TB	3 hours	30 hours	12 days	124 days	3 years	34 years
10 TB	18 minutes	3 hours	30 hours	12 days	124 days	3 years
1 TB	2 minutes	18 minutes	3 hours	30 hours	12 days	124 days
100 GB	11 seconds	2 minutes	18 minutes	3 hours	30 hours	12 days
10 GB	1 second	11 seconds	2 minutes	18 minutes	3 hours	30 hours
1 GB	0.1 seconds	1 second	11 seconds	2 minutes	18 minutes	3 hours

Cloud Storage: Storage Transfer Service







Exam Tip: *Storage Transfer Service can be set up one-off (e.g., move bucket to new location) and recurring (e.g., back up from S3 to GCS with rsync-like semantics)*

Diagnostic Question Discussion

Your operations team currently stores 10 TB of data in an object storage service from a third-party provider. They want to move this data to a Cloud Storage bucket as quickly as possible, following Google-recommended practices. They want to minimize the cost of this data migration.

Which approach should they use?

A. Use the “gcloud storage mv” command to move the data.

B. Use the Storage Transfer Service to move the data.

C. Download the data to a Transfer Appliance, and ship it to Google.

D. Download the data to the on-premises data center, and upload it to the Cloud Storage bucket.

Diagnostic Question Discussion

Your operations team currently stores 10 TB of data in an object storage service from a third-party provider. They want to move this data to a Cloud Storage bucket as quickly as possible, following Google-recommended practices. They want to minimize the cost of this data migration.

Which approach should they use?

A. Use the “gcloud storage mv” command to move the data.

B. Use the Storage Transfer Service to move the data.

C. Download the data to a Transfer Appliance, and ship it to Google.

D. Download the data to the on-premises data center, and upload it to the Cloud Storage bucket.

Diagnostic Question Discussion

Your company wants to migrate their 10-TB on-premises database export into Cloud Storage. You want to minimize the time it takes to complete this activity, the overall cost, and database load. The bandwidth between the on-premises environment and Google Cloud is 1 Gbps. You want to follow Google-recommended practices.

What should you do?

A. Develop a Dataflow job to read data directly from the database and write it into Cloud Storage.

B. Use the Data Transfer appliance to perform an offline migration.

C. Use a commercial partner ETL solution to extract the data from the on-premises database and upload it into Cloud Storage.

D. Compress the data and upload it with gsutil -m to enable multi-threaded copy.

Diagnostic Question Discussion

Your company wants to migrate their 10-TB on-premises database export into Cloud Storage. You want to minimize the time it takes to complete this activity, the overall cost, and database load. The bandwidth between the on-premises environment and Google Cloud is 1 Gbps. You want to follow Google-recommended practices.

What should you do?

A. Develop a Dataflow job to read data directly from the database and write it into Cloud Storage.

B. Use the Data Transfer appliance to perform an offline migration.

C. Use a commercial partner ETL solution to extract the data from the on-premises database and upload it into Cloud Storage.

D. Compress the data and upload it with gsutil -m to enable multi-threaded copy.

#GCPSketchnote
@PVERGADIA
THECLOUDGIRL.DEV
03.30.2021

Options to move data to Google Cloud

GCS TRANSFER TOOLS

For small transfers upto a few TBs

TRANSFER SERVICE

Large-scale online transfer

Cloud data | On-premises

TRANSFER APPLIANCE

Large scale transfers from low bandwidth networks

BIGQUERY DATA TRANSFER SERVICE

Data from SaaS & 3rd party apps

HOW DO THEY WORK?

Upload data directly to GCS

TOOLS - GSUTIL, UI, JSON API

S3 / Azure Cloud

TOOLS
UI, Client Libraries, HTTP REST API

On-premises

TOOLS
On-premise agent with GUI

1. Request Appliance
2. Upload data SFTP, SCP or NFS
3. Ship to Google
4. GCS
5. Erase NIST 800 standard

S3
Teradata
RedShift
Google SaaS apps
GCS
3rd party

SOME COOL THINGS TO KNOW

GSUTIL - Fast multi threaded

rsync

Streaming

Scheduled & Incremental updates
Scale to 10's of Gbps

Data moves over Google's high-bandwidth network pipes

Minimize transfer time max available bandwidth performance optimizations

All SSDs
Minimal software
Performance features
Multiple network connectivity options

Automatic Schedule

Mirror or Append data

SECURITY

HTTPS encrypted TLS connections

Cloud sources accessed using private credentials

All bytes checksummed & encrypted in-flight

AES 256 encryption on the appliance
Tamper resistant, Ruggedized
Customer Managed Encryption Key (CMEK)

HTTPS encrypted TLS connections

USE CASES FOR DATA TRANSFER

Data Center Migration

Decommission Tape Libraries & Infrastructure

Machine Learning

Storage & Delivery

Backup & Archival

Diagnostic Question Discussion

Your company has created an application that uploads a report to a Cloud Storage bucket. When the report is uploaded to the bucket, you want to publish a message to a Cloud Pub/Sub topic. You want to implement a solution that will take a small amount to effort to implement.

What should you do?

A. Create an App Engine application to receive the file; when it is received, publish a message to the Cloud Pub/Sub topic.

B. Configure the Cloud Storage bucket to trigger Cloud Pub/Sub notifications when objects are modified.

C. Create a Cloud Function that is triggered by the Cloud Storage bucket. In the Cloud Function, publish a message to the Cloud Pub/Sub topic.

D. Create an application deployed in a Google Kubernetes Engine cluster to receive the file; when it is received, publish a message to the Cloud Pub/Sub topic.

Diagnostic Question Discussion

Your company has created an application that uploads a report to a Cloud Storage bucket. When the report is uploaded to the bucket, you want to publish a message to a Cloud Pub/Sub topic. You want to implement a solution that will take a small amount to effort to implement.

What should you do?

A. Create an App Engine application to receive the file; when it is received, publish a message to the Cloud Pub/Sub topic.

B. Configure the Cloud Storage bucket to trigger Cloud Pub/Sub notifications when objects are modified.

C. Create a Cloud Function that is triggered by the Cloud Storage bucket. In the Cloud Function, publish a message to the Cloud Pub/Sub topic.

D. Create an application deployed in a Google Kubernetes Engine cluster to receive the file; when it is received, publish a message to the Cloud Pub/Sub topic.

https://cloud.google.com/storage/docs/pubsub-notifications#other_notification_options

Cloud Storage

#GCPSketchnote

@PVERGADIA THECLOUDGIRL.DEV

8.8.2020

What is Cloud Storage?

A GLOBAL, SECURE AND SCALABLE OBJECT STORE

GLOBAL SECURE SCALABLE

.png .jpg .mpg .mov .txt other

How does it WORK?

WORKFLOW

Image → Bucket (PHOTOS) → Project → Organization

4 STORAGE CLASSES

Based on Budget, Availability and Access Frequency

STANDARD	NEARLINE	COLDLINE	ARCHIVE
Frequent access High Availability	Once a month	Once a quarter	Once a year

New Version >30 Days >90 Days

OBJECT LIFECYCLE MANAGEMENT

AUTO VERSIONING → v1 → v2 → v3

Cloud Storage Use case example

STANDARD → Website + Streaming + Document

NEARLINE → Backups + Disaster Recovery

COLDLINE → Backups + Disaster Recovery

ARCHIVE → Long Term Archiving

STREAMING DATA, BATCH DATA → AI PLATFORM, BIGQUERY

SECURITY for Cloud Storage

- ☑ Encryption at rest
- ☑ Bring your own encryption key
  - CMEK - Customer Managed
  - CSEK - Customer Supplied

Cloud Storage PRICING

STANDARD	NEARLINE	COLDLINE	ARCHIVE
$$$$	$$$	$$	$
Automatic Redundancy Frequent Access			

How to USE Cloud Storage

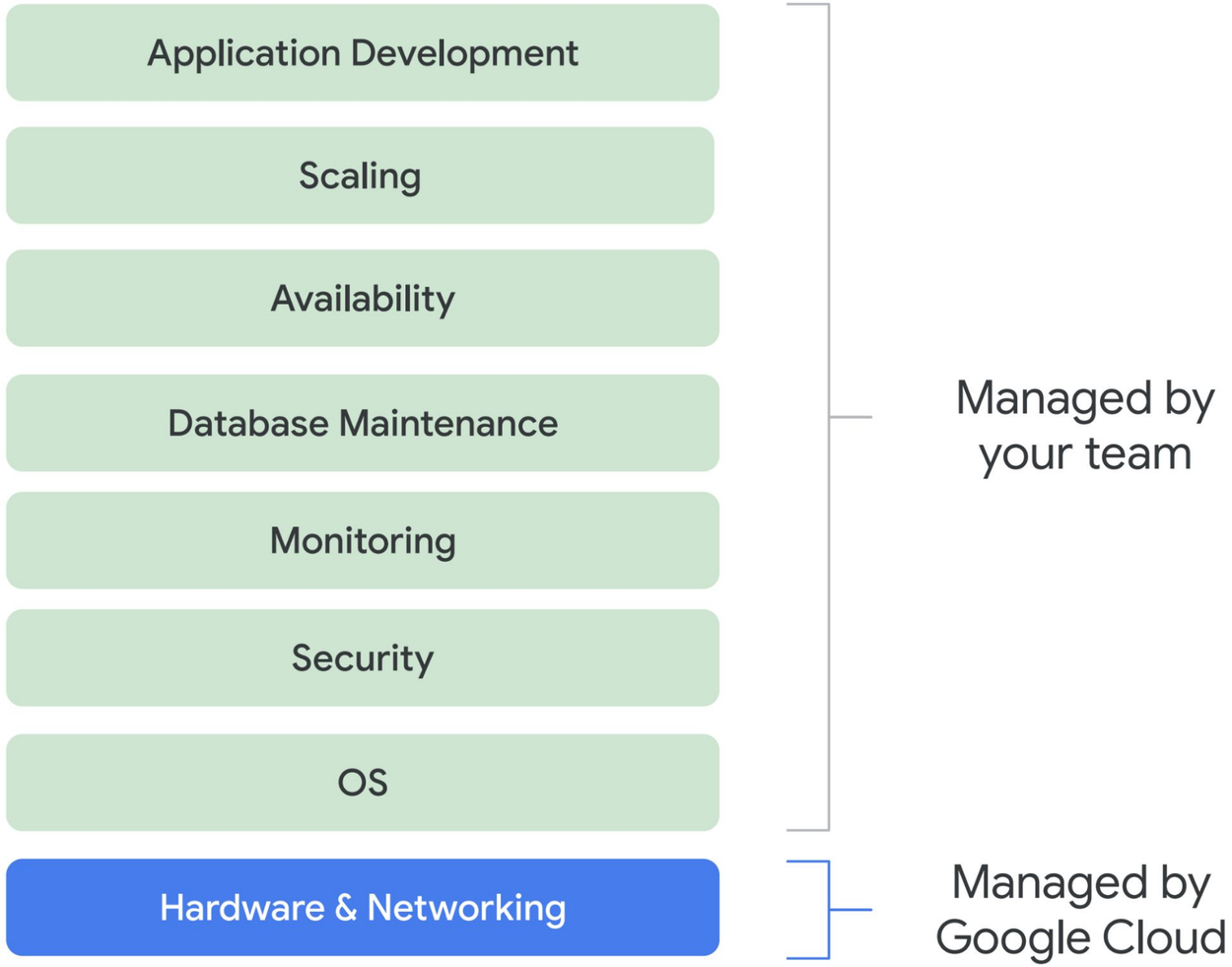
ONLINE TRANSFER	TRANSFER SERVICE	TRANSFER APPLIANCE
gsutil, API, UI <gsutil cp image.png gs://my-bucket>	Transfer data from other clouds & on-premise	Hardware for >100tb data transfer

image.png API

Cloud SQL

Managed databases: the “why”

Self-managed DBs on GCE VMs



Exam Tip: *custom OS images / startup scripts / products from GCP Marketplace etc…*

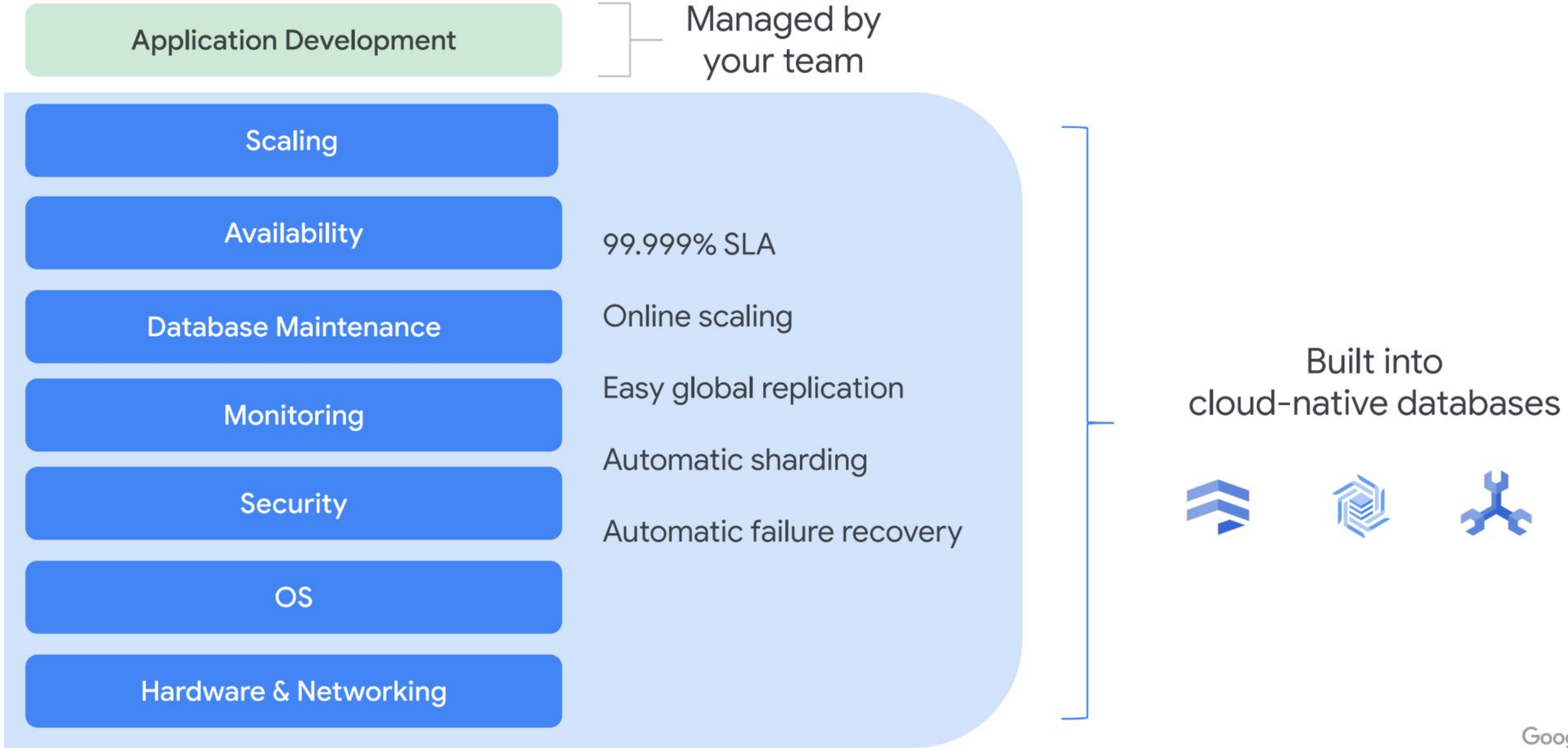
I can automate the installation, but you still need to…

- Provision resources
- Install database engine
- Configure it
- Patch & update
- Handle high availability
- Implement & manage backup & restore
- Resize when needed
- Implement monitoring
- … and so on

Exam Tip: *Hence* ***self-managed databases are NOT a preferred option from the exam perspective****… unless you have a valid reason.*

Managed database services.

Exam Tip: *using managed services is usually a preferred approach from exam perspective (unless you're running into some constraints / have special needs.*

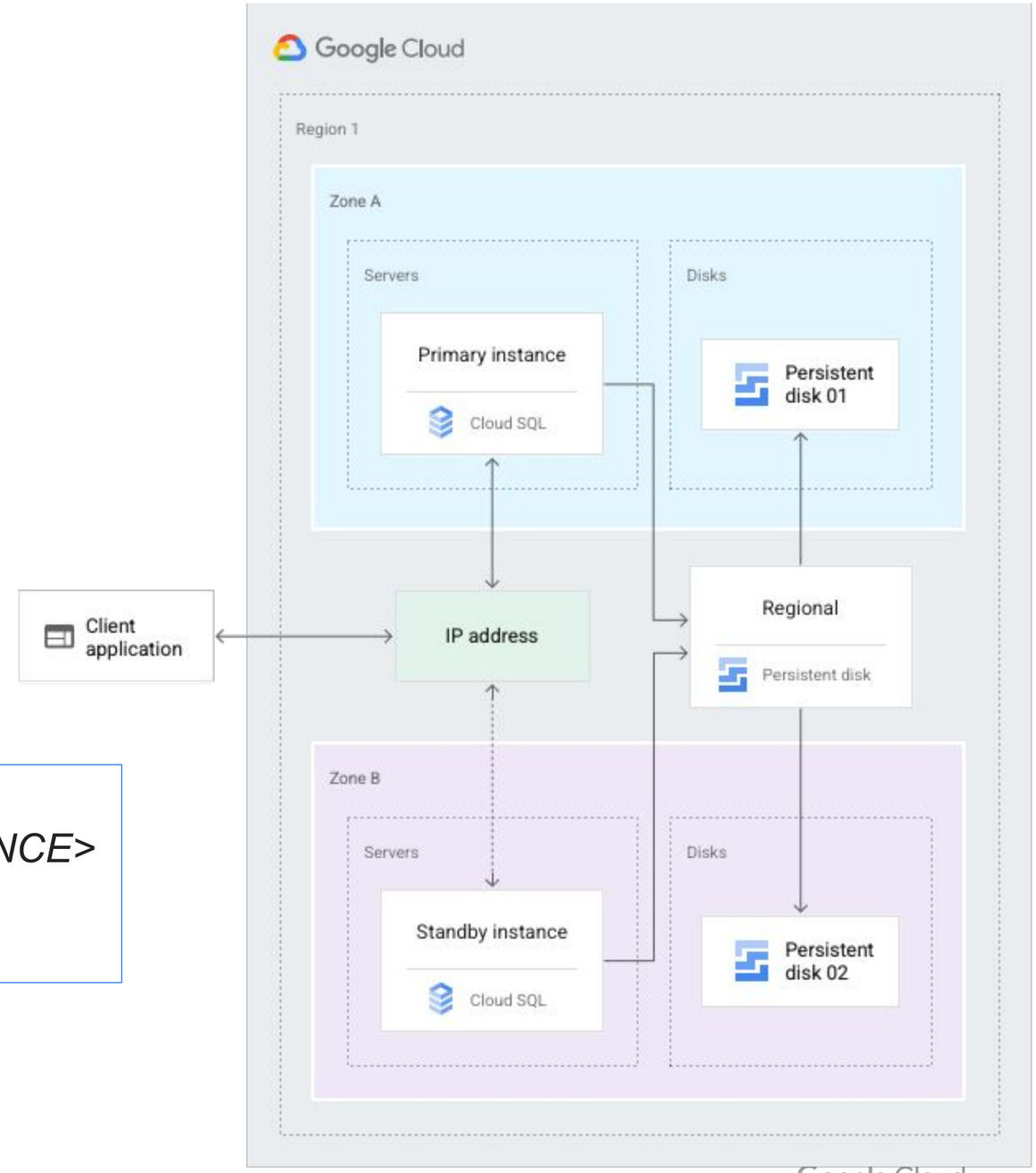


Cloud SQL High availability

- Primary and secondary in different zones within the configured region
- Synchronous replication to each zone's persistent disk
- If heartbeat of the primary instance is unavailable for ~60 sec → automatic failover
- The persistent disk is then attached to the standby instance
- Less than 3 min of unavailability, the same IP address for the client application

Exam Tip: *Know how to:*

- *Initiate failover: gcloud sql instances failover <PRIM_INSTANCE>*
- *Check if instance is / isn't set for HA: gcloud sql instances describe (availabilityType = REGIONAL / ZONAL)*



Diagnostic Question Discussion

You need to set up Microsoft SQL Server on GCP. Management requires that there's no downtime in case of a data center outage in any of the zones within a GCP region.

What should you do?

A. Configure a Cloud Spanner instance with a regional instance configuration.

B. Set up SQL Server on Compute Engine, using Always On Availability Groups using Windows Failover Clustering. Place nodes in different subnets.

C. Configure a Cloud SQL instance with high availability enabled.

D. Set up SQL Server Always On Availability Groups using Windows Failover Clustering. Place nodes in different zones.

Diagnostic Question Discussion

You need to set up Microsoft SQL Server on GCP. Management requires that there's no downtime in case of a data center outage in any of the zones within a GCP region.

What should you do?

A. Configure a Cloud Spanner instance with a regional instance configuration.

B. Set up SQL Server on Compute Engine, using Always On Availability Groups using Windows Failover Clustering. Place nodes in different subnets.

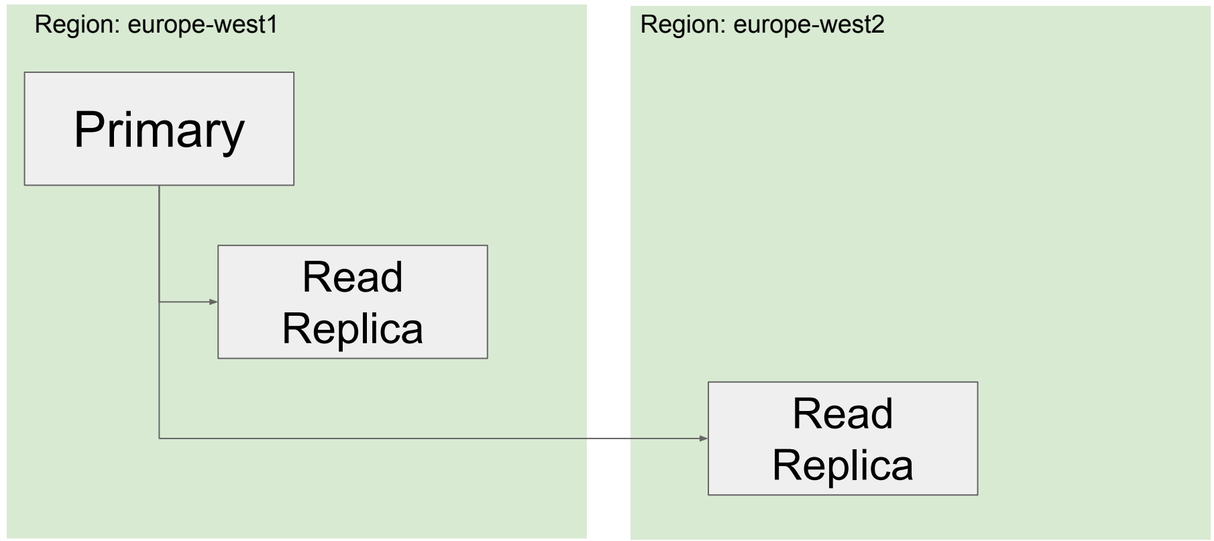
C. Configure a Cloud SQL instance with high availability enabled.

D. Set up SQL Server Always On Availability Groups using Windows Failover Clustering. Place nodes in different zones.

Cloud SQL: Read Replicas

Use cases: Disaster Recovery / offload analytics workloads / migrate between platforms or regions

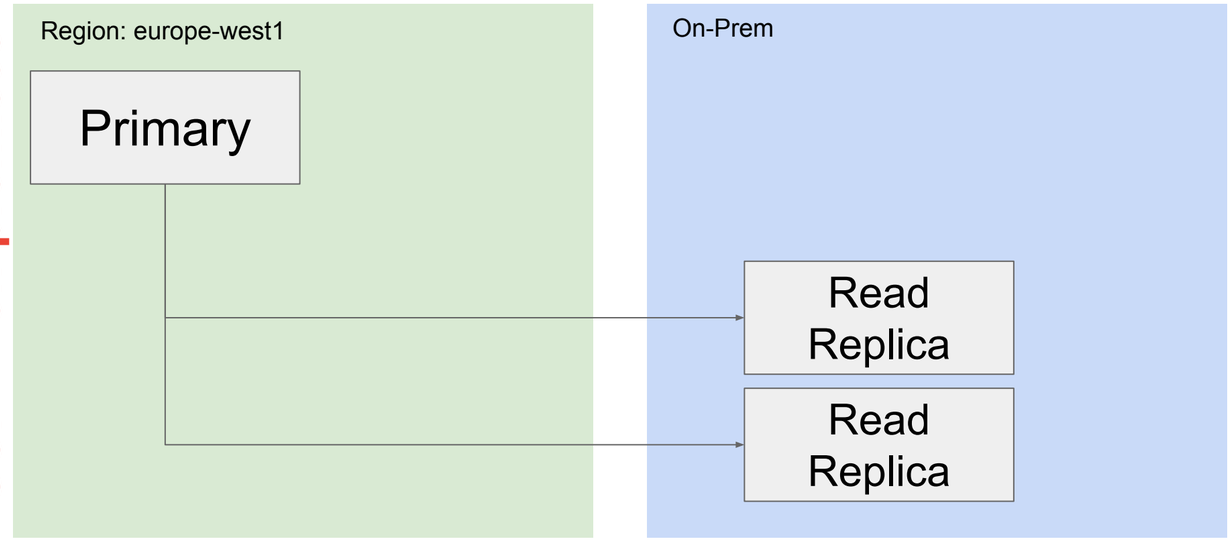
Read Replica
GCP -> GCP



Benefits & Use Cases

- Additional Read capacity (read only)
- Analytics target (adding secondary indexes)
- Read replicas can be different machine types than primary (never less vcpus for postgres)
- Settings of primary are propagated to replicas incl. root pwd &user table changes
- No load balancing between replicas
- Mysql Parallel replication (read replica side)

External Read Replica
GCP -> on-premises



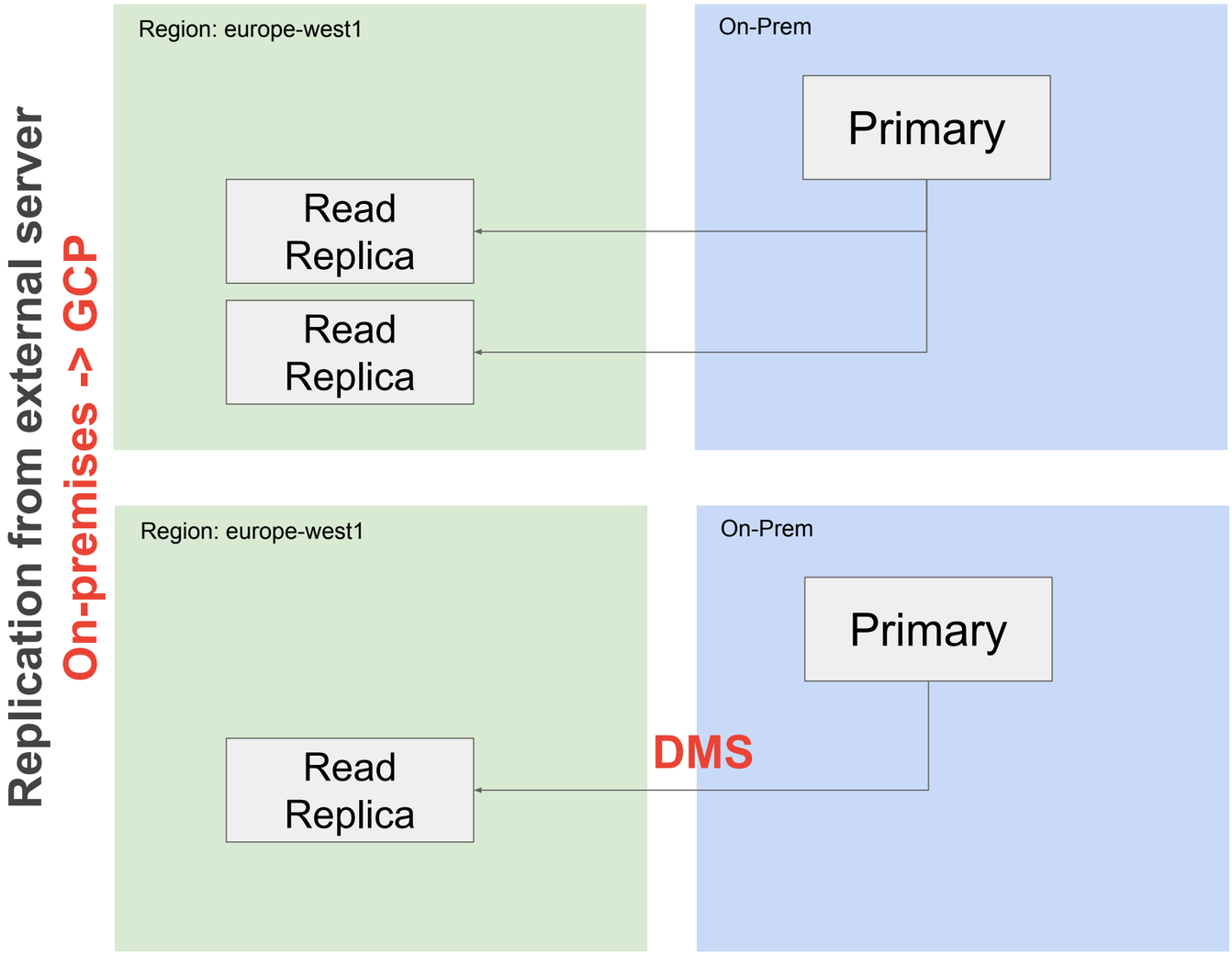
Benefits & Use Cases

- Reduce latency for external connection
- Analytics target
- Migration path to other platforms
- In case of e.g. network outage on-prem the replication lag might be too large and replicas need to be recreated

Exam Tip: *Docus on replicating TO external server*

Cloud SQL: Read Replicas

Use cases: Disaster Recovery / offload analytics workloads / migrate between platforms or regions



MYSQL Benefits & Use Cases

- Migration path to Cloud SQL with minimum downtime
- Data replication to GCP
- Offloading admin overhead of replicas to GCP
- Analytics target
- Parallel replication (read replica)

POSTGRES - DMS

- Use DMS to replicate from an external DB Server to a Cloud SQL Read replica (One-off Migration or Continuous cdc replication)
- DB Source can be self-managed DB (on-prem or IaaS), Aws Rds, Aurora, Cloud SQL

Exam Tip: *Docus on replicating FROM external server*

Diagnostic Question Discussion

During a high traffic portion of the day, one of your relational databases crashes, but the replica is never promoted to a master. You want to avoid this in the future.

A. Use a different database

B. Choose larger instances for your database

C. Create snapshots of your database more regularly

D. Implement routinely scheduled failovers of your databases

What should you do?

Diagnostic Question Discussion

During a high traffic portion of the day, one of your relational databases crashes, but the replica is never promoted to a master. You want to avoid this in the future.

A. Use a different database

B. Choose larger instances for your database

C. Create snapshots of your database more regularly

D. Implement routinely scheduled failovers of your databases

What should you do?

https://cloud.google.com/solutions/cloud-sql-mysql-disaster-recovery-complete-failover-fallback

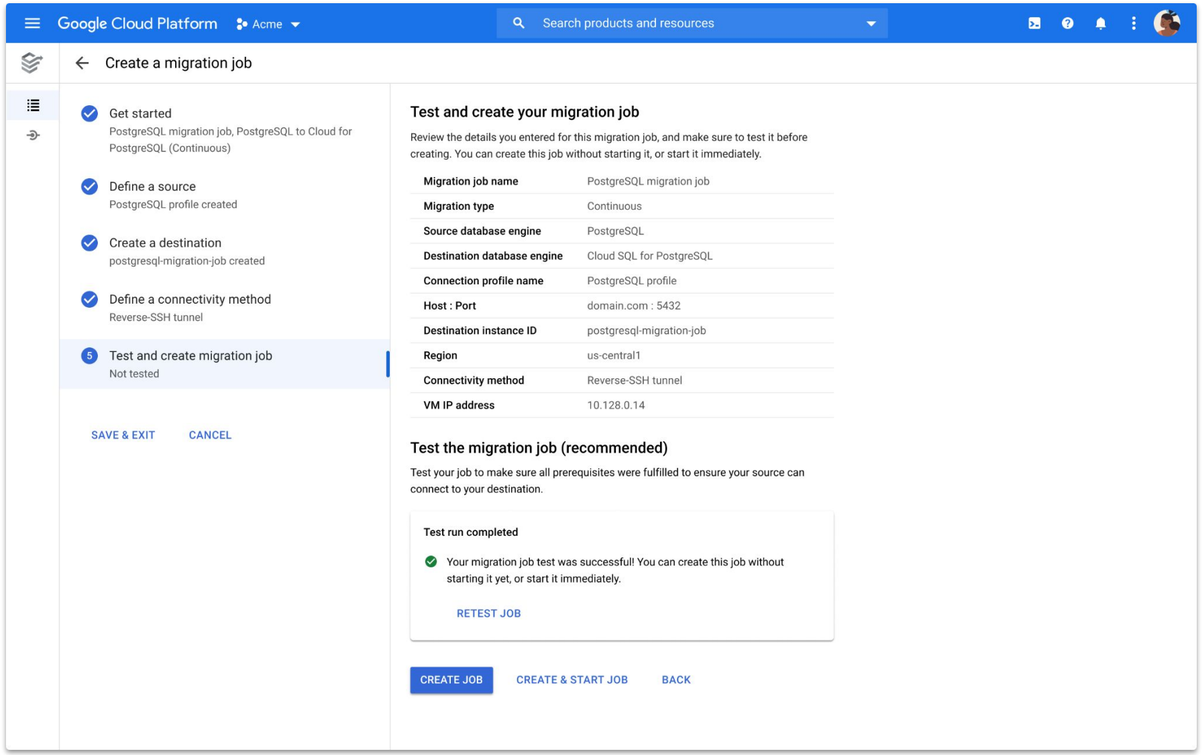
Simplified migration with Data Migration Service (DMS)

Continuous migration path to Cloud SQL with minimal downtime

Simplest way to migrate to Cloud SQL:

- No migration servers to manage
- Baked-in configuration support
- Native replication method

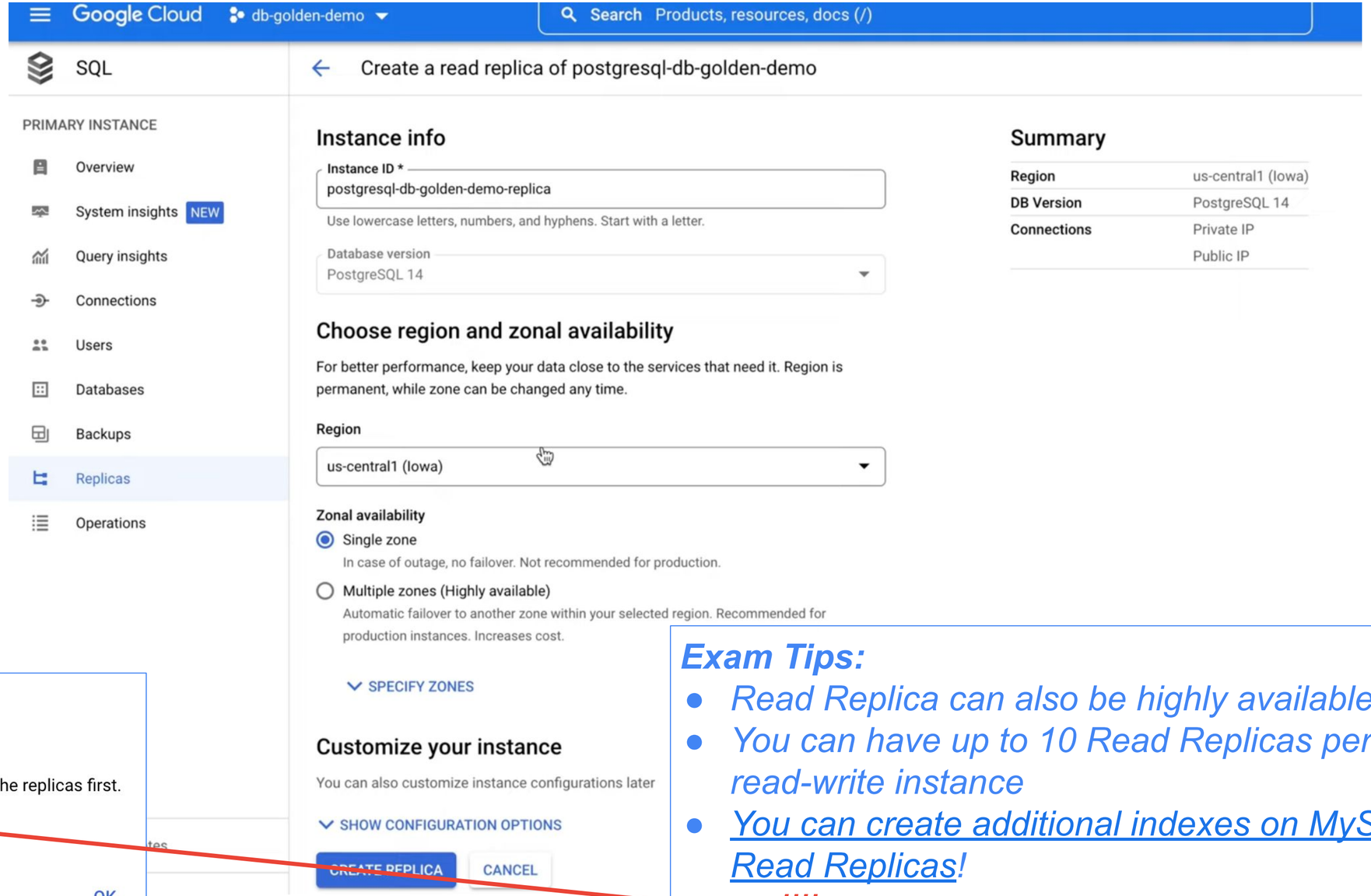
Secure connection options for encrypted data and using private networking



Exam Tip: *Make sure to be familiar with this overview: Database Migration Service.*

Cloud SQL DR with cross-region Read Replicas

How to create



Instance has replicas

You cannot stop an instance that has replicas. You must delete the replicas first.

OK

Exam Tips:

- *Read Replica can also be highly available.*
- *You can have up to 10 Read Replicas per read-write instance*
- *You can create additional indexes on MySQL Read Replicas!*
- *!!!!*

Google Cloud

Cloud SQL: GCP-native Backup and Restore

Types

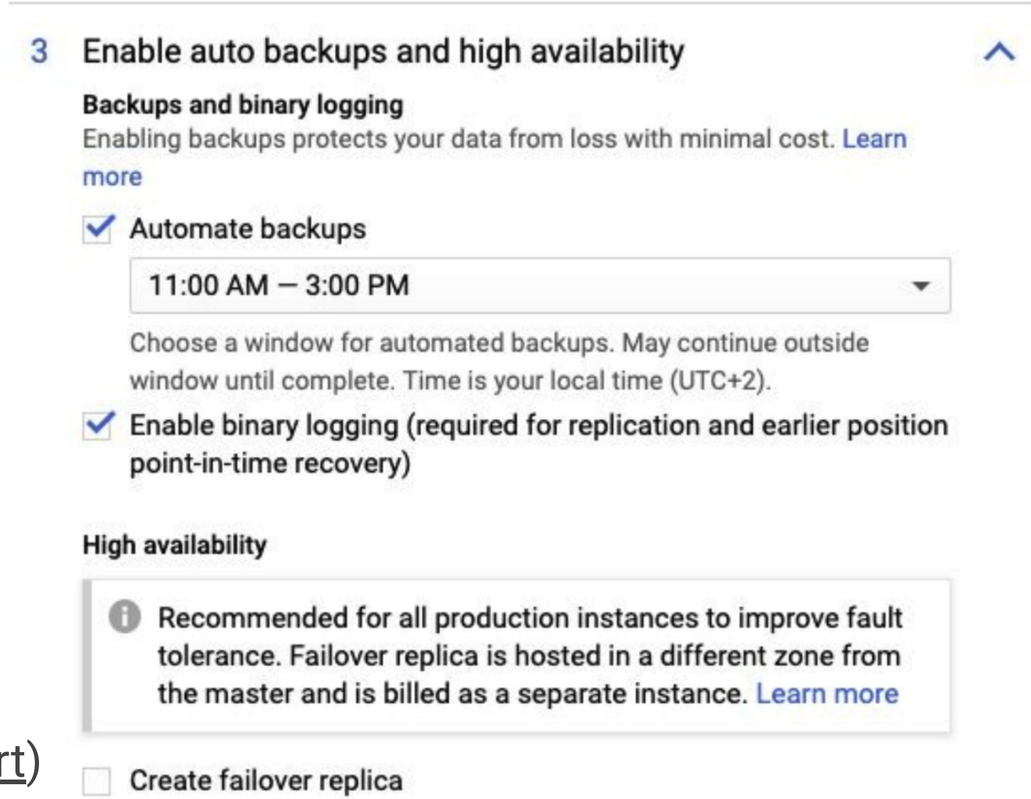
- **On-Demand**
  - Create disk-level snapshot backup at any time
  - Not deleted automatically

- **Automated**
  - 4 hour backup window (e.g. 11am - 3pm)
  - Schedule when instance has least activity
  - If data has not changed since last backup then no backup is taken

Characteristics

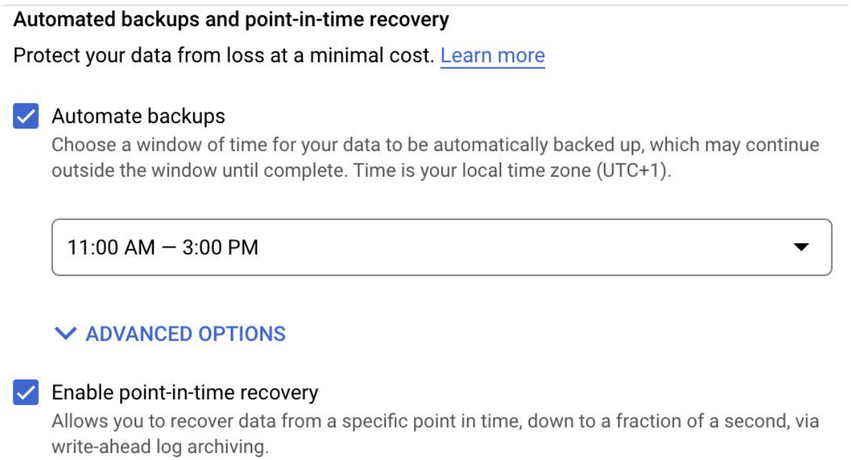
- Up to 365 daily automated backups for each instance. (Only up to 7 days for binlog/WAL files)
- Incremental Backups
- Storage used by backups is charged at a reduced rate. (see pricing)
- Backups can not be exported - only instance data (see doc for export)
- Backups are deleted after instance is deleted (Data export required to retain data; read replica for export without perf. impact)
- Backups are disk-level snapshots stored on GCS

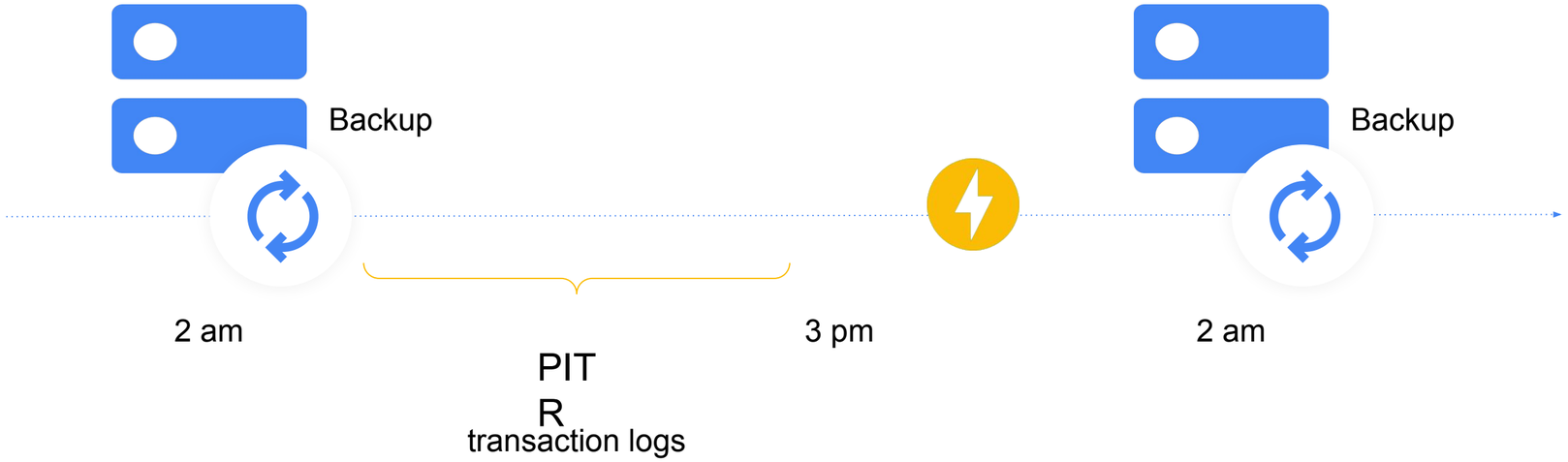
Exam Tip: *Cloud SQL backup window is NOT the same as maintenance window.*



Cloud SQL: Point-in-time recovery

recover an instance to a specific point in time



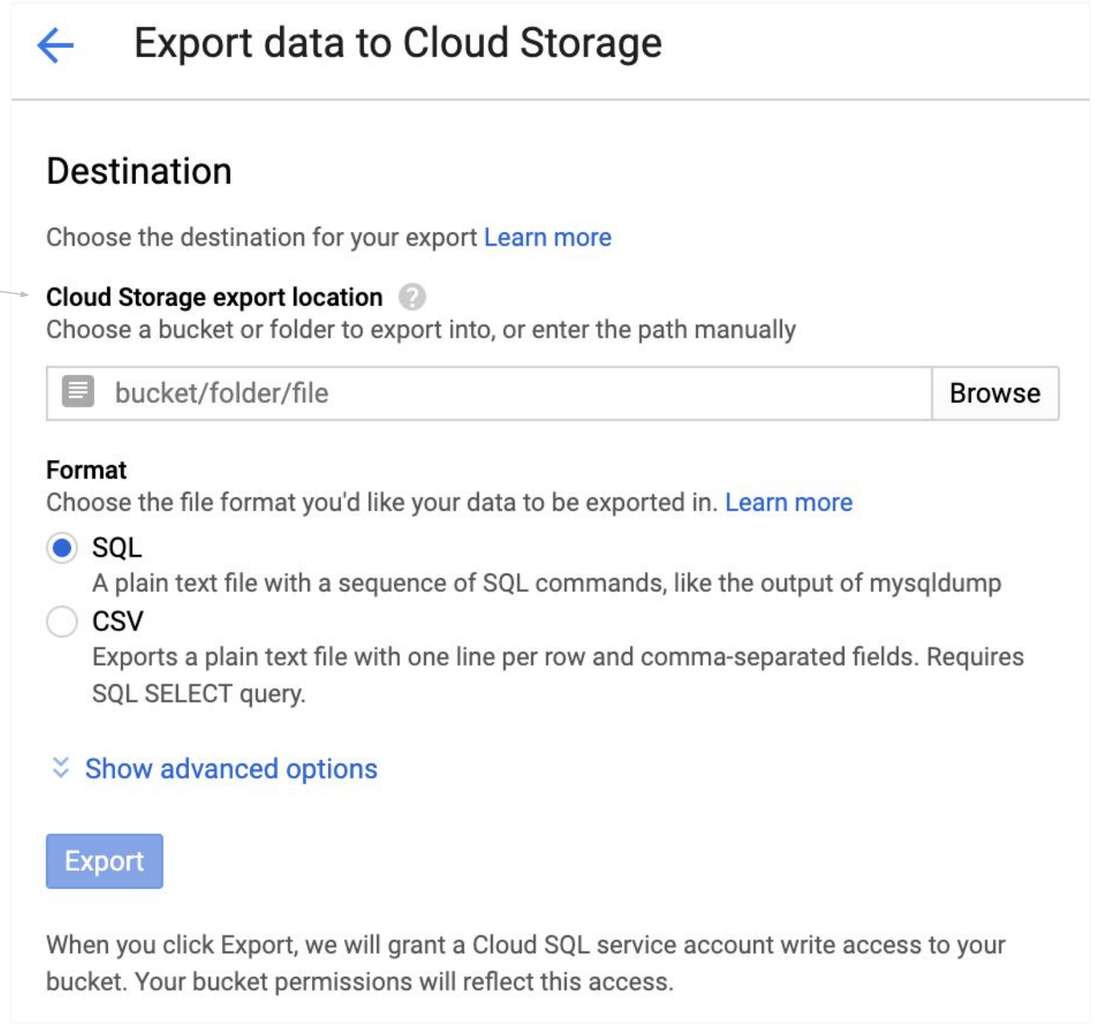


Cloud SQL: Data Export

Export (to GCS)

- ➔ SQL - high fidelity
- ➔ CSV - database-agnostic

Note:
Export to different buckets in different project is also supported if you have granted the service account with write permissions on this bucket.



Exam Tip: *For regular & automatic Cloud SQL exports, use Cloud Functions and Cloud Scheduler.*

Diagnostic Question Discussion

You are implementing a single Cloud SQL MySQL second-generation database that contains business-critical transaction data. You want to ensure that the minimum amount of data is lost in case of logical data inconsistency.

Which two features should you implement? (Choose two.)

A. Sharding

B. Read replicas

C. Binary logging

D. Automated backups

E. Semisynchronous replication

Diagnostic Question Discussion

You are implementing a single Cloud SQL MySQL second-generation database that contains business-critical transaction data. You want to ensure that the minimum amount of data is lost in case of logical data inconsistency.

Which two features should you implement? (Choose two.)

A. Sharding

B. Read replicas

C. Binary logging

D. Automated backups

E. Semisynchronous replication

Cloud SQL: Connection Options

Exam Tip: *Make sure to know when to use which pattern: Cloud SQL Connection options*

Exam Tip: *Common solution to questions about connectivity from a GKE cluster to Cloud SQL*

Connection option	Secure, encrypted?	More information	Notes
Public IP address with SSL	Yes	• Configuring SSL for Instances • Configuring access for IP connections • Connect mysql client using SSL	SSL certificate management required.
Public IP address without SSL	No	• Configuring access for IP connections	Not recommended for production instances.
Cloud SQL Proxy	Yes	• Connecting from an external application using the Cloud SQL Proxy • Connecting mysql Client Using the Cloud SQL Proxy • About the Cloud SQL Proxy	
Cloud SQL Proxy Docker image	Yes	• Connecting mysql Client Using the Cloud SQL Proxy Docker Image • About the Cloud SQL Proxy	
JDBC Socket Library	Yes	• External connections with Java • JDBC socket factory GitHub page	Java programming language only.
Go Proxy Library	Yes	• External connections with Go • Cloud SQL Proxy GitHub page	Go programming language only.
Cloud Shell	No	• Using the mysql client in the Cloud Shell	Uses the Cloud SQL Proxy to easily connect from the Google Cloud Console. Best for quick administration tasks requiring the `mysql` command-line tool.
Apps Script	Yes	• External connections with Apps Script • Apps Script sample GitHub page	Apps Script can connect to external databases through the JDBC service, a wrapper around the standard Java Database Connectivity technology.

Cloud SQL

IP address assignment

Private IP:

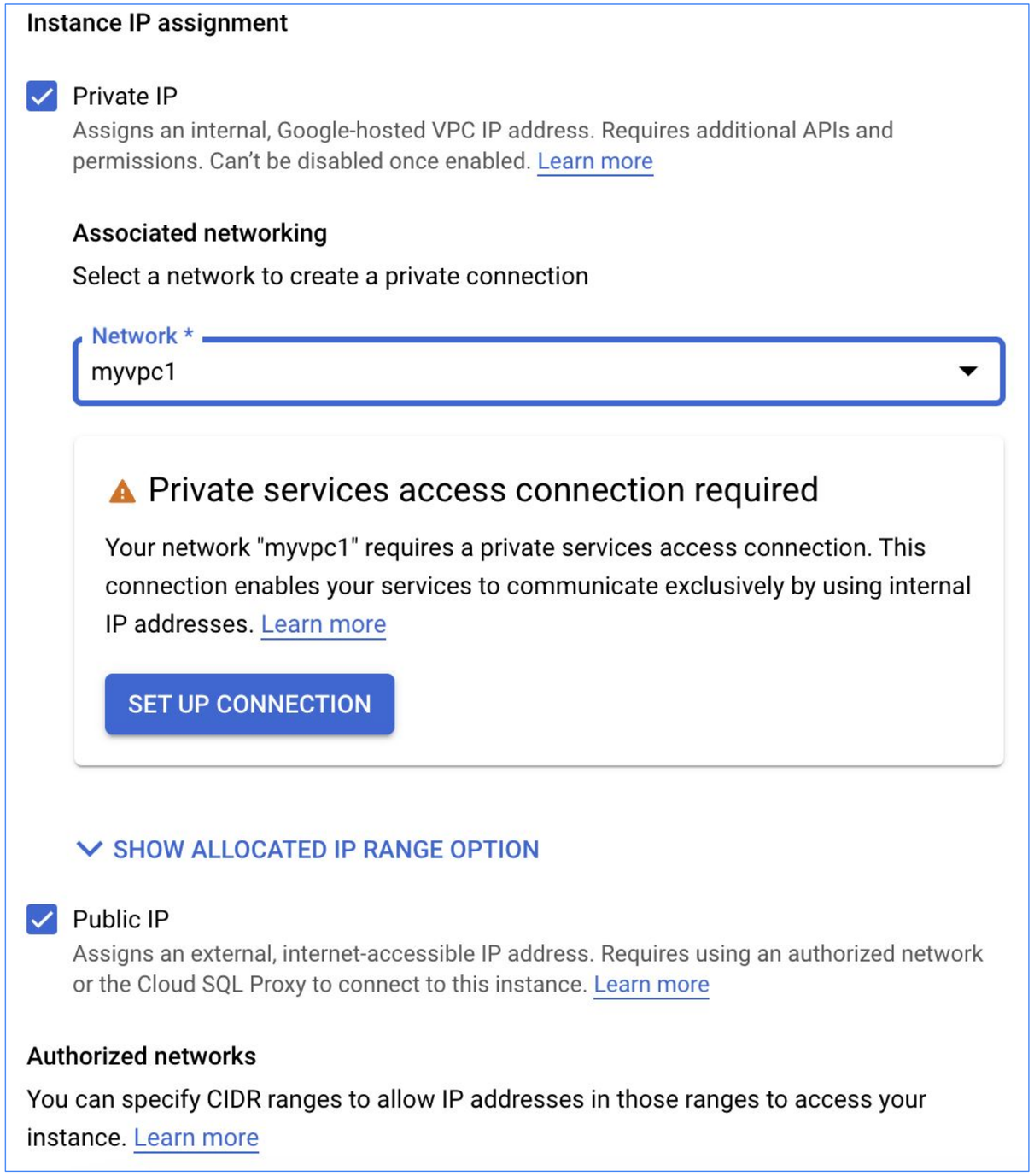
- Preferred when client is coming from resource with internal visibility (not necessarily from the same VPC!
- IPv4 address accessible from VPC
- Connections **may** be configured to use Cloud SQL proxy or self-managed SSL certificates
- Low latency and increased security

Public IP:

- IPv4 address accessible from the public network
- Connections **must** be authorized using either the Cloud SQL Auth proxy or authorized networks

Exam Tip: *Cloud SQL instances can have **both** a public and a private IP address. If private IP address is configured, Private Service Access (technically: VPC peering) is configured underneath.*

MUST-WATCH VIDEO

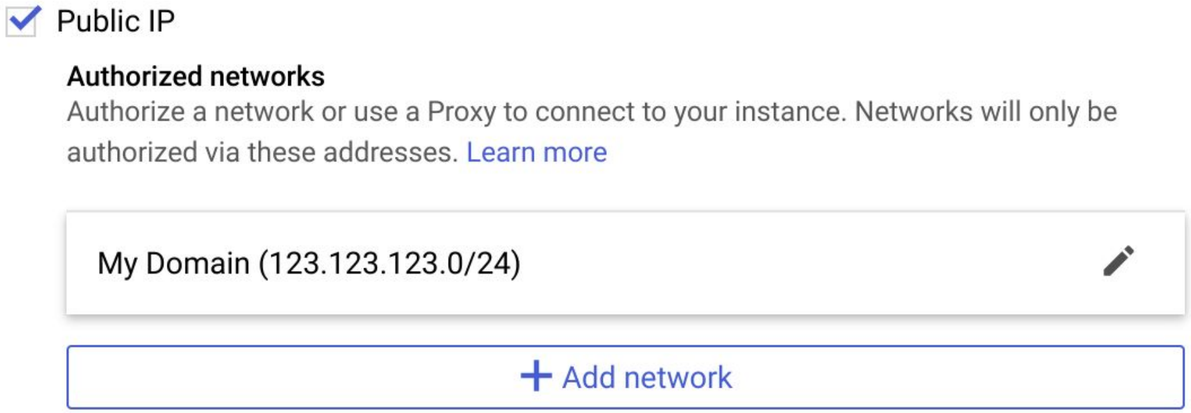


Cloud SQL: Public IP & risk mitigation

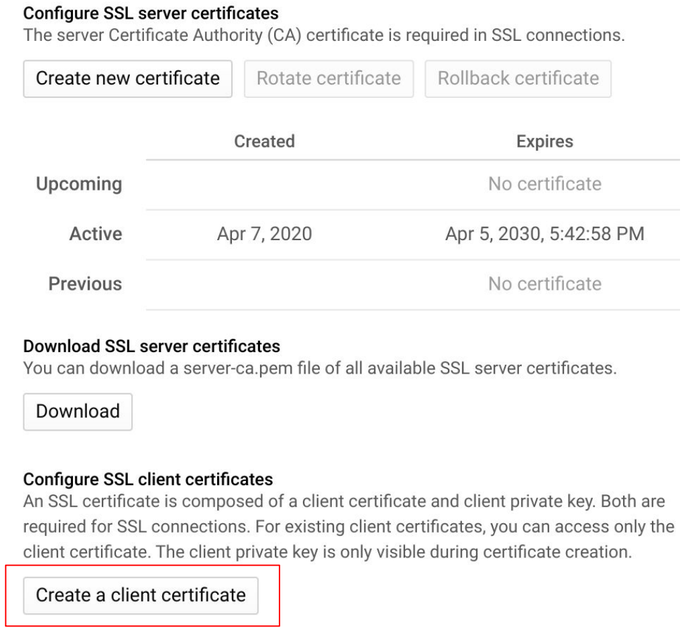
Access by public IP, without SSL : maximum risk for your data !!

Risk mitigation options:

Set an authorized network domain



Use SSL Certificate for transit data




```
psql "sslmode=verify-ca sslrootcert=server-ca.pem \
      sslcert=client-cert.pem sslkey=client-key.pem \
      hostaddr=01.23.45.67 \
      user=postgres dbname=postgres"
```

Cloud SQL: Private IP

Characteristics

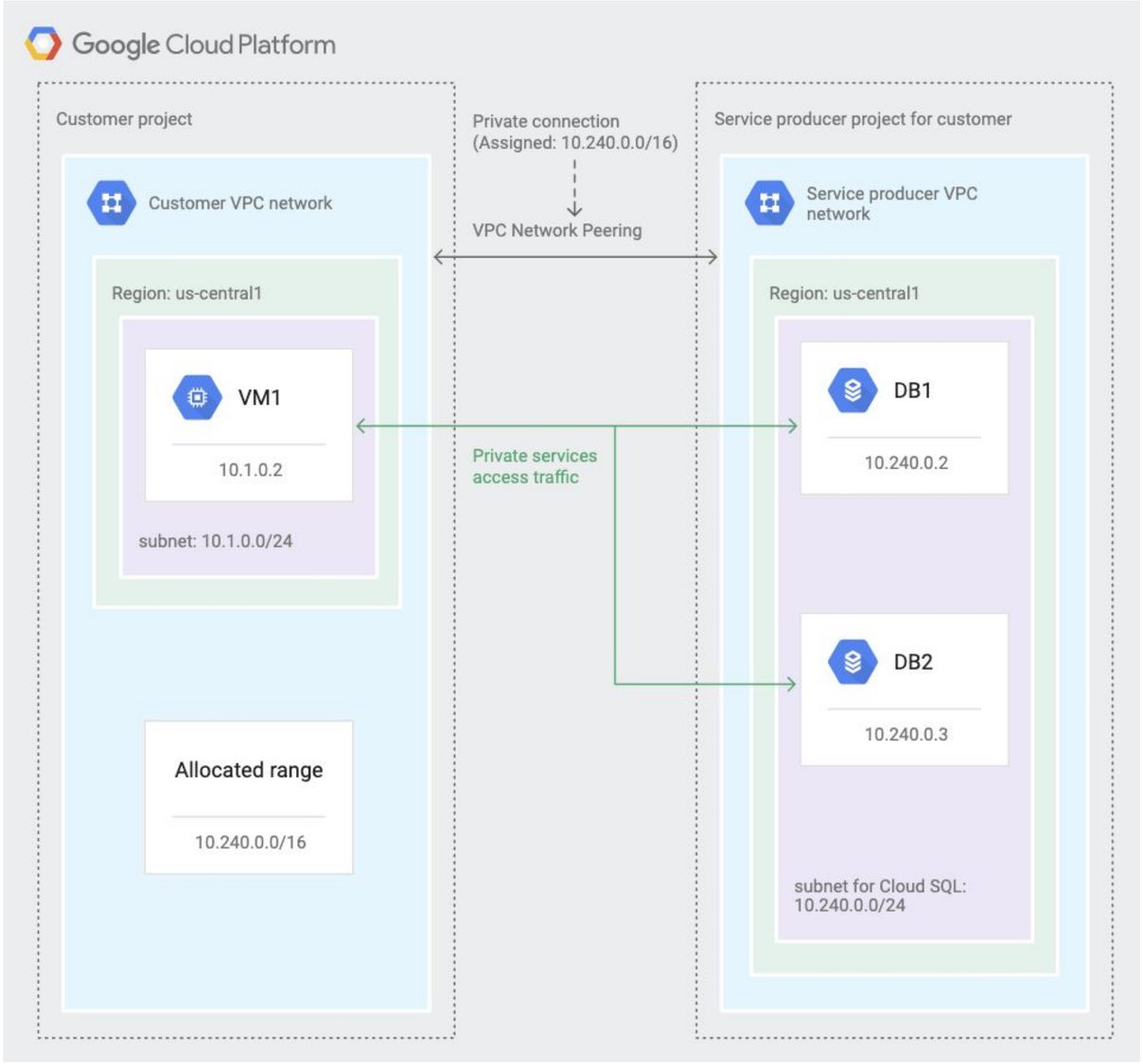
- Allows VM instances in your VPC network to use internal IP addresses to reach the service resources that have internal IP addresses
  → i.e. Connect CloudSQL to GCE or GKE instances
- **GCP uses network peering to create connection**

Benefits

- **Lower network latency**
  Best performance
- **Improved network security**
  Traffic is never exposed to public internet
- **Lower egress cost**
  Regular network pricing still applies to all traffic.

Limitations

- **Max 25 Peering connection per VPC network**
- **Transitive peering is not supported.**
- **Subnet in Peered VPC cannot overlap with CloudSQL**



Cloud SQL

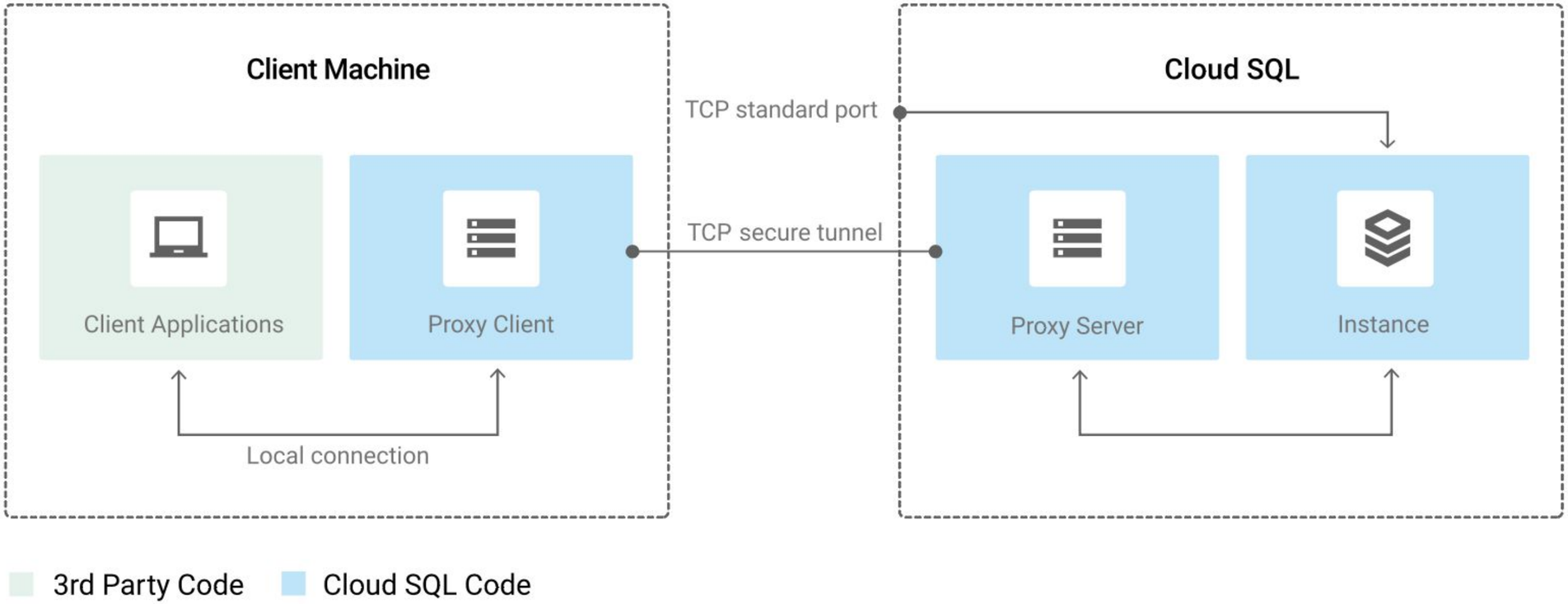
Access authorization -> Cloud SQL Auth proxy details

How the Cloud SQL Auth proxy works?

- a local client running in the local environment + companion process running on the server.
- doesn't provide connection pooling, but can be paired with other connection pooling to increase efficiency.
- also available as a Docker container.

Exam Tips:

- *Cloud SQL Proxy is the recommended option even when connecting to Cloud SQL behind a Private IP (because of strong encryption and authentication using IAM)*



Diagnostic Question Discussion

You have deployed an application to Google Kubernetes Engine (GKE), and are using the Cloud SQL proxy container to make the Cloud SQL database available to the services running on Kubernetes. You are notified that the application is reporting database connection issues. Your company policies require a post-mortem.

What should you do?

A. Use gcloud sql instances restart.

B. Validate that the Service Account used by the Cloud SQL proxy container still has the Cloud Build Editor role.

C. In the GCP Console, navigate to Cloud Logging. Consult logs for (GKE) and Cloud SQL.

D. In the GCP Console, navigate to Cloud SQL. Restore the latest backup. Use kubectl to restart all pods.

Diagnostic Question Discussion

You have deployed an application to Google Kubernetes Engine (GKE), and are using the Cloud SQL proxy container to make the Cloud SQL database available to the services running on Kubernetes. You are notified that the application is reporting database connection issues. Your company policies require a post-mortem.

What should you do?

A. Use gcloud sql instances restart.

B. Validate that the Service Account used by the Cloud SQL proxy container still has the Cloud Build Editor role.

C. In the GCP Console, navigate to Cloud Logging. Consult logs for (GKE) and Cloud SQL.

D. In the GCP Console, navigate to Cloud SQL. Restore the latest backup. Use kubectl to restart all pods.

Cloud SQL

Access authentication

- Basic roles (should NOT be used!):
  - Owner (Full access and control for all Google Cloud resources)
  - Editor (Read-write access to all Google Cloud resources)
  - Viewer (Read-only access to all Google Cloud resources)

Common Cloud SQL IAM Roles:

Role (predefined)	**Privileges**	**For who/which service**
Cloud SQL Admin	Full control for all Cloud SQL resources.	DBA Team / DB owner
Cloud SQL Editor	Manage Cloud SQL resources. No ability to see or modify permissions, nor modify users or sslCerts. No ability to import data or restore from a backup, nor clone, delete, or promote instances. No ability to start or stop replicas. No ability to delete databases, replicas, or backups.	DB Operator
Cloud SQL Viewer	View all Cloud SQL resources (read-only)	Audit, Security, DevOps Team
Cloud SQL Client	Connectivity access to Cloud SQL instances from App Engine and the Cloud SQL Proxy. Not required for accessing an instance using IP addresses.	Apps service (AppEngine, CloudSQL Auth Proxy)

Exam Tip: *Understand permissions in predefined Cloud SQL roles: Admin / Editor / Viewer / Client.*

CloudSQL

#GCPSketchnotes

@PVERGADIA THECLOUDGIRL.DEV

What is CloudSQL?

FULLY MANAGED RELATIONAL DB FOR

MySQL PostgreSQL SQL Server

How does it WORK?

CREATE

region
+ zone
+ machine type (cpu & memory)
+ storage (SSD or HDD)
= Instance

- [x] Enable automatic storage increases

BACKUPS

- [x] Automate backups [time windows]
- [x] Enable point-in-time recovery

HIGH AVAILABILITY

Automatic failover to another zone or region

ZONE A
AUTOMATIC FAILOVERS
ZONE B

How do you USE it?

CONNECTIVITY WITH OTHER SERVICES

CloudSQL connects to App Engine, GKE, GCE, Cloud Run and Workstation

CloudSQL

Steps to MIGRATE

EXISTING MYSQL DB TO CLOUDSQL

1 2 3 4

1. PROVIDE details on your data source
2. CREATE a Cloud SQL read replica
3. SYNC read replica with source
4. PROMOTE read replica to primary instance (optional)

SECURITY for CloudSQL?

ENCRYPTED AT REST & IN MOTION

CloudSQL PRICING

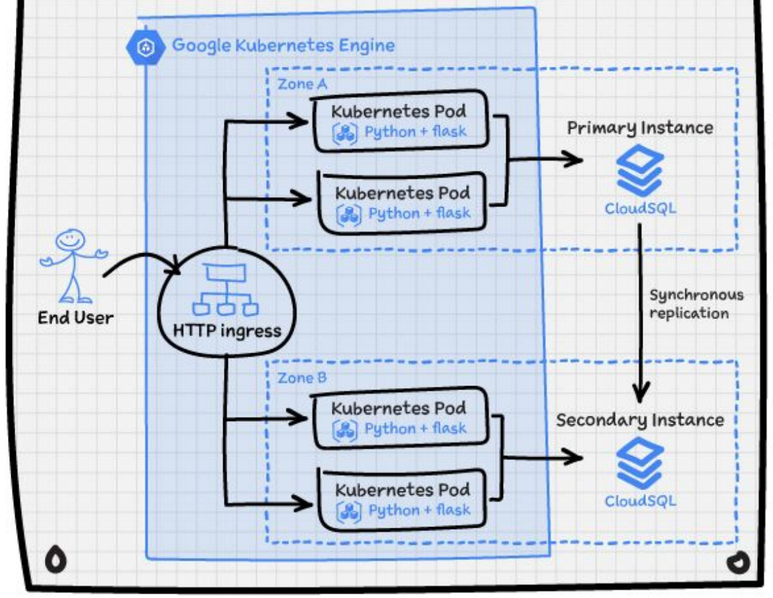
IN GENERAL PRICING IS A FACTOR OF:

Instance + CPU + Memory + Storage + Network Cost

$

CloudSQL Use case (example)

- [x] Online Transaction processing (OLTP)
- [x] Frequent queries
- [x] Fast response times



EHR Healthcare

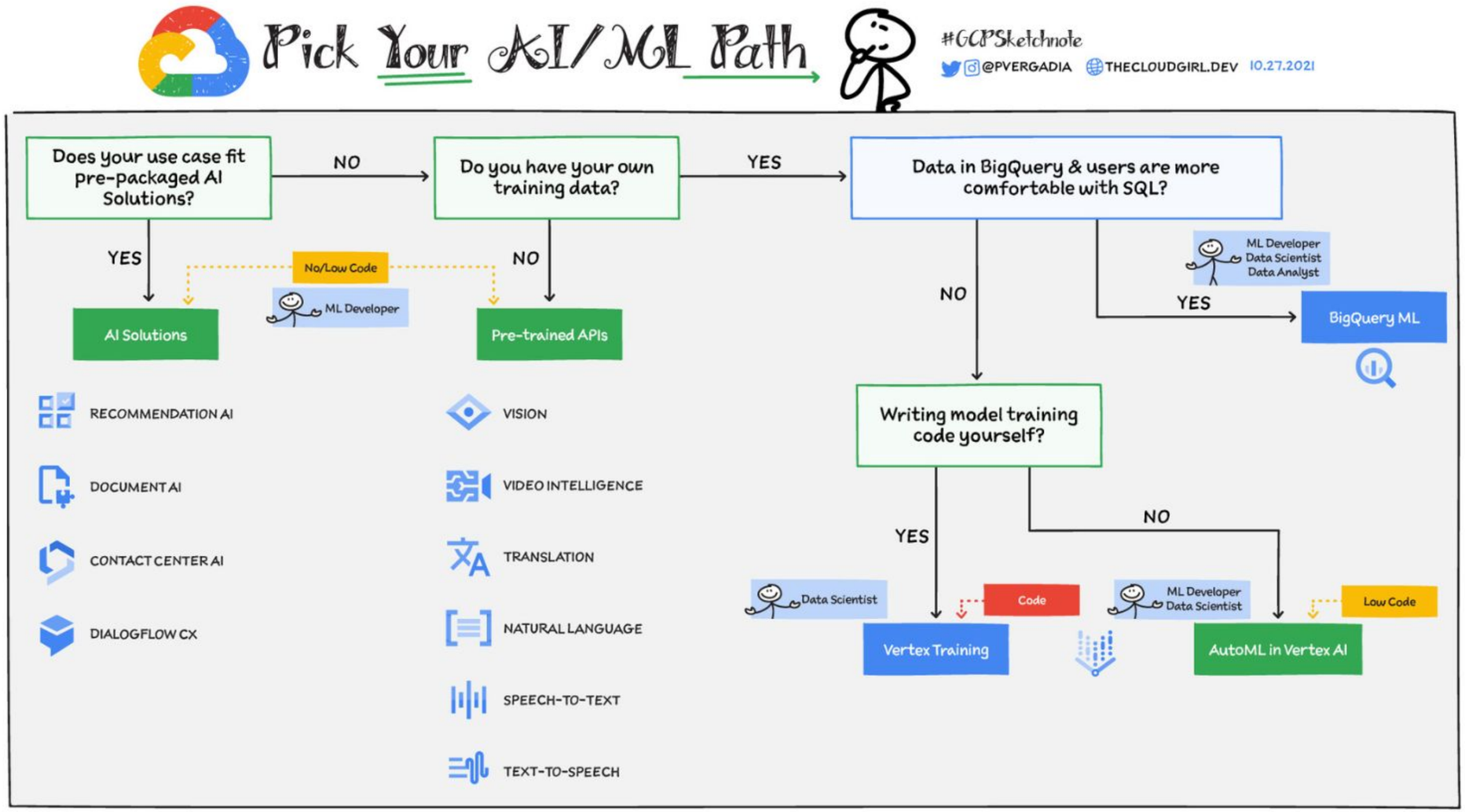
case study

Proposed Technical Solution

EHR HEALTHCARE

- Data protection: HIPAA, Sensitive Data Protection, data encryption (possibly CMEK, 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 / Cloud Service Mesh (“multiple, potentially different environments”)
  - consistent management, possibly from a single system: Config Controller
  - Manage traffic and execute resiliency tests with Service Mesh: Fault Injection, Circuit Breaking, Request Timeouts
- MySQL + MS SQL Server -> Cloud SQL (DMS for migration); 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: Cloud Build + Artifact Registry.
- Ingesting and processing data from new providers: ETL pipeline (possibly Pub/Sub -> Dataflow -> BigQuery)
- Dynamic provisioning of new environments: IaaC (Terraform).
- Making predictions: ML in the form of Vertex AI / AutoML / BigQuery ML / pre-built models (nothing very concrete)
- Generate reports on industry trends based on provider data: Vertex AI Search for Healthcare
- Security products: Cloud Armor, Security Command Center

Google Cloud (pre Gen-AI) machine learning spectrum



Exam Tip: *4 high-level ways to approach ML in GCP. All depends on particular use-case, but the approach should be like with compute: start from more managed / easier approaches and choose more advanced ones only if needed.*

[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 materials

[READING]

- Pub/Sub notifications for Cloud Storage
- Read about Database Migration Service.
- [pre Gen-AI!] How to choose optimal AI/ML path in GCP?

[VIDEOS]

- Cloud Networking 103 (Securing Network): Cloud OnAir: CE TV: Google Cloud Networking 103 - Securing your Network
- How to transfer data to GCS: How to transfer data to Google Cloud? #GCPSketchnote
- Authentication controls for Cloud Storage
- [IMPORTANT!] Different patterns for connecting to Cloud SQL: Cloud SQL: Concepts of Networking
- Great demo of how to centralize network management and set up Shared VPC in GCP: Level Up From Zero Episode 4: Shared VPC
- Accelerating cloud migrations with managed databases: Accelerating cloud migration with managed databases
- [Highly recommended] Choose your database on Google Cloud: Choose your database on Google Cloud
- Introducing Database Migration Service: Introducing Database Migration Service
- How to achieve high resiliency and availability with GCP: How to achieve high resiliency and availability with Google Cloud infrastructure
- Infrastructure as code with Terraform and Cloud Run: Infrastructure as code with Terraform and Cloud Run
- Build ETL Pipelines using Cloud Dataflow: Build ETL Pipelines using Cloud Dataflow

Make sure to…

Enjoy the journey as much as the destination!