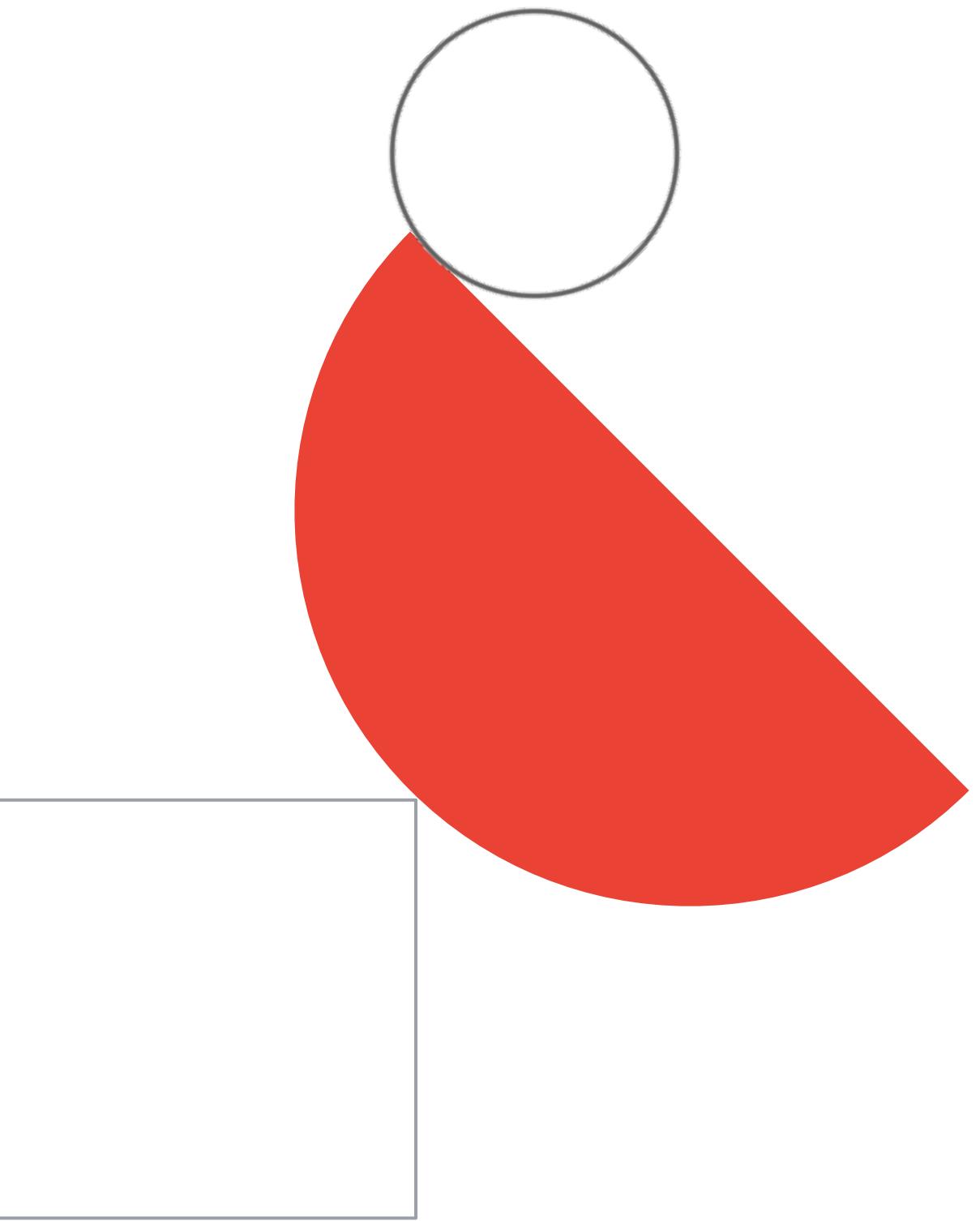
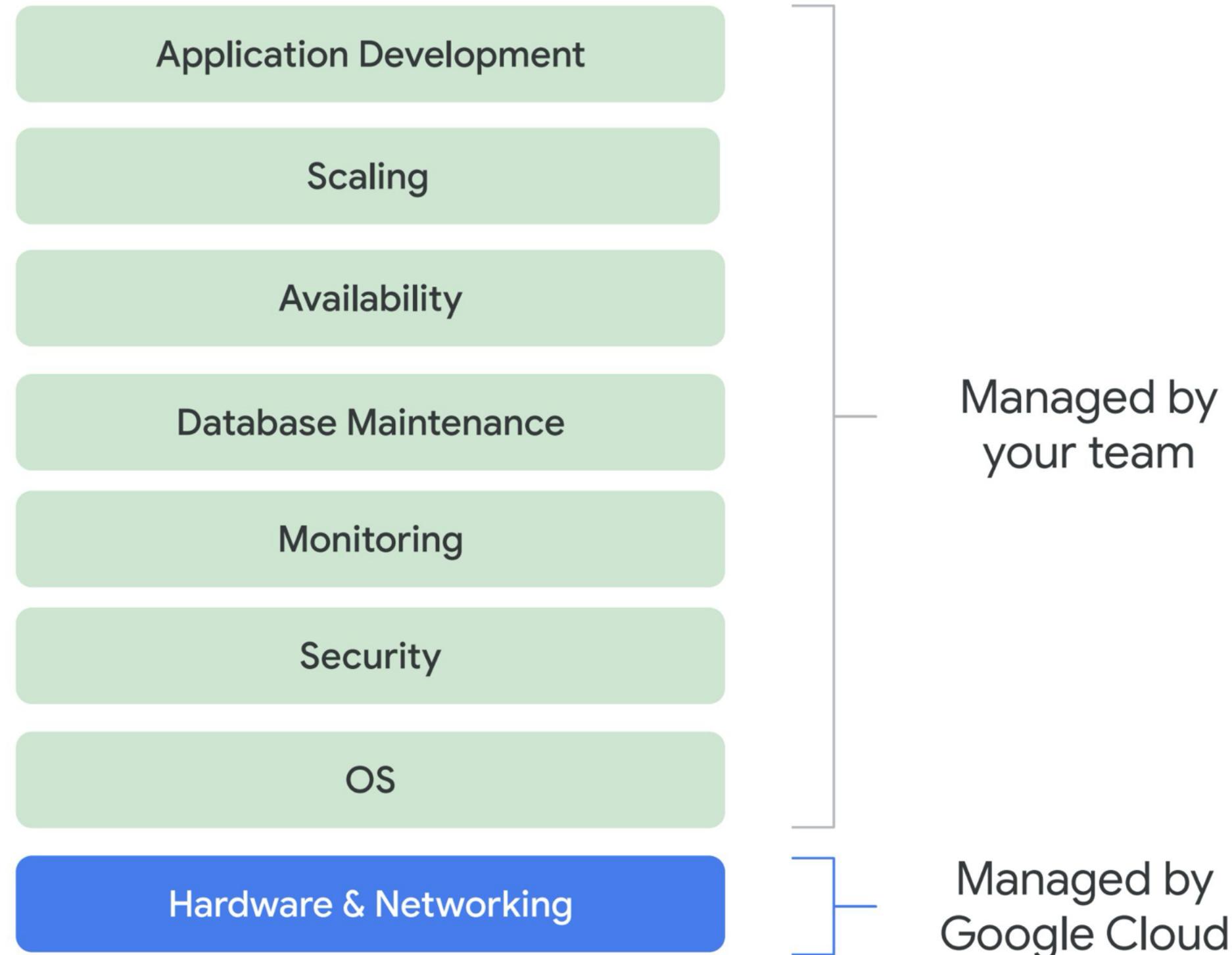


Cloud SQL



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...

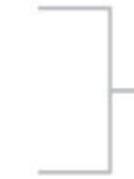
- Provision resources
- Install database engine
- Configure it
- Patch & update
- Handle high availability
- Implement & manage backup & restore
- Resize when needed
- Implement monitoring
- ... and so on

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).

Application Development



Managed by
your team

Scaling

Availability

99.999% SLA

Database Maintenance

Online scaling

Monitoring

Easy global replication

Security

Automatic sharding

OS

Automatic failure recovery

Hardware & Networking

Built into
cloud-native databases

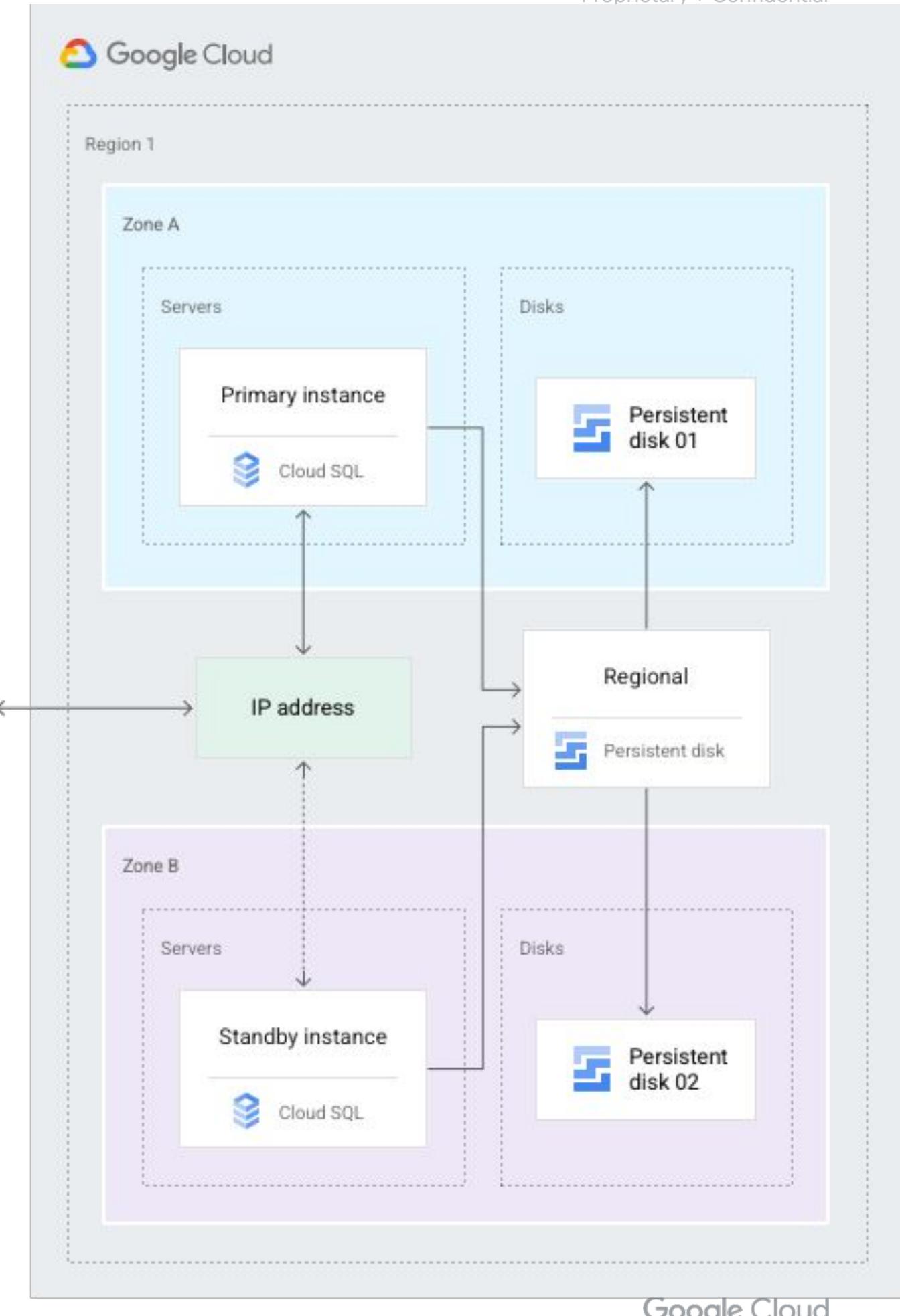


Cloud SQL High availability

- 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:

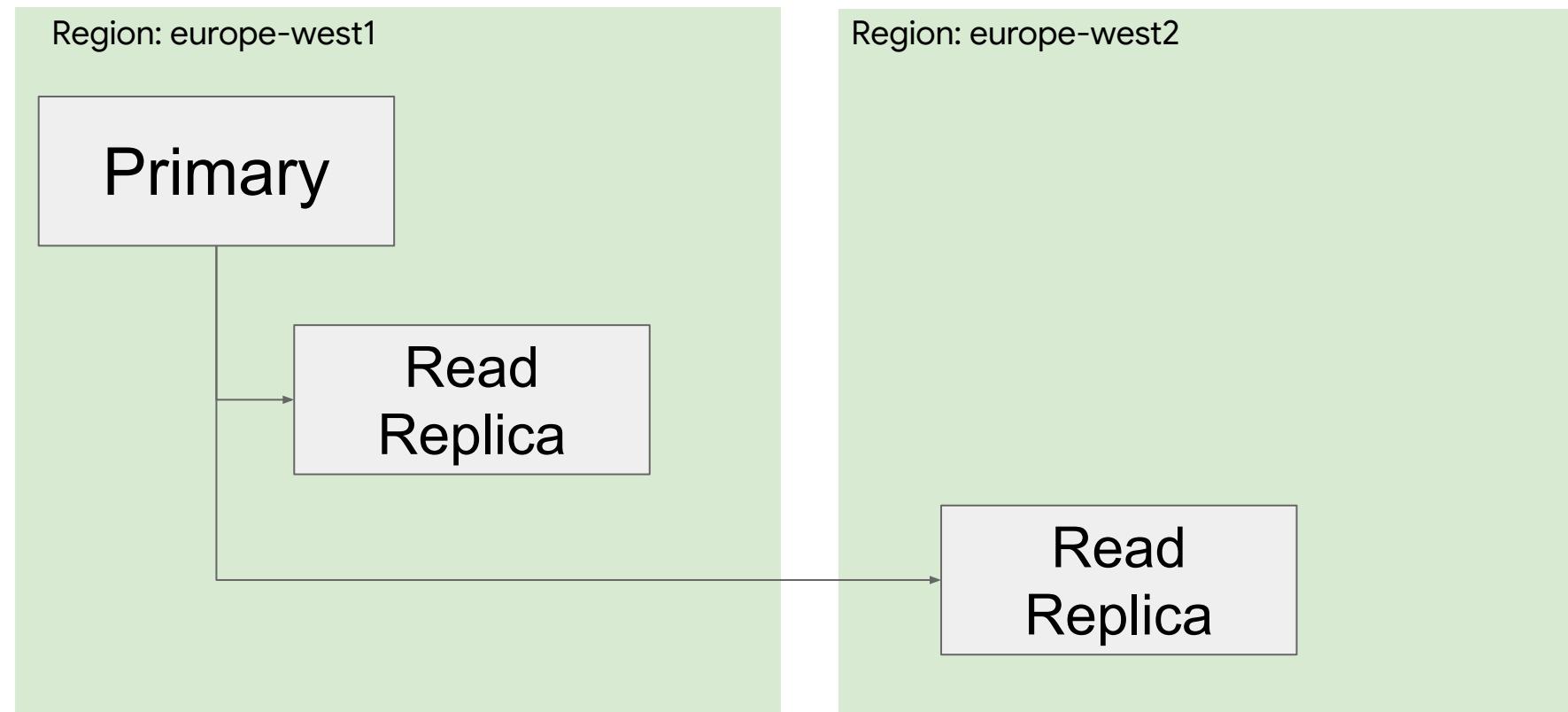
- **Initiate failover:** `gcloud sql instances failover <PRIM_INSTANCE>`
- **Check if instance is / isn't set for HA:** `gcloud sql instances describe (availabilityType = REGIONAL / ZONAL)`



Cloud SQL: Read Replicas

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

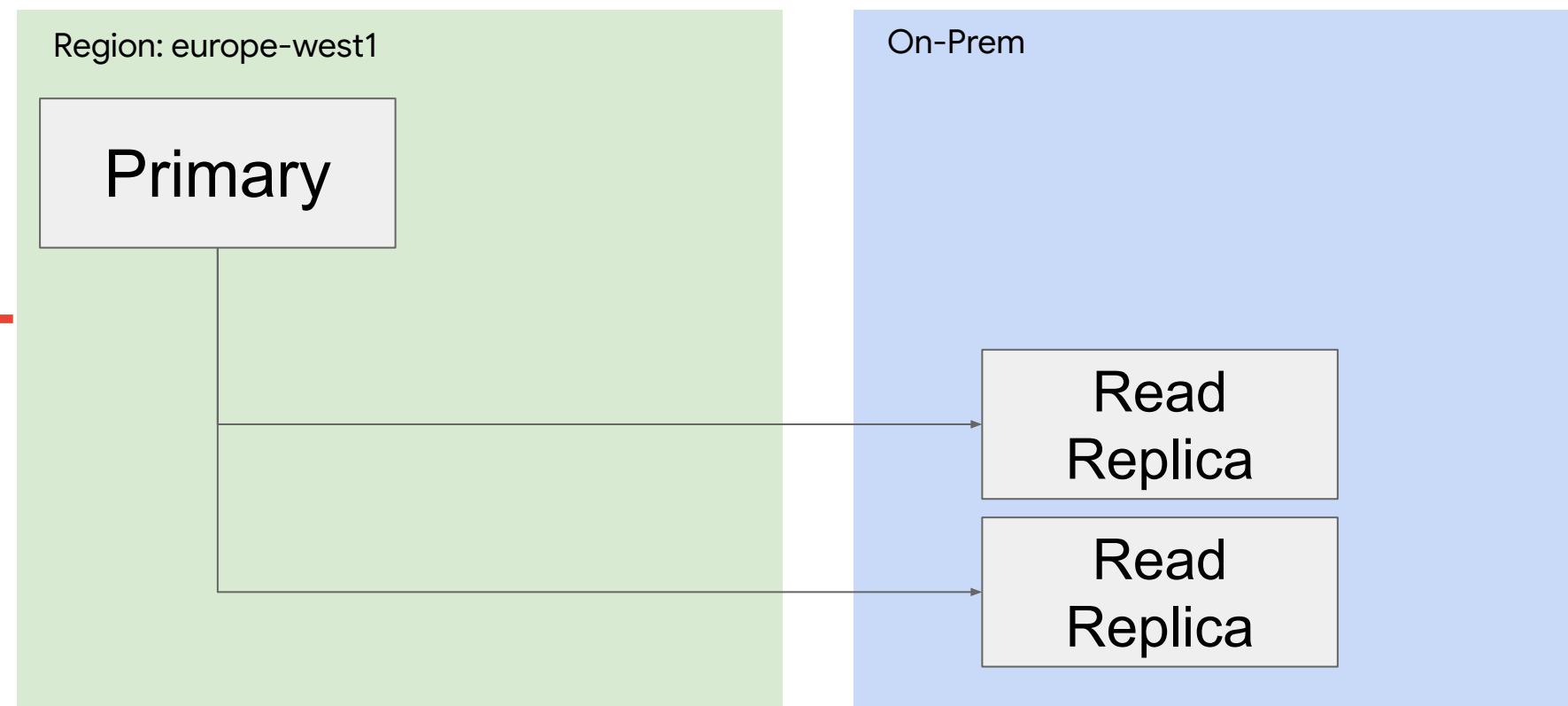
Read Replica
GCP → GCP



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

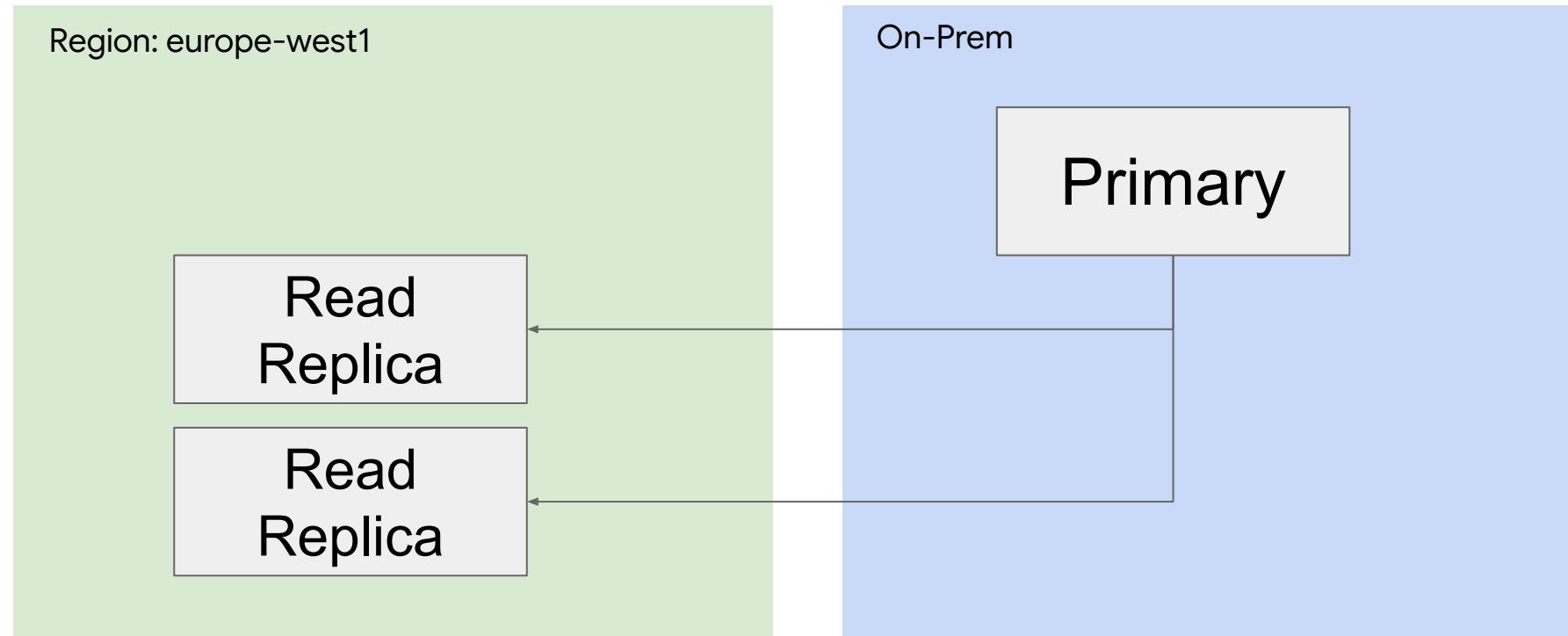
- Reduce latency for external connection
- Analytics target
- Migration path to other platforms
- In case of e.g. network outage on-prem the replication lag might be too large and replicas need to be recreated

Exam Tip: Focus on replicating TO external server

Cloud SQL: Read Replicas

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

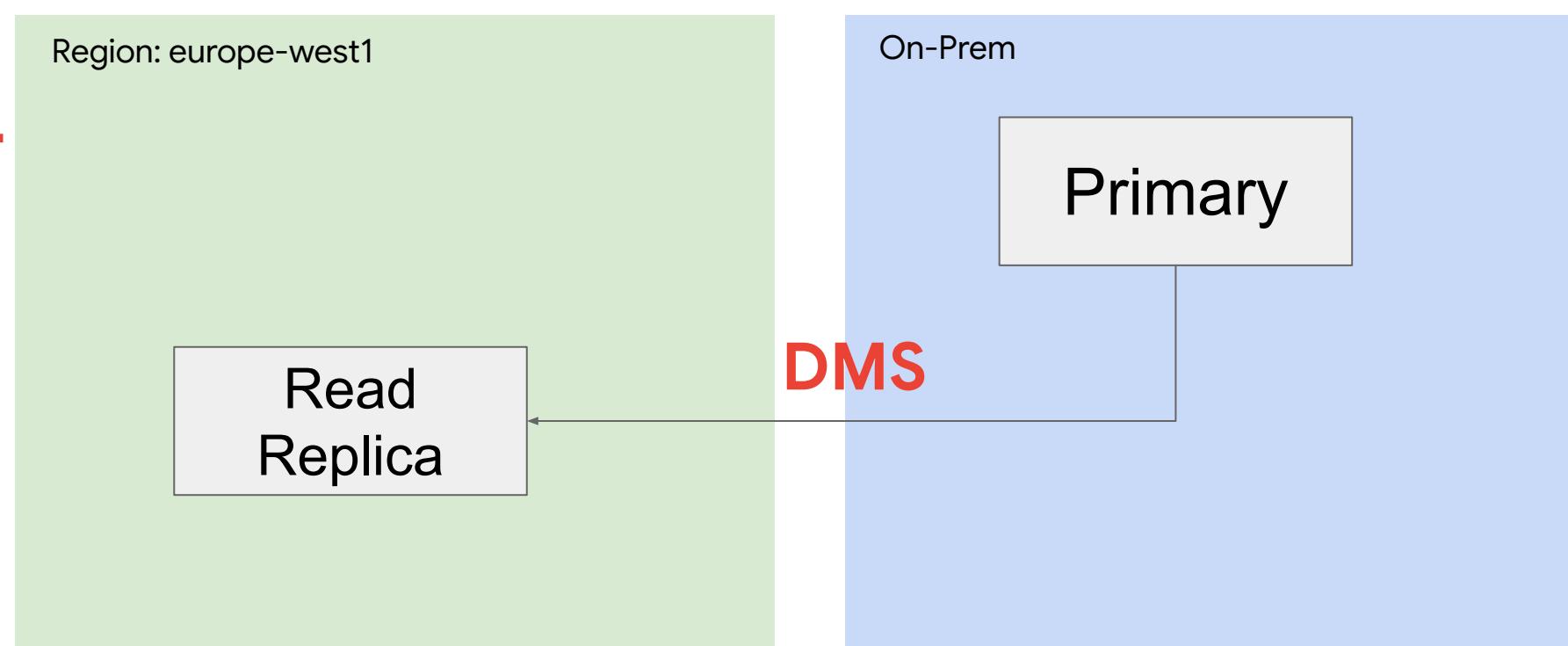
Replication from external server
On-premises → GCP



