Cloud Services — GCP (25 Questions)

Q1: GKE workloads in a private cluster can't pull images from Artifact Registry during deployment.

Answer:
Private clusters need Cloud NAT or VPC-SC-compliant egress to reach Artifact Registry. Check if a private Google access or NAT gateway exists. For security, attach a Workload Identity IAM binding so the pod pulls with a service account's Artifact Registry permissions instead of static docker creds.

Sample Points:

- Private Google access/NAT required.
- Use Workload Identity for image pulls.
- Assign minimal `roles/artifactregistry.reader`.

Example Code:

```
gcloud compute routers nats create gke-nat \
  --router=my-router --auto-allocate-nat-external-ips
--nat-all-subnet-ip-ranges
```

Q2: Cloud SQL Postgres reports connection exhaustion during peak CI builds.

Answer:
Introduce Cloud SQL Auth Proxy for connection pooling, or use the built-in IAM DB auth. Tune max_connections and configure CI to batch DB actions. For heavy parallelism, route reporting to a read replica.

Sample Points:

- Auth Proxy to pool connections.
- IAM auth removes static creds.

- Offload reads to replicas.

Example Code:

```
cloud-sql-proxy mydb:region:instance --auto-iam-authn
```

Q3: You need cross-project Pub/Sub messaging with strict publisher identity verification.

Answer:
Grant roles/pubsub.publisher to a service account in the source project, enable topic IAM policy with `--member serviceAccount:...`, and enable `--message-filter` on subscriber side. For security, use VPC-SC if projects are in the same org.

Sample Points:

- Cross-project IAM binding.
- Message filtering to enforce type/tenant.
- VPC-SC for in-org isolation.

Example Code:

```
gcloud pubsub topics add-iam-policy-binding my-topic\
--member=serviceAccount:ci@src.iam.gserviceaccount.com
--role=roles/pubsub.publisher
```

Q4: Cloud Run service must access Firestore in private mode.

Answer:
Use a Serverless VPC Connector to route traffic into the VPC, enable Private Google Access, and attach a service account with roles/datastore.user. Avoid public egress and block unauthorized networks via VPC-SC.

Sample Points:

- VPC Connector bridges to private Firestore.
- Least-privilege SA for access.

- Private Google Access needed.
  Example Code:

```
gcloud run services update my-service \
  --vpc-connector my-connector --no-allow-unauthenticated
```

Q5: GCE VM boot time doubled after enabling OS Login + Shielded VM.

Answer:
OS Login adds IAM-based SSH checks; Shielded VM runs secure boot checks. Optimize by pre-baking images with needed drivers, using OS Config for patch mgmt, and ensuring metadata server IAM policy is lean.
Sample Points:

- OS Login centralizes SSH control.
- Shielded VM adds boot-time integrity checks.
- Bake images to reduce boot overhead.
  Example Code:

```
gcloud compute instances add-metadata myvm --metadata
enable-oslogin=TRUE
```

Q6: A GKE ingress with HTTPS is not issuing certs from managedCertificate.

Answer:
Verify domain DNS A record to LB IP, ensure ManagedCertificate CRD is Active, and that ingress annotations match the correct cert name. DNS must be globally resolvable for Google-managed certs to issue.
Sample Points:

- DNS resolution prerequisite.

- ManagedCertificate must be bound via annotation.
- Check CRD status for Active.

Example Code:

```
kubectl describe managedcertificate my-cert
```

Q7: You must restrict Cloud Storage bucket access to a set of IP ranges.

Answer:
Enable Uniform Bucket-Level Access, then configure an IAM Condition with request.auth.claims if federated, or use Signed URLs for external clients. For IP restrictions, use VPC-SC perimeter ingress rules.

Sample Points:

- Uniform access removes ACL drift.
- VPC-SC for IP/network perimeter.
- Signed URLs for external users.

Example Code:

```
gcloