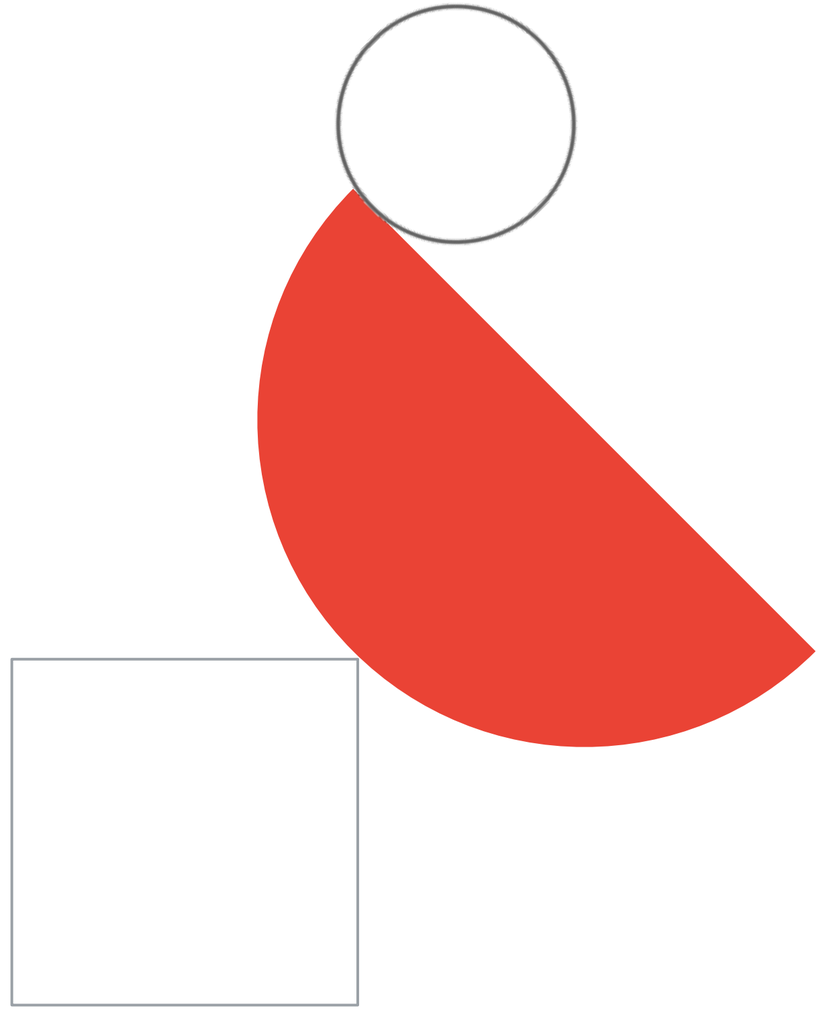
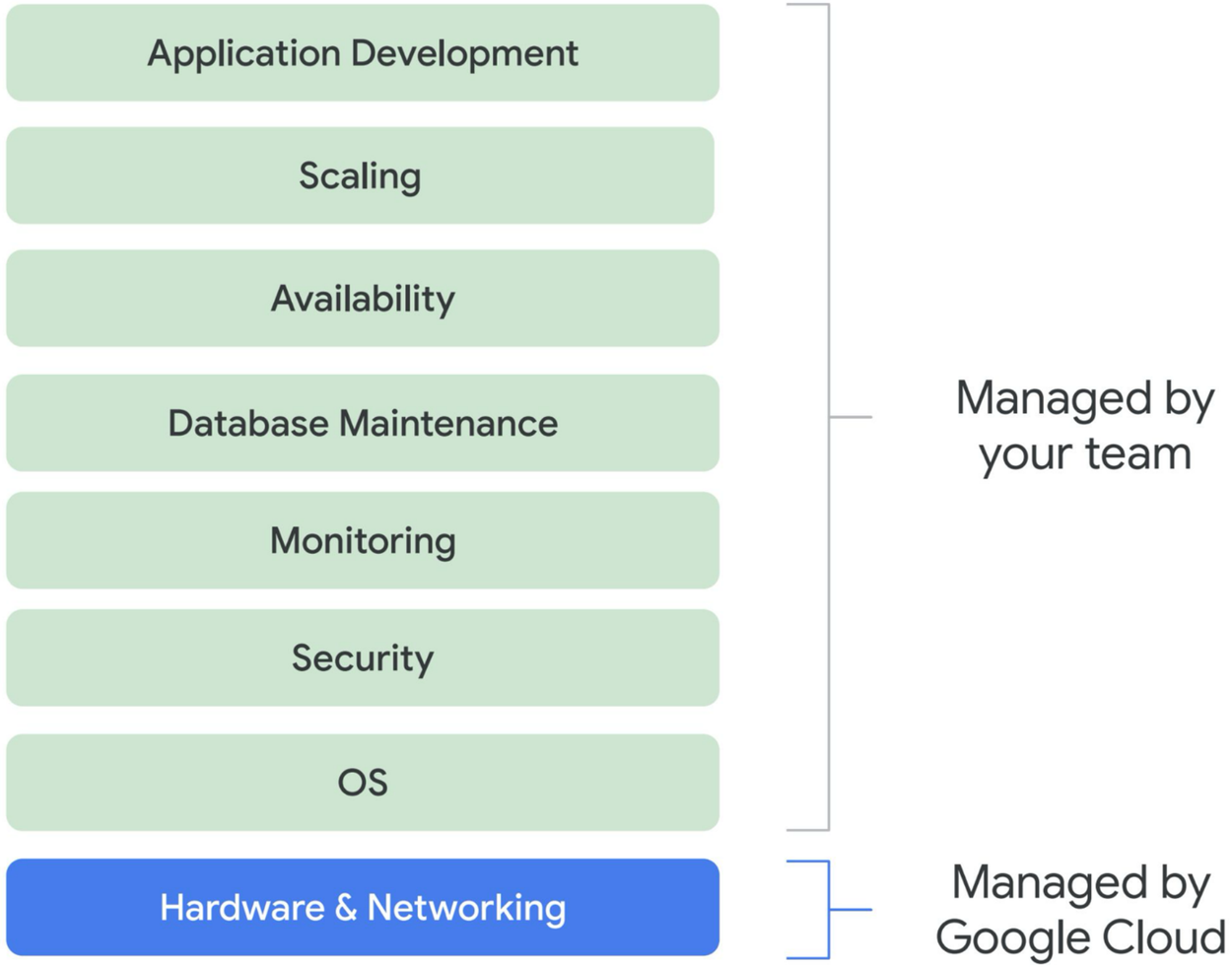
# Cloud SQL



# 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

Database Maintenance

Monitoring

Security

OS

Hardware & Networking

99.999% SLA

Online scaling

Easy global replication

Automatic sharding

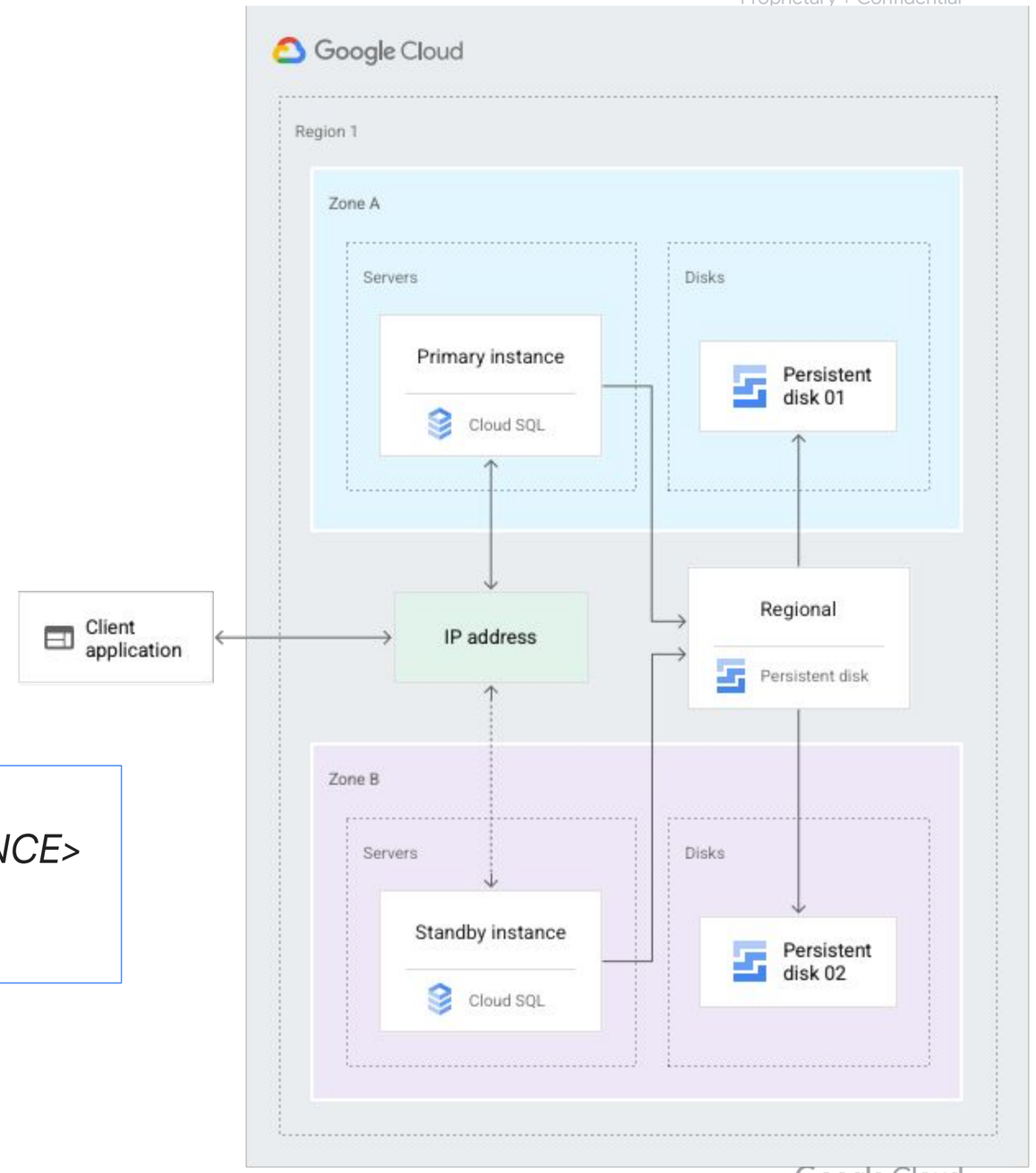
Automatic failure recovery

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

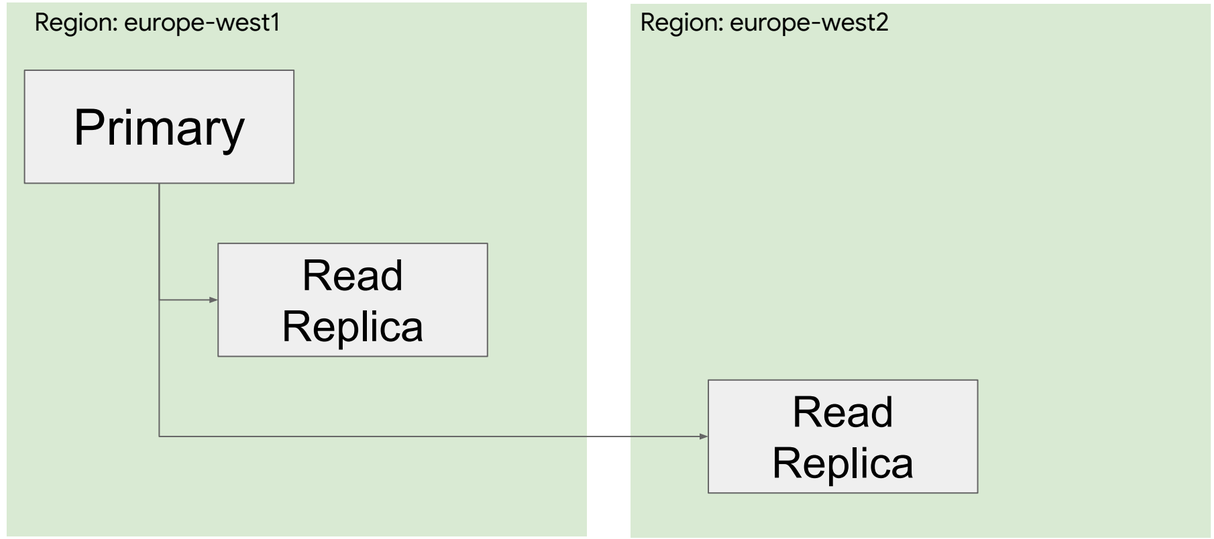
***Exam Tip:*** *Know how to:*
- *Initiate failover: gcloud sql instances failover <PRIM_INSTANCE>*
- *Check if instance is / isn't set for HA: gcloud sql instances describe (availabilityType = REGIONAL / ZONAL)*



# Cloud SQL: Read Replicas

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

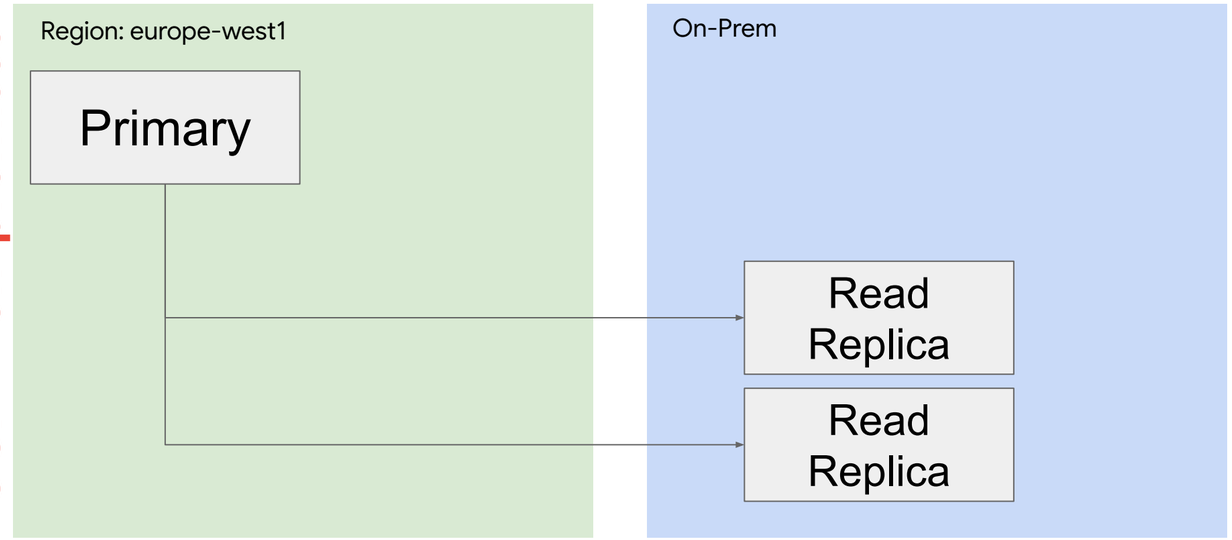
**Read Replica**
**GCP -> GCP**




### 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

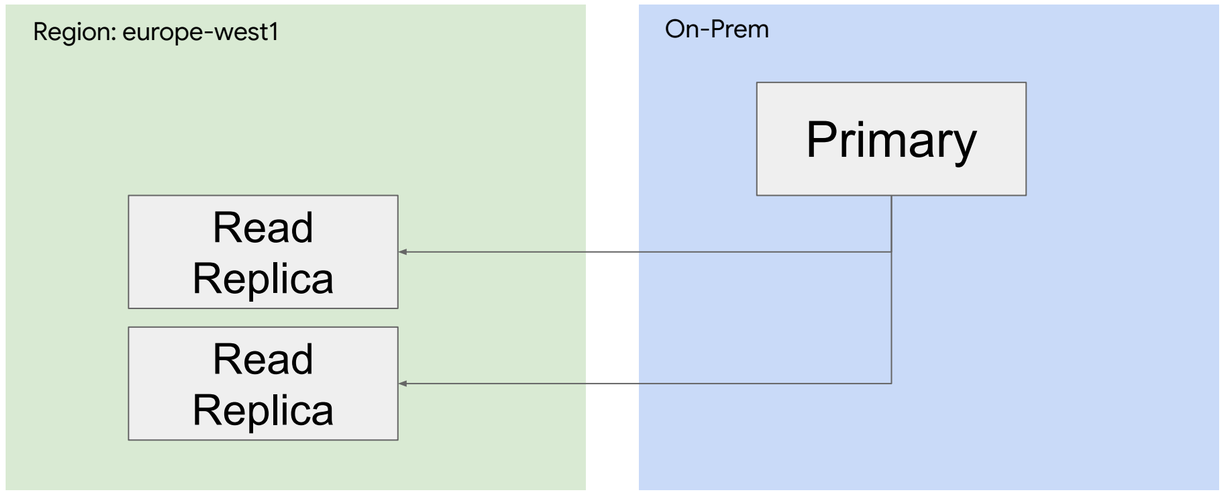
***Exam Tip:*** *Docus on replicating TO external server*

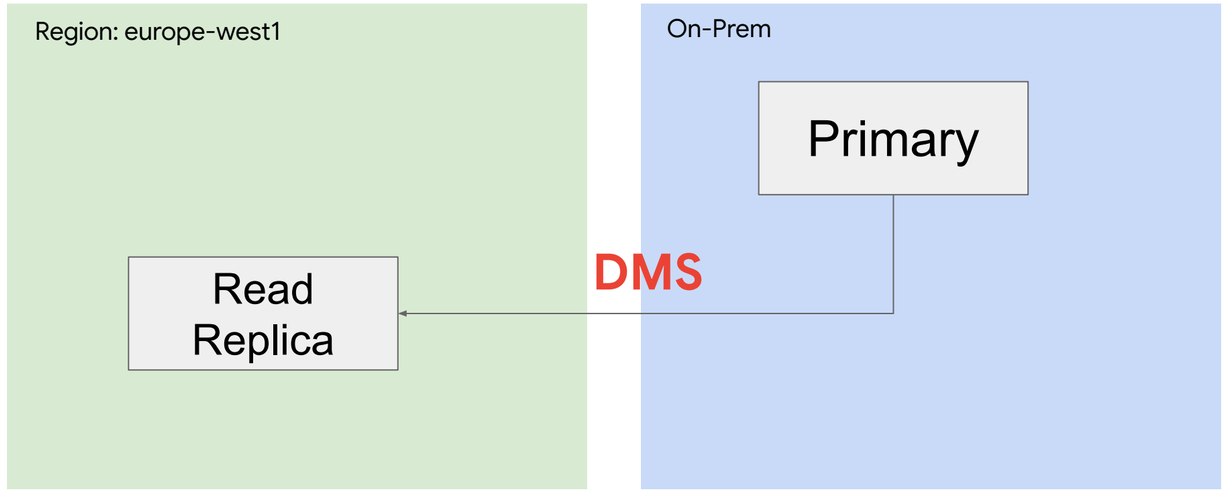
# Cloud SQL: Read Replicas

## 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)

### 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*

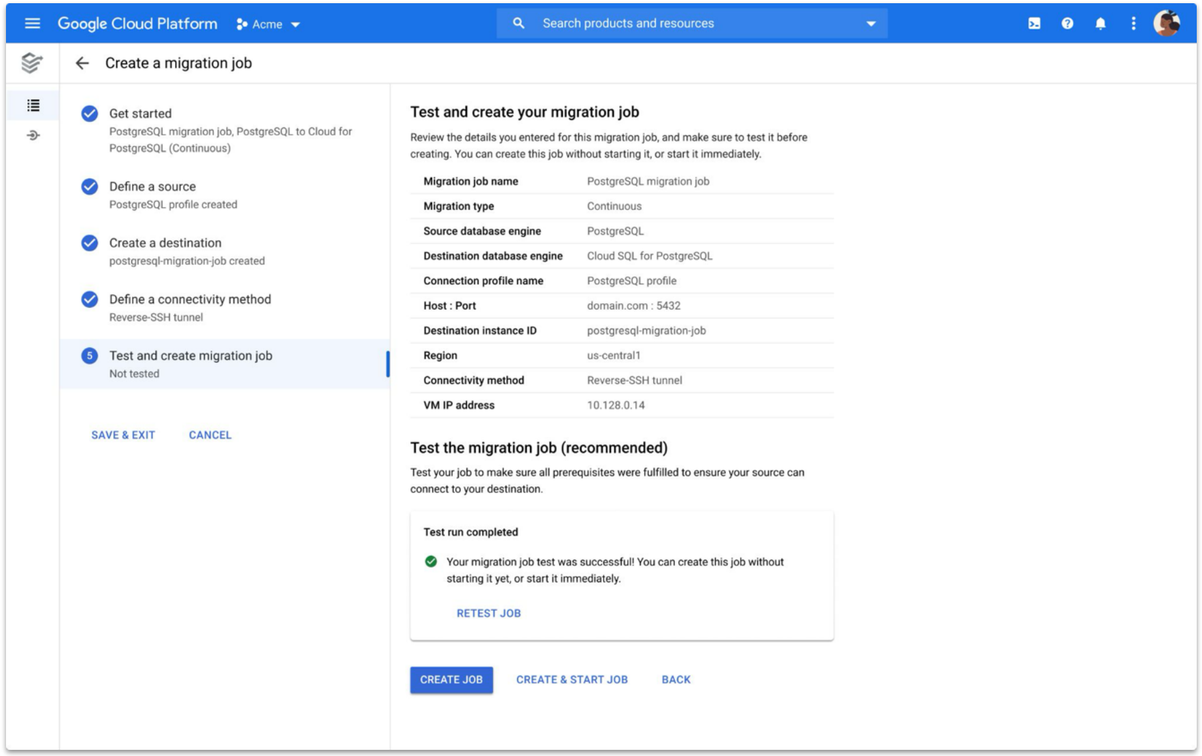
# Simplified migration with Data Migration Service (DMS)

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:***

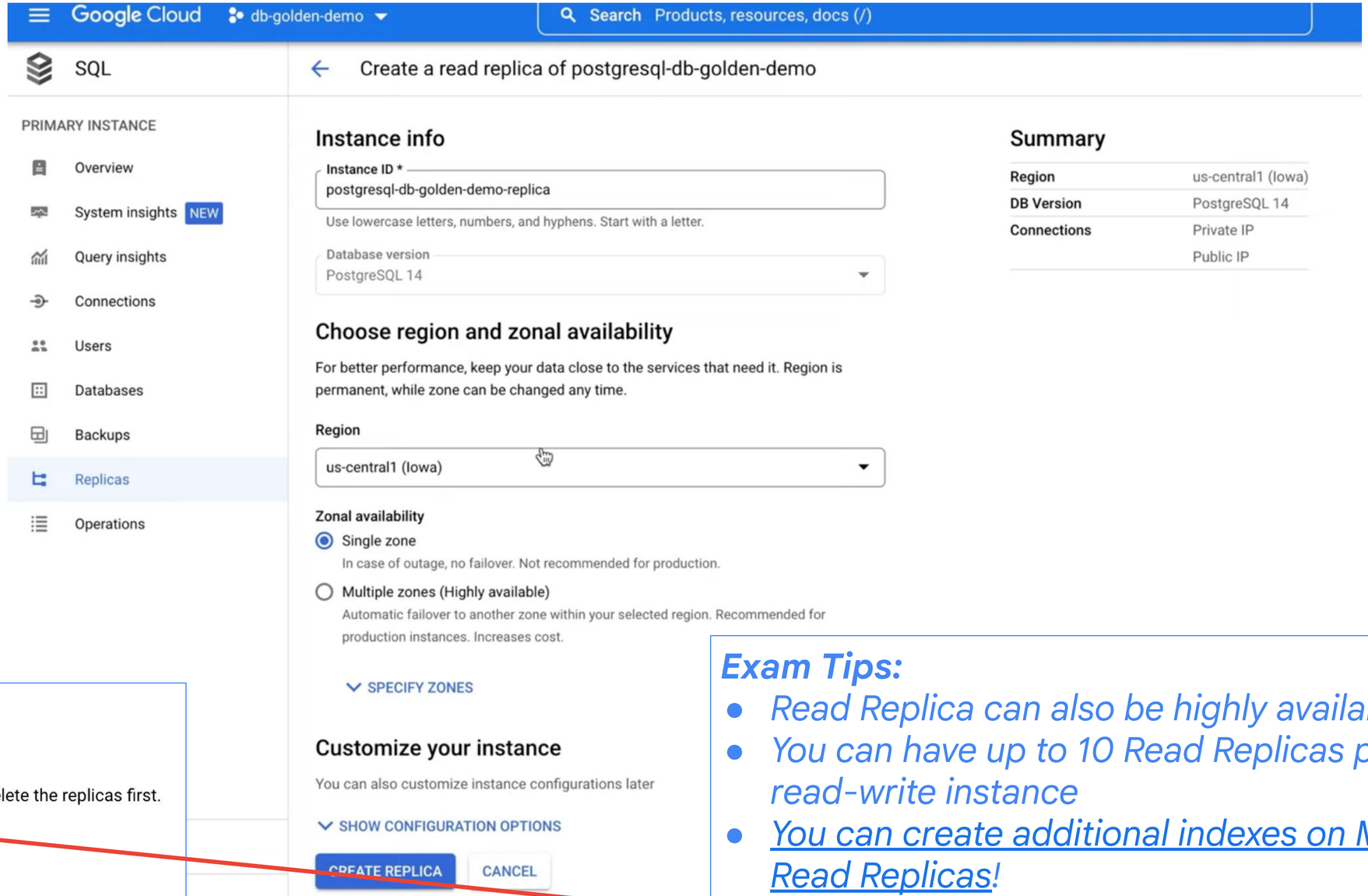
- *Have a look at replication lag topic (MySQL / PostgreSQL / SQL Server)*
- *You can use the **replica_lag** and **network_lag** metrics to monitor replication lag*
- *There are two ways to make a MySQL replica apply changes faster:*
  - *Parallel replication*
  - *High performance flushing*

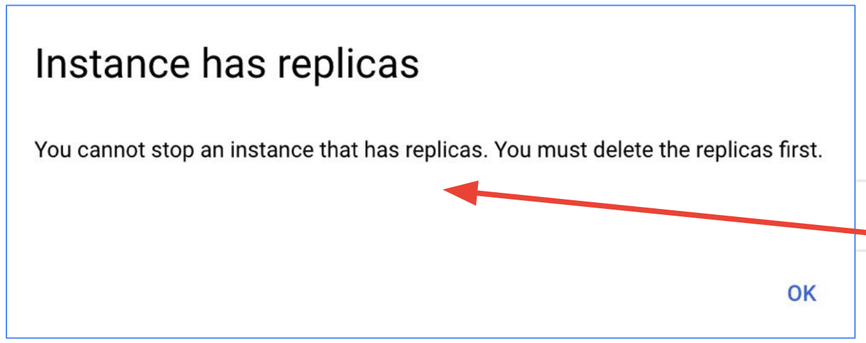
***Exam Tips:***

- *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




***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: edit instance

| | | |
|---|---|---|
| Zone | Y | The possible values depend on the region. |
| Database version | N | Console string / API enum string<br>**PostgreSQL 14** POSTGRES_14<br>**PostgreSQL 13** (default) POSTGRES_13<br>**PostgreSQL 12** POSTGRES_12<br>**PostgreSQL 11** POSTGRES_11<br>**PostgreSQL 10** POSTGRES_10<br>**PostgreSQL 9.6** 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 vCPU (1 - 96)

Memory * 624 GB (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

...

## 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)

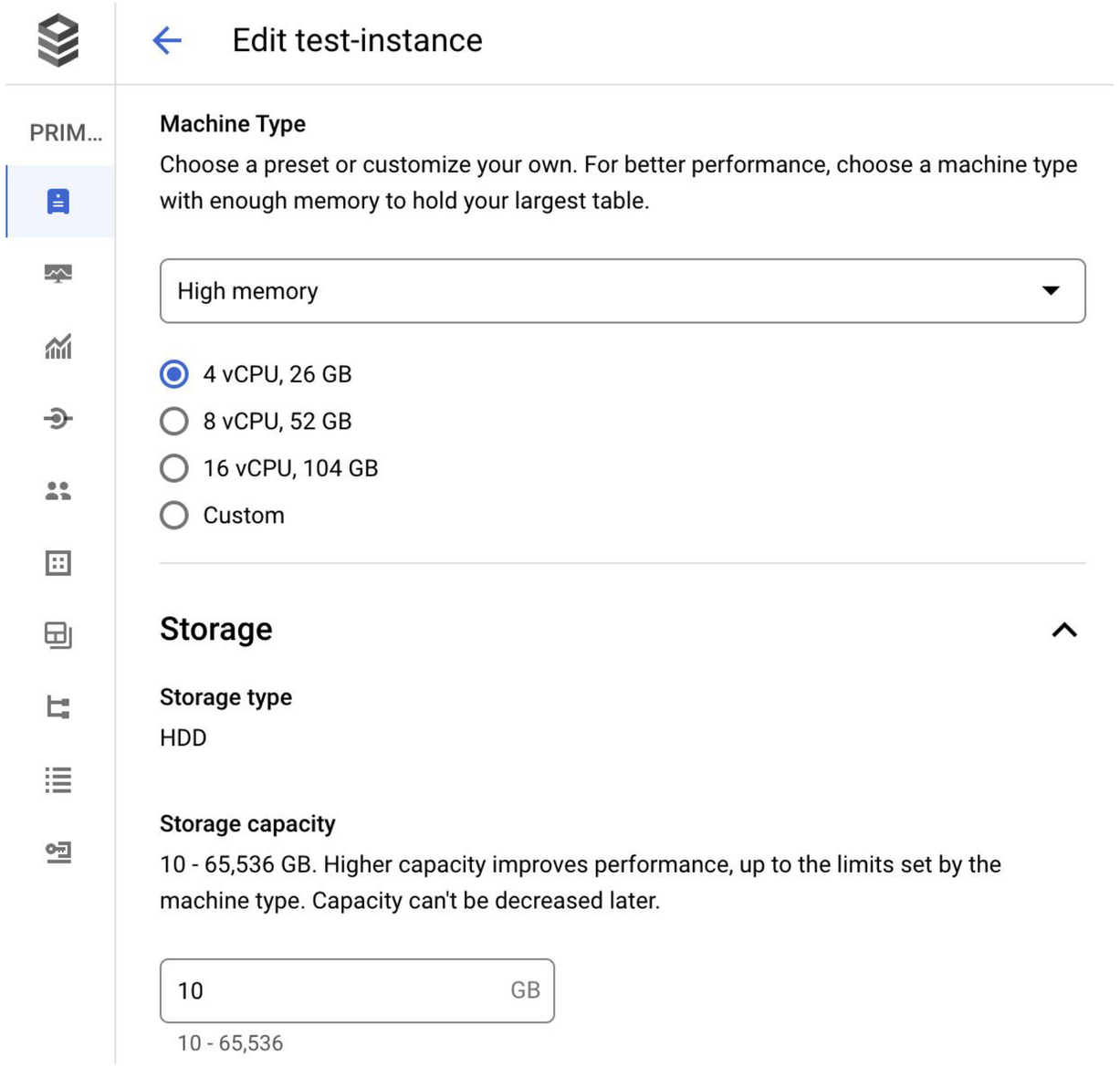
[x] Enable automatic storage increases

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

# 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



# Cloud SQL: GCP-native Backup and Restore

## Types

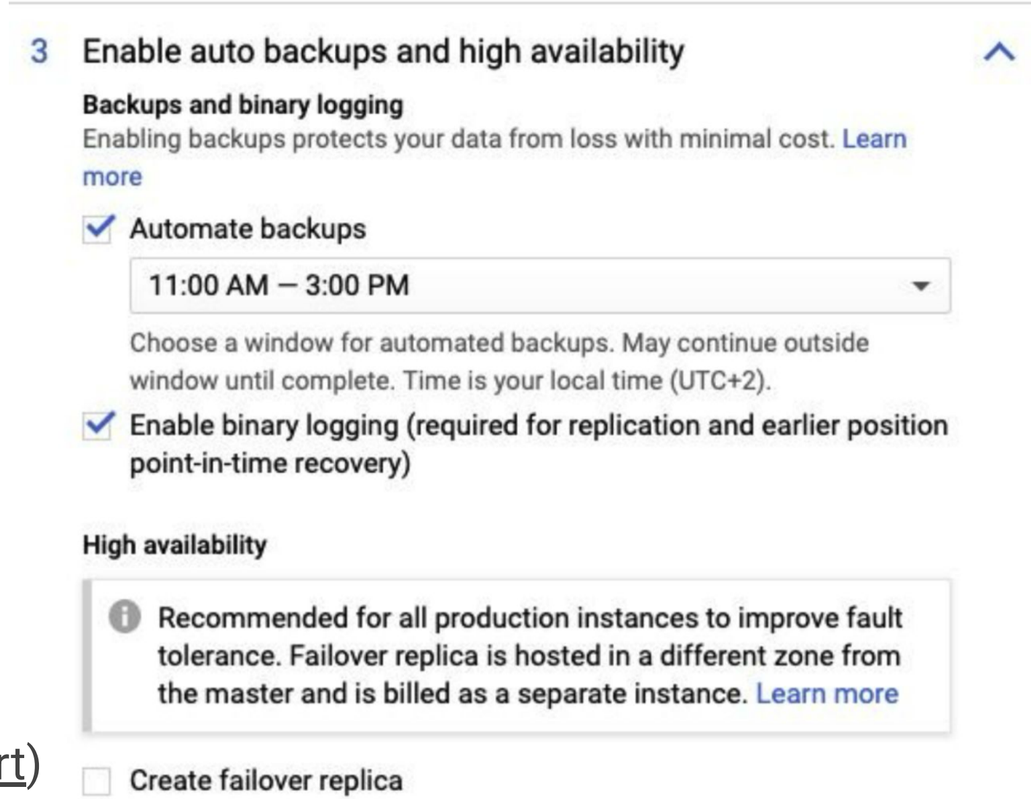
- **On-Demand**
  - Create disk-level snapshot backup at any time
  - Not deleted automatically

- **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

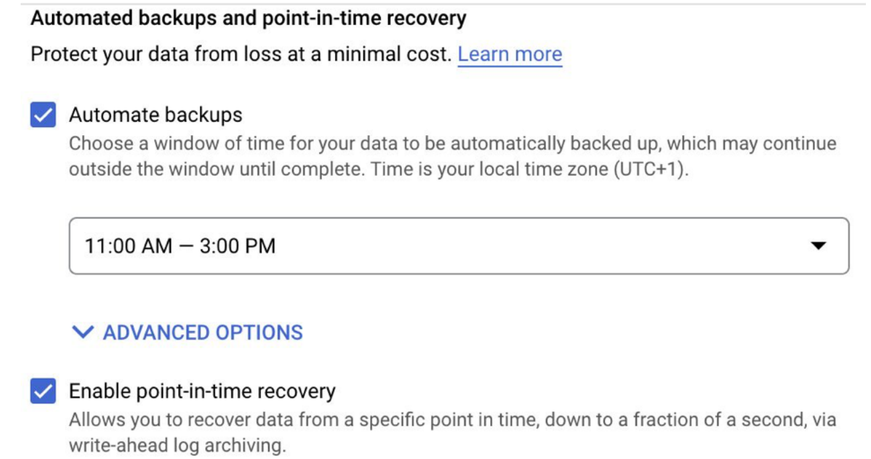
- Up to 365 daily automated backups for each instance. (Only up to 7 days for binlog/WAL files)
- Incremental Backups
- Storage used by backups is charged at a reduced rate. (see pricing)
- Backups can not be exported - only instance data (see doc for export)
- Backups are deleted after instance is deleted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

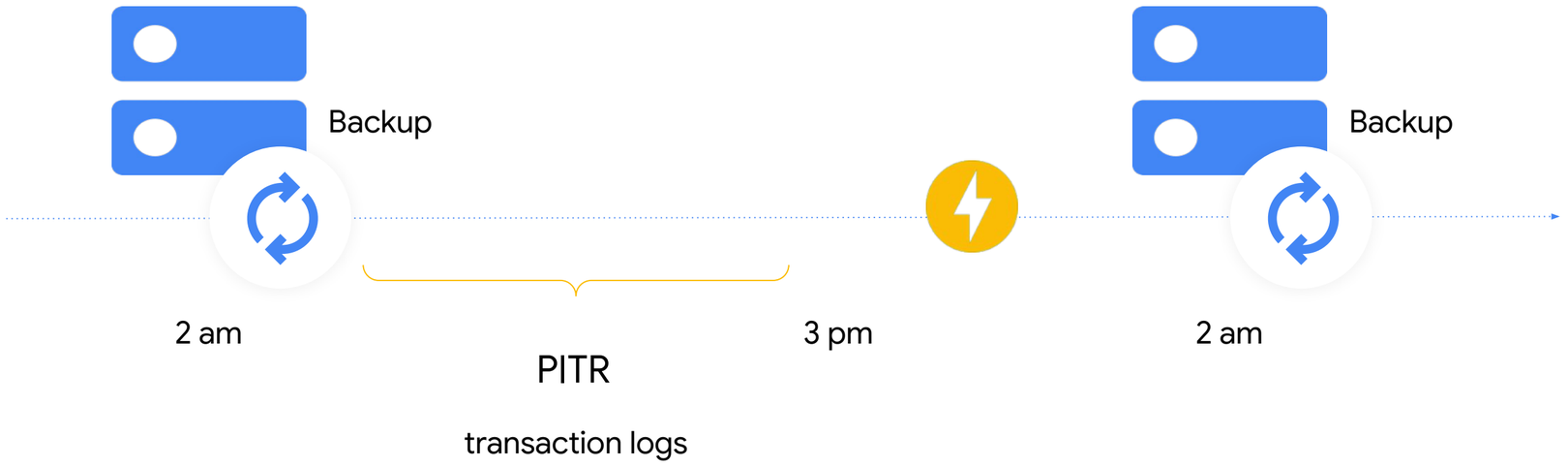
***Exam Tip:*** *Cloud SQL backup window is NOT the same as maintenance window.*



# Cloud SQL: Point-in-time recovery

## recover an instance to a specific point in time



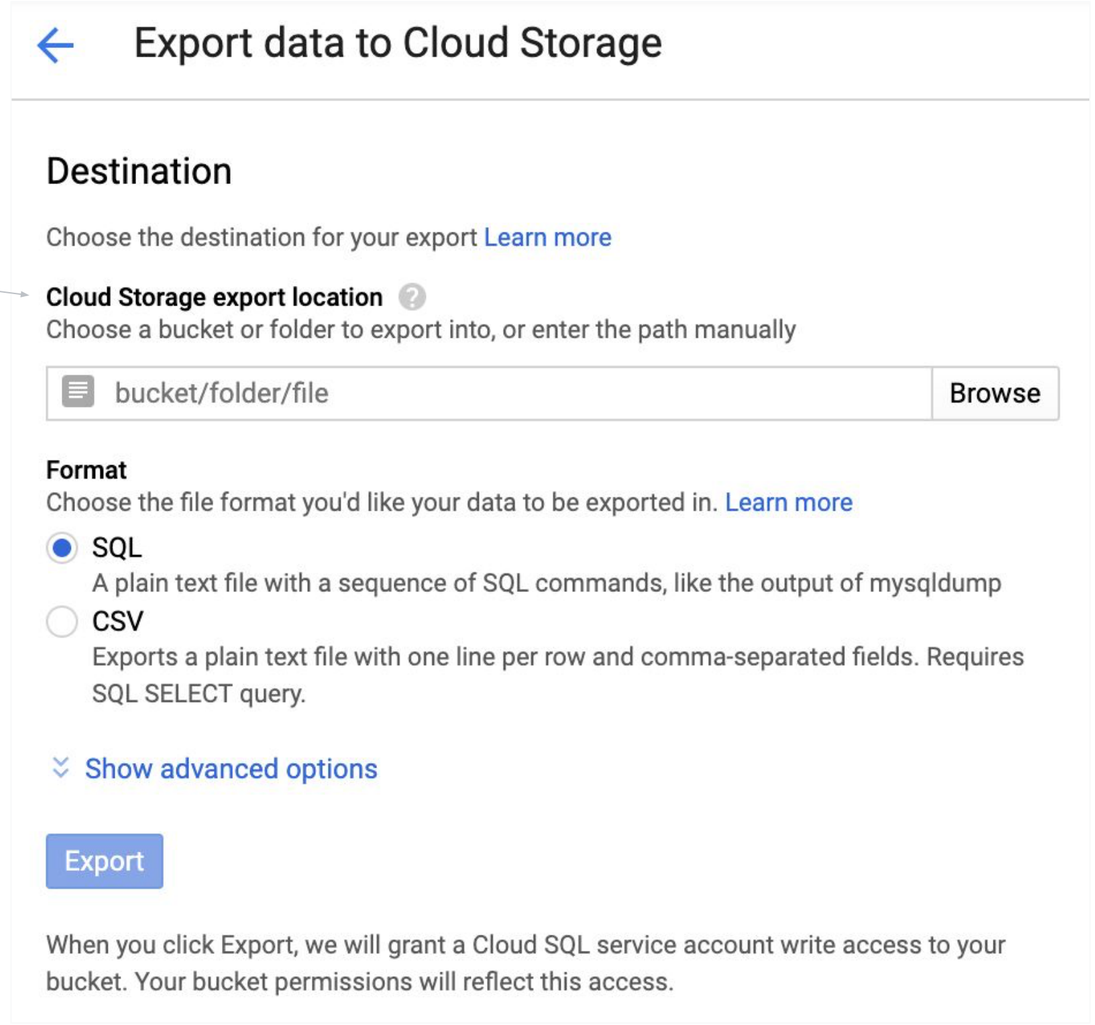



# Cloud SQL: Data Export

**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.*

# Connection Options (external apps)

***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<br>• Configuring access for IP connections<br>• 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<br>• Connecting mysql Client Using the Cloud SQL Proxy<br>• About the Cloud SQL Proxy | |
| **Cloud SQL Proxy Docker image** | Yes | • Connecting mysql Client Using the Cloud SQL Proxy Docker Image<br>• About the Cloud SQL Proxy | |
| **JDBC Socket Library** | Yes | • External connections with Java<br>• JDBC socket factory GitHub page | Java programming language only. |
| **Go Proxy Library** | Yes | • External connections with Go<br>• 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<br>• 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:

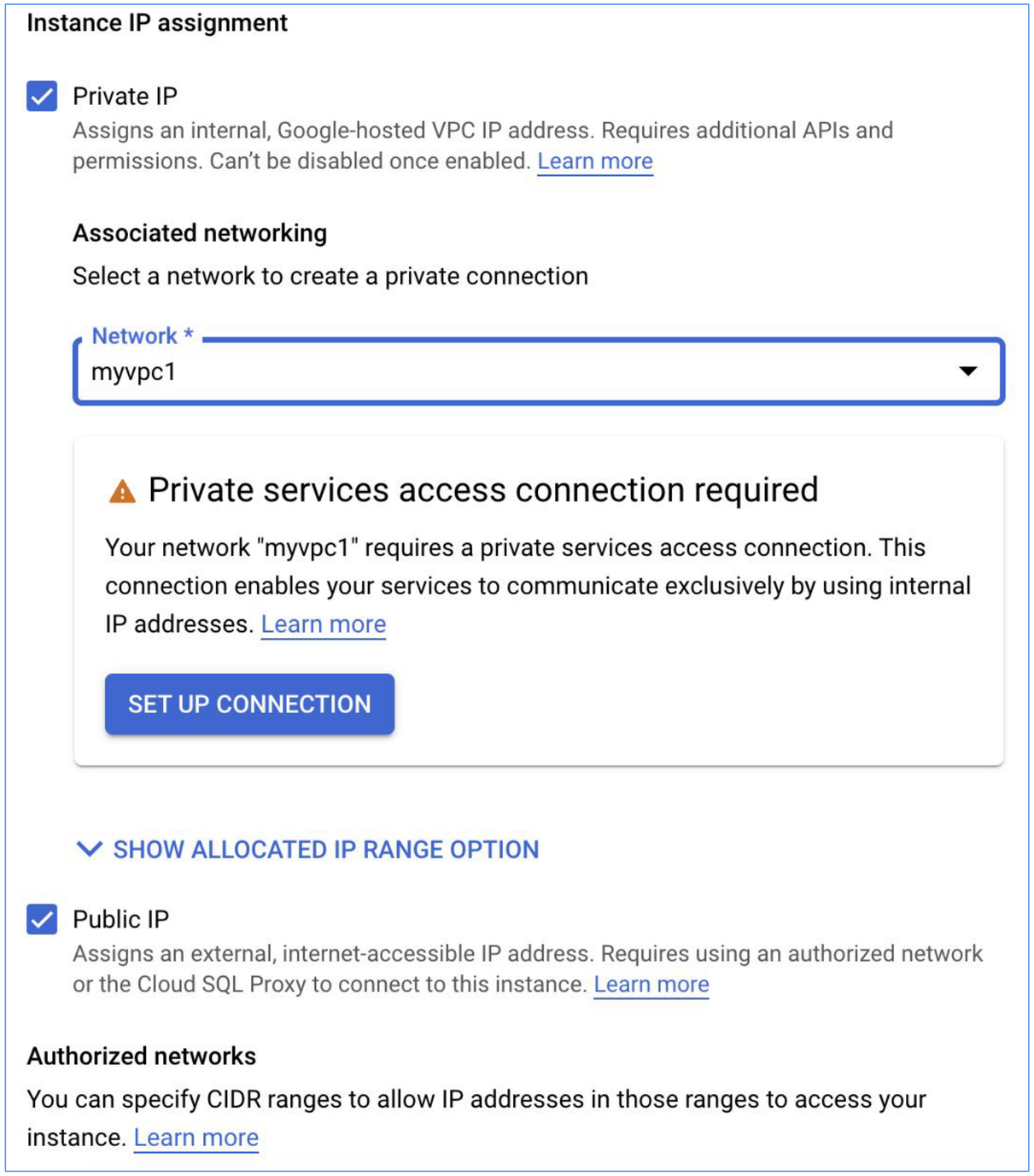
- Preferred when client is coming from resource with internal visibility (not necessarily from the same VPC!
- IPv4 address accessible from VPC
- Connections **may** be configured to use Cloud SQL proxy or self-managed SSL certificates
- Low latency and increased security

### 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*

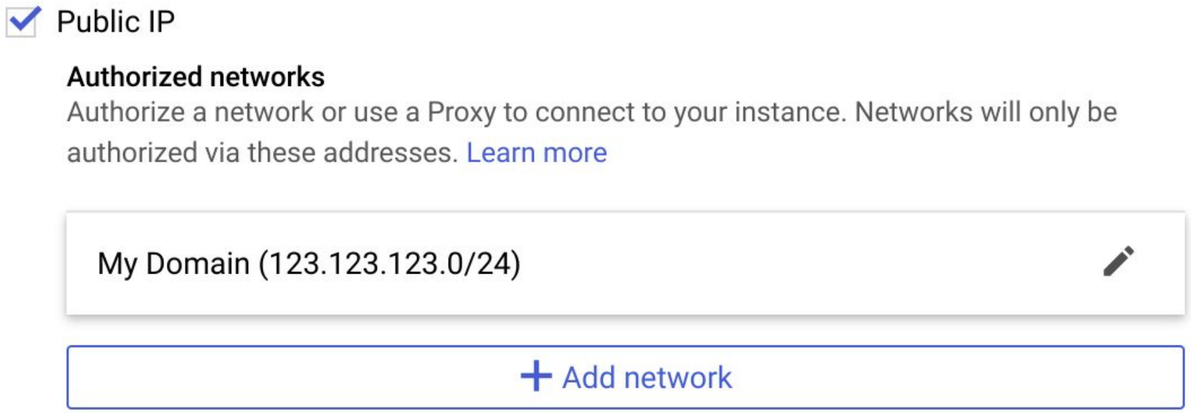


# Cloud SQL: Public IP & risk mitigation

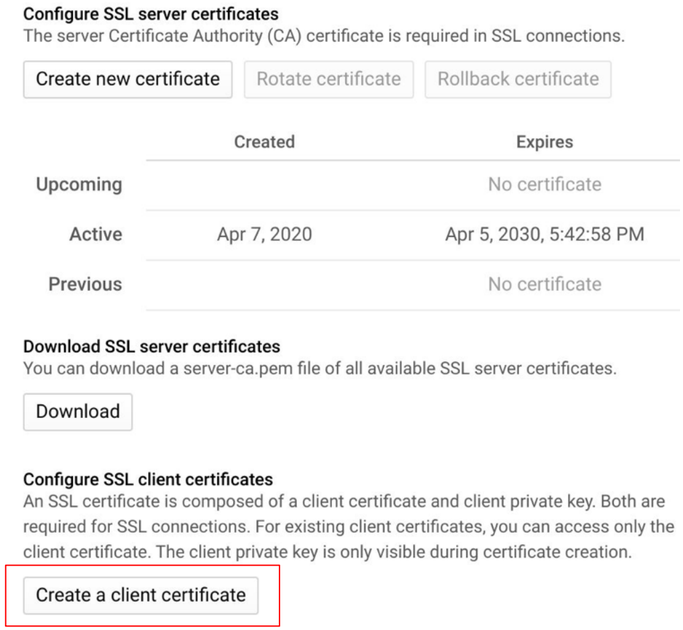

**Access by public IP, without SSL : maximum risk for your data !!**

## 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

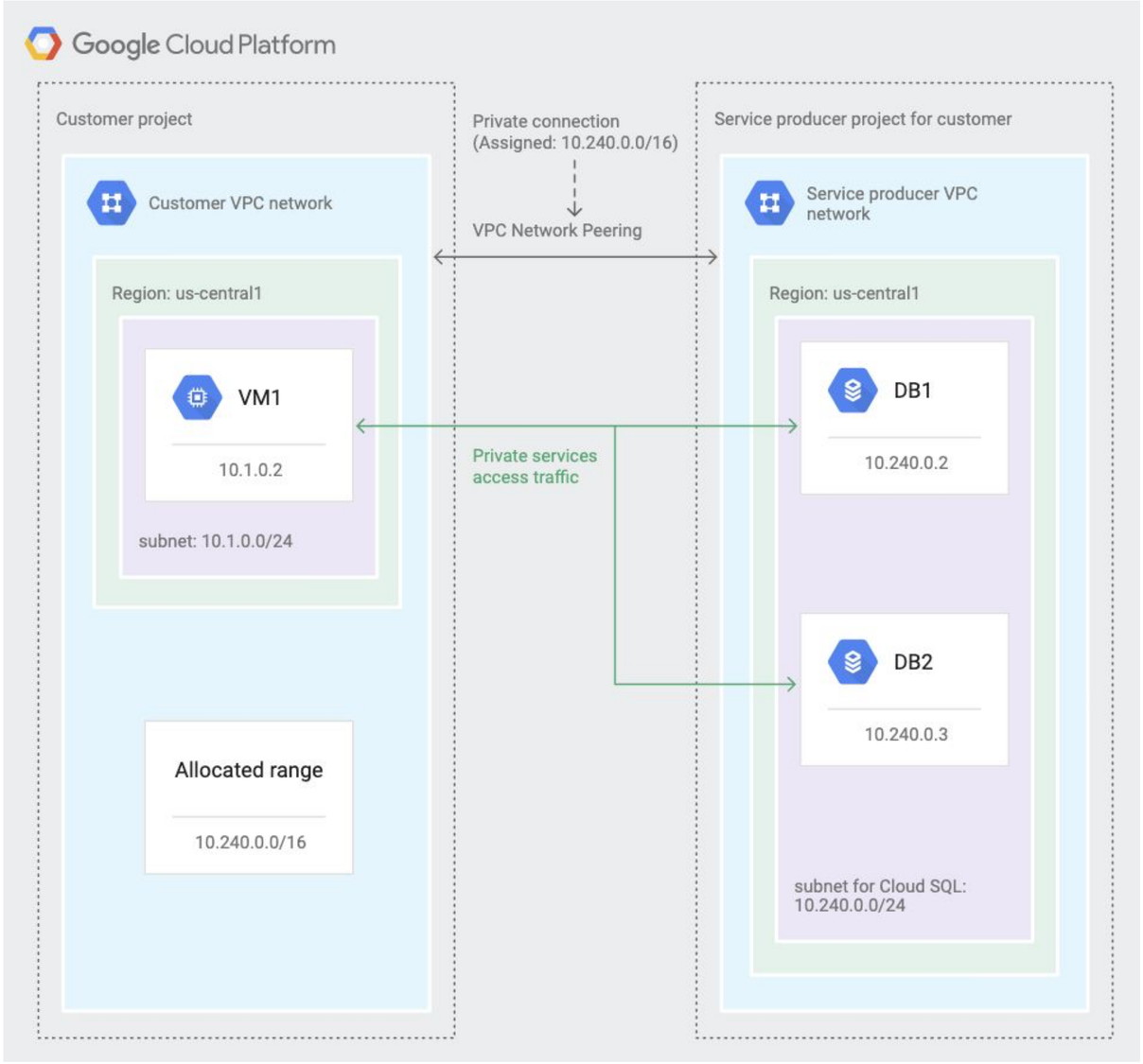
- Allows VM instances in your VPC network to use internal IP addresses to reach the service resources that have internal IP addresses
  → i.e. Connect CloudSQL to GCE or GKE instances
- **GCP uses network peering to create connection**

## 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 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.<br>Not required for accessing an instance using IP addresses. | Apps service<br>(AppEngine, CloudSQL Auth Proxy) |

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

# Cloud SQL

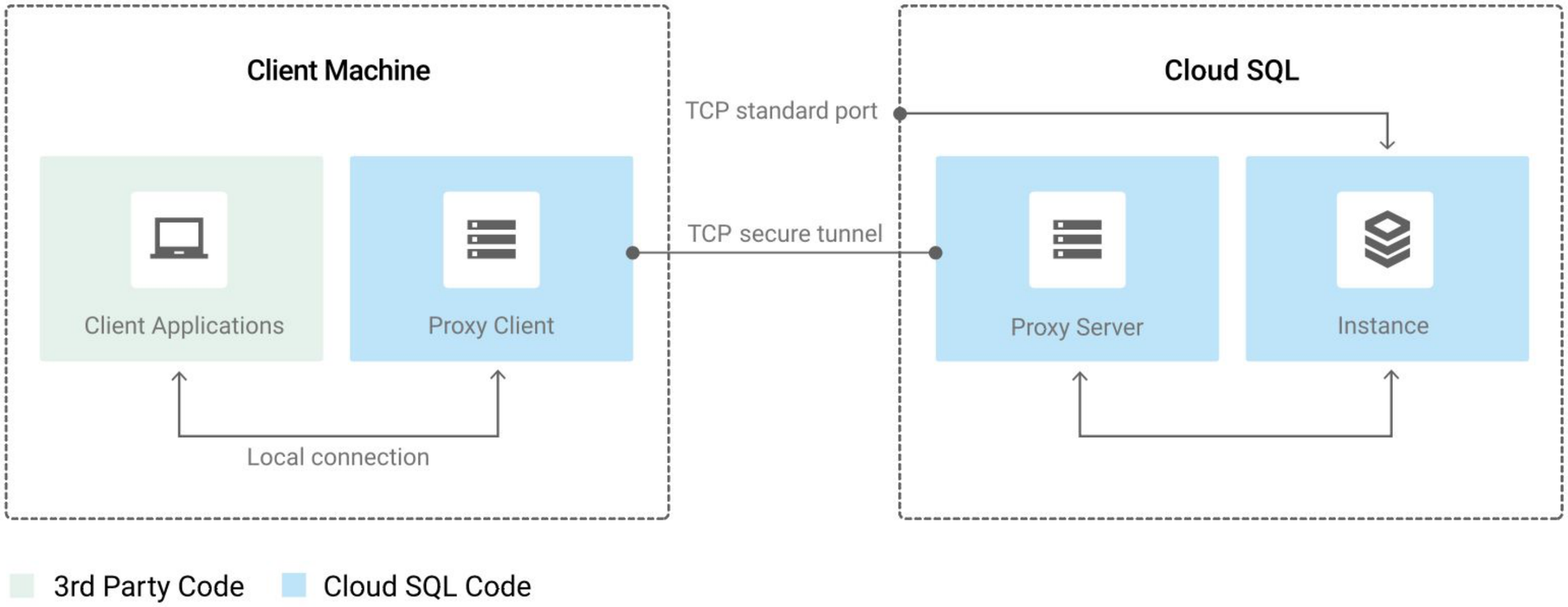
## Access authorization -> Cloud SQL Auth proxy details

### 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

## 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