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)

Replication from external server
On-premises → GCP



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: Focus on replicating *FROM* external server

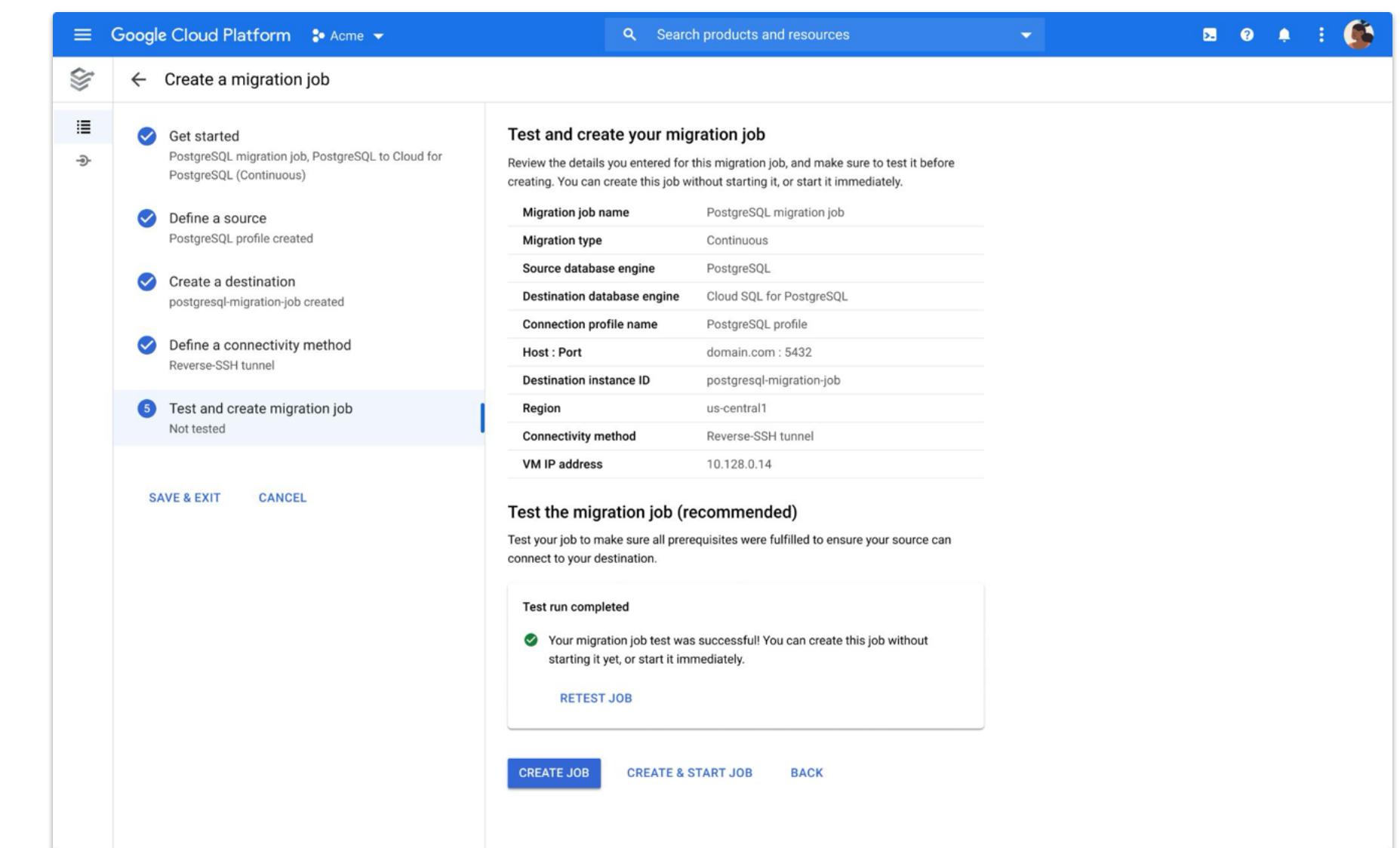
Simplified migration with Data Migration Service (DMS)

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](#).

How to reduce Cloud SQL replication lag

Steps to enable parallel replication:

- On a read replica, [disable replication](#).
- On the read replica, [set the flags for parallel replication](#) (Use the gcloud command to set the flags. [The Google Cloud console option is disabled when replication is disabled](#)):
 - [Slave_parallel_workers](#), [slave_parallel_type](#), [slave_preserve_commit_order](#), [slave_pending_jobs_size_max](#)
- On the read replica, [enable replication](#), using gCloud command or console
- Optionally, on the primary instance, [set the flags](#) to optimize performance for parallel replication.

Exam Tips:

- Have a look at replication lag topic ([MySQL](#) / [PostgreSQL](#) / [SQL Server](#))
- You can use the [replica_lag](#) and [network_lag](#) metrics to [monitor replication lag](#)
- There are [two ways to make a MySQL replica apply changes faster](#):
 - Parallel replication
 - High performance flushing

Exam Tips:

- Know [how to enable & disable replication using gcloud](#)!
 - `gcloud sql instances patch REPLICA_NAME --no-enable-database-replication`
 - `gcloud sql instances patch REPLICA_NAME --enable-database-replication`
- Know how to set a flag:
 - `gcloud sql instances patch INSTANCE_NAME --database-flags=FLAG1=VALUE1`

Cloud SQL DR with cross-region Read Replicas

How to create

The screenshot shows the Google Cloud SQL interface for creating a read replica of a primary instance named "postgresql-db-golden-demo".

- Primary Instance:** Overview, System insights (NEW), Query insights, Connections, Users, Databases, Backups, **Replicas** (selected), Operations.
- Instance info:** Instance ID * **postgresql-db-golden-demo-replica** (lowercase letters, numbers, and hyphens. Start with a letter.), Database version PostgreSQL 14.
- Summary:** Region us-central1 (Iowa), DB Version PostgreSQL 14, Connections Private IP, Public IP.
- Choose region and zonal availability:** For better performance, keep your data close to the services that need it. Region is permanent, while zone can be changed any time.
 - Region:** us-central1 (Iowa) (selected).
 - Zonal availability:**
 - Single zone:** In case of outage, no failover. Not recommended for production.
 - Multiple zones (Highly available):** Automatic failover to another zone within your selected region. Recommended for production instances. Increases cost.
- SPECIFY ZONES:** Customizable later.
- Customize your instance:** You can also customize instance configurations later.
- SHOW CONFIGURATION OPTIONS:** CREATE REPLICA (blue button), CANCEL.

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!

!!!!

Instance has replicas

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

OK

Cloud SQL: edit instance

Zone	Y	The possible values depend on the region.		
Database version	N	Console string PostgreSQL 14 PostgreSQL 13 (default) PostgreSQL 12 PostgreSQL 11 PostgreSQL 10 PostgreSQL 9.6	API enum string POSTGRES_14 POSTGRES_13 POSTGRES_12 POSTGRES_11 POSTGRES_10 POSTGRES_9_6	
Set password policy	Y	Configured or not.		
Private IP		After it is enabled, it cannot be disabled.	Enabled or disabled.	
Public IP	Y	Enabled or disabled.		
Authorized networks	Y	If Public IP is enabled, IP addresses authorized to connect to the instance. You can also specify this value as an IP address range, in CIDR notation .		
Private path for Google Cloud services	Y	Enabled or disabled.		
Machine type	Y	Select from Shared core, Lightweight, Standard (Most common), or High memory. Select the Custom radio button to create a custom machine type. Learn more		

Exam Tips:

- Can be done with command: `gcloud sql instances patch INSTANCE_NAME --<setting_name> <value>`
- Have a look at the [parameter list](#), know the most important ones and focus if those can be changed AFTER instance creation or not.
- Storage (=regional PD) size CANNOT be reduced (just like with normal VMs)

Cloud SQL - Performance & scaling

Machine Type

Choose a preset or customize your own. For better performance, choose a machine type with enough memory to hold your largest table.

Shared core

- 1 vCPU, 0.614 GB
- 1 vCPU, 1.7 GB

Custom

vCPUs *

96

1 - 96

Memory *

624

86.5 - 624

Storage

Storage type

Choice is permanent. Storage type affects performance.

SSD (Recommended)

Most popular choice. Lower latency than HDD with higher QPS and data throughput.

HDD

Lower performance than SSD with lower storage rates.

Storage capacity

10 - 65,536 GB. Higher capacity improves performance, up to the limits set by the machine type. Capacity can't be decreased later.

10 GB

Enable automatic storage increases

If enabled, whenever you are nearing capacity, storage will be incrementally (and permanently) increased. [Learn more](#)

Storage

Storage type

Choice is permanent. Storage type affects performance.

SSD (Recommended)

Most popular choice. Lower latency than HDD with higher QPS and data throughput.

HDD

Lower performance than SSD with lower storage rates.

Storage capacity

10 - 65,536 GB. Higher capacity improves performance, up to the limits set by the machine type. Capacity can't be decreased later.

10 GB

20 GB

100 GB

200 GB

Custom

65536

GB

10 - 65,536

Cloud SQL: storage

Can't change between HDD <-> SSD

- SSD recommended
- Performance scales with size
- HDD / SSD decision is permanent
 - Change requires creating a separate instance and migrating data...
- Balanced disks NOT available for Cloud SQL
- Secondary (HA) instances are of the same size & disk size&type
- Read Replicas can be of larger (not smaller!) size (vCPUs/memory), but the same disk size&type

← Edit test-instance

PRIM...

Machine Type

Choose a preset or customize your own. For better performance, choose a machine type with enough memory to hold your largest table.

High memory

4 vCPU, 26 GB
 8 vCPU, 52 GB
 16 vCPU, 104 GB
 Custom

Storage

Storage type

HDD

Storage capacity

10 - 65,536 GB. Higher capacity improves performance, up to the limits set by the machine type. Capacity can't be decreased later.

10 GB

10 - 65,536

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.

3 Enable auto backups and high availability

Backups and binary logging

Enabling backups protects your data from loss with minimal cost. [Learn more](#)

Automate backups

11:00 AM – 3:00 PM

Choose a window for automated backups. May continue outside window until complete. Time is your local time (UTC+2).

Enable binary logging (required for replication and earlier position point-in-time recovery)

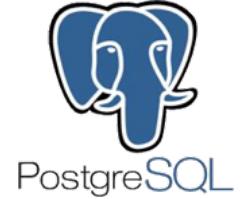
High availability

i Recommended for all production instances to improve fault tolerance. Failover replica is hosted in a different zone from the master and is billed as a separate instance. [Learn more](#)

Create failover replica

Cloud SQL: Point-in-time recovery

recover an instance to a specific point in time



Automated backups and point-in-time recovery

Protect your data from loss at a minimal cost. [Learn more](#)

Automate backups

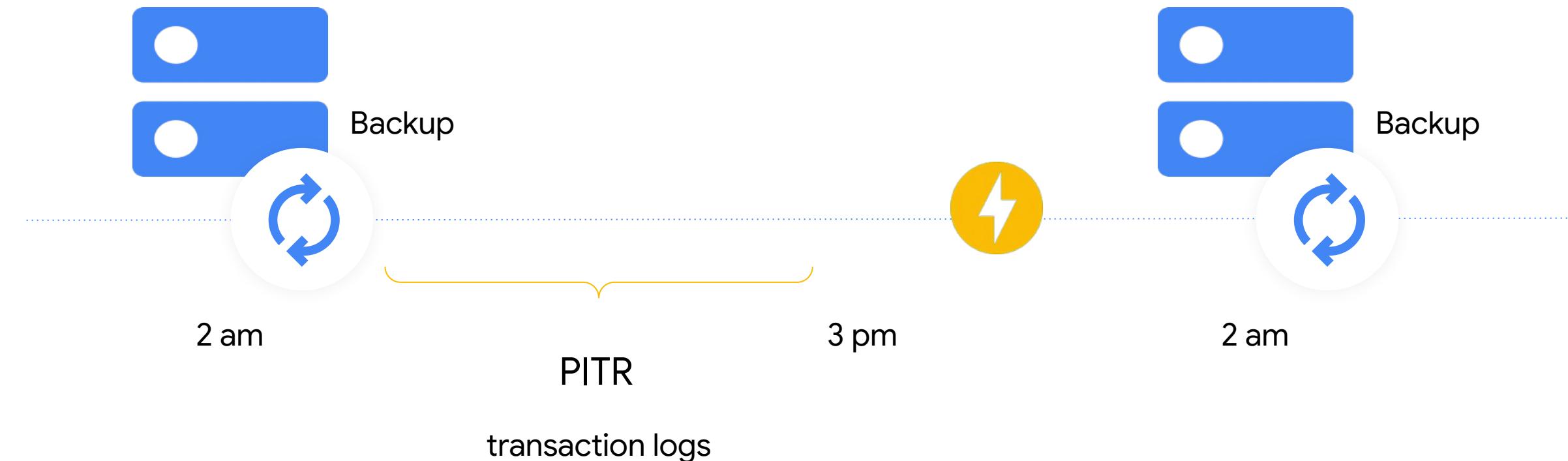
Choose a window of time for your data to be automatically backed up, which may continue outside the window until complete. Time is your local time zone (UTC+1).

11:00 AM – 3:00 PM ▾

▼ ADVANCED OPTIONS

Enable point-in-time recovery

Allows you to recover data from a specific point in time, down to a fraction of a second, via write-ahead log archiving.



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.

← Export data to Cloud Storage

Destination

Choose the destination for your export [Learn more](#)

Cloud Storage export location ?

Choose a bucket or folder to export into, or enter the path manually

bucket/folder/file [Browse](#)

Format

Choose the file format you'd like your data to be exported in. [Learn more](#)

SQL
A plain text file with a sequence of SQL commands, like the output of mysqldump

CSV
Exports a plain text file with one line per row and comma-separated fields. Requires SQL SELECT query.

[Show advanced options](#)

Export

When you click Export, we will grant a Cloud SQL service account write access to your bucket. Your bucket permissions will reflect this access.

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

Google Cloud

Connection Options (external apps)

Exam Tip: Make sure to know when to use which pattern: [Cloud SQL Connection options](#)

Connection option	Secure, encrypted?	More information	Notes
Public IP address with SSL	Yes	<ul style="list-style-type: none">Configuring SSL for InstancesConfiguring access for IP connectionsConnect mysql client using SSL	SSL certificate management required.
Public IP address without SSL	No	<ul style="list-style-type: none">Configuring access for IP connections	Not recommended for production instances.
Cloud SQL Proxy	Yes	<ul style="list-style-type: none">Connecting from an external application using the Cloud SQL ProxyConnecting mysql Client Using the Cloud SQL ProxyAbout the Cloud SQL Proxy	
Cloud SQL Proxy Docker image	Yes	<ul style="list-style-type: none">Connecting mysql Client Using the Cloud SQL Proxy Docker ImageAbout the Cloud SQL Proxy	
JDBC Socket Library	Yes	<ul style="list-style-type: none">External connections with JavaJDBC socket factory GitHub page	Java programming language only.
Go Proxy Library	Yes	<ul style="list-style-type: none">External connections with GoCloud SQL Proxy GitHub page	Go programming language only.
Cloud Shell	No	<ul style="list-style-type: none">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 <code>mysql</code> command-line tool.
Apps Script	Yes	<ul style="list-style-type: none">External connections with Apps ScriptApps Script sample GitHub page	Apps Script can connect to external databases through the JDBC service, a wrapper around the standard Java Database Connectivity technology.

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

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**](#)

Instance IP assignment

Private IP

Assigns an internal, Google-hosted VPC IP address. Requires additional APIs and permissions. Can't be disabled once enabled. [Learn more](#)

Associated networking

Select a network to create a private connection

Network *

myvpc1

⚠ Private services access connection required

Your network "myvpc1" requires a private services access connection. This connection enables your services to communicate exclusively by using internal IP addresses. [Learn more](#)

SET UP CONNECTION

▼ SHOW ALLOCATED IP RANGE OPTION

Public IP

Assigns an external, internet-accessible IP address. Requires using an authorized network or the Cloud SQL Proxy to connect to this instance. [Learn more](#)

Authorized networks

You can specify CIDR ranges to allow IP addresses in those ranges to access your instance. [Learn more](#)

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

Public IP

Authorized networks

Authorize a network or use a Proxy to connect to your instance. Networks will only be authorized via these addresses. [Learn more](#)

My Domain (123.123.123.0/24)



+ Add network

Use SSL Certificate for transit data

Configure SSL server certificates

The server Certificate Authority (CA) certificate is required in SSL connections.

[Create new certificate](#) [Rotate certificate](#) [Rollback certificate](#)

	Created	Expires
Upcoming		No certificate
Active	Apr 7, 2020	Apr 5, 2030, 5:42:58 PM
Previous		No certificate

Download SSL server certificates

You can download a server-ca.pem file of all available SSL server certificates.

[Download](#)

Configure SSL client certificates

An SSL certificate is composed of a client certificate and client private key. Both are required for SSL connections. For existing client certificates, you can access only the client certificate. The client private key is only visible during certificate creation.

[Create a client certificate](#)

```
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

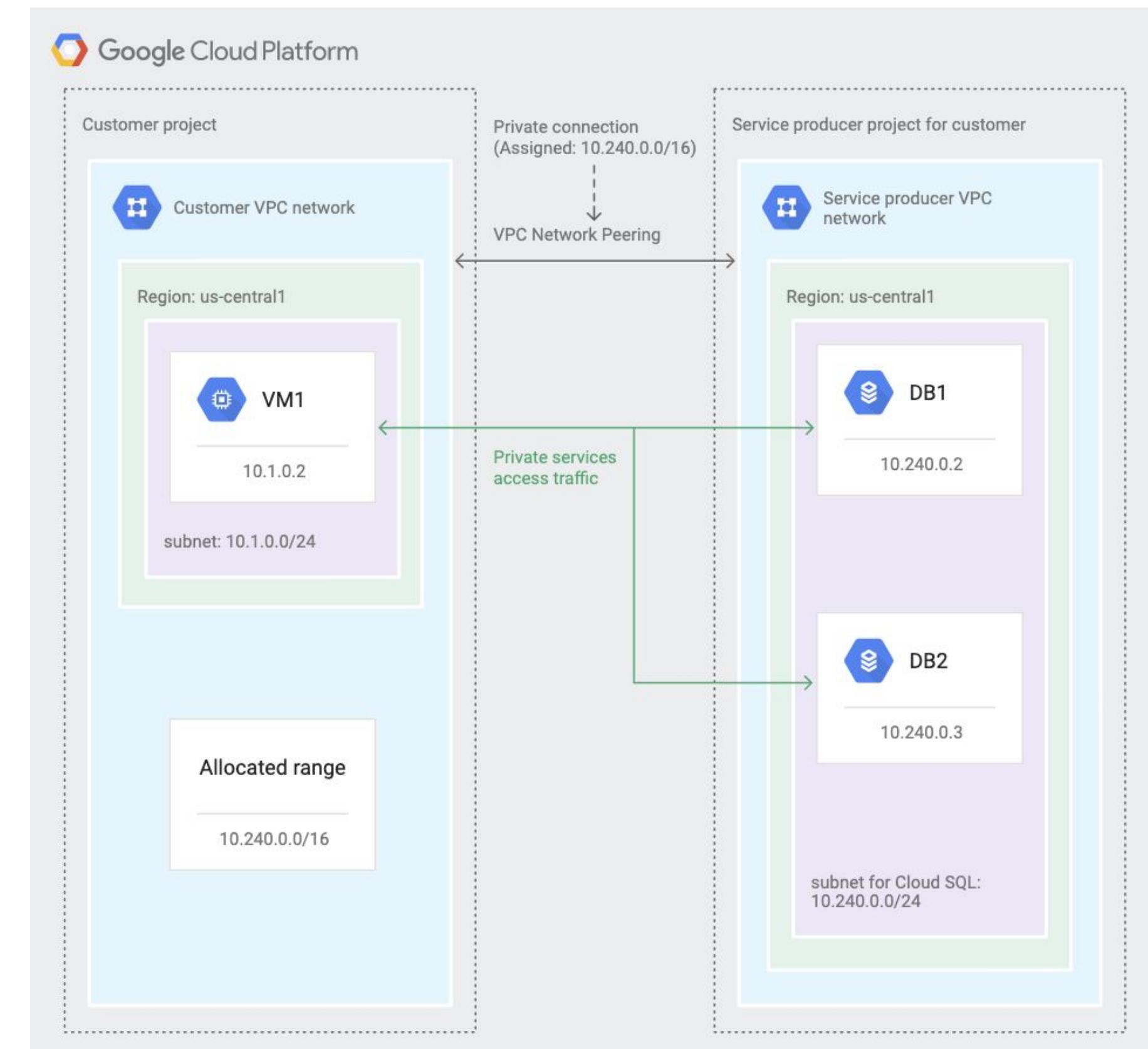
- Allows VM instances in your VPC network to use internal IP addresses to reach the service resources that have internal IP addresses
→ i.e. Connect CloudSQL to GCE or GKE instances
- **GCP uses network peering to create connection**

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 authentication

Common Cloud SQL IAM Roles:

- 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)

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.

Cloud SQL

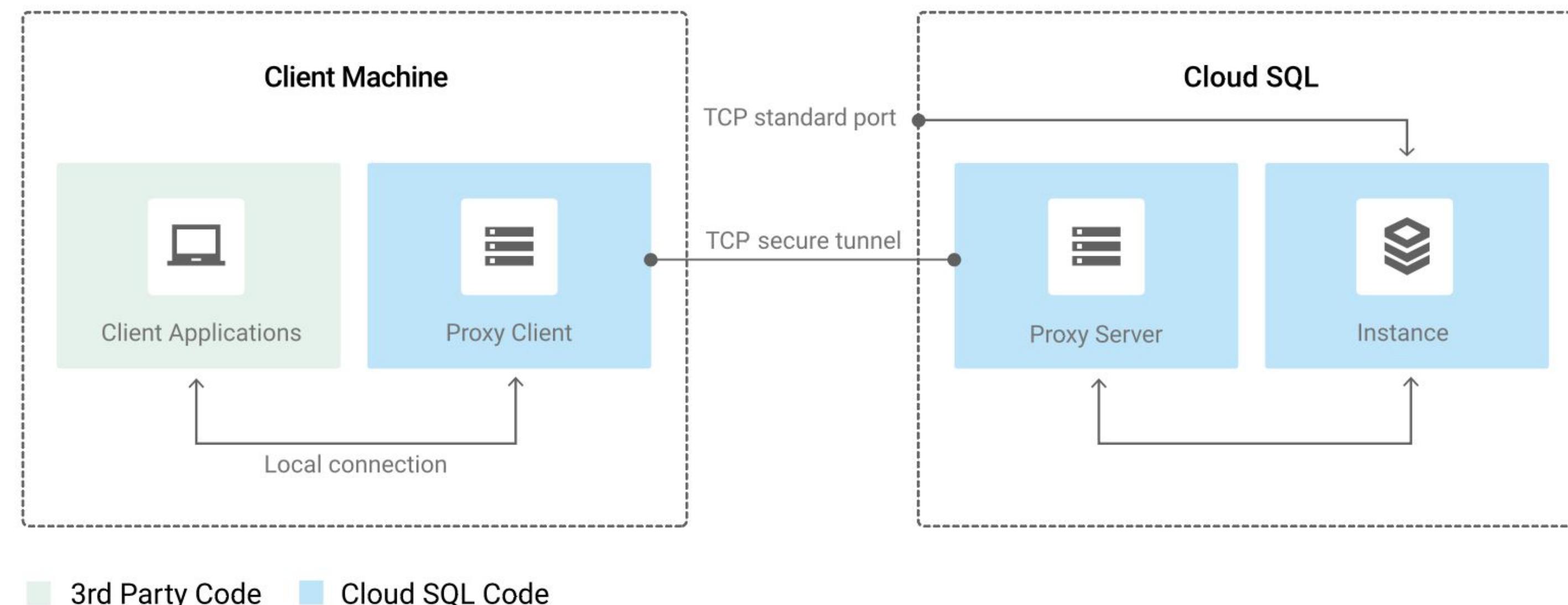
Access authorization -> Cloud SQL Auth proxy details

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)*





CloudSQL

#GCPSketchnotes

@PVERGADIA

THECLOUDGIRL.DEV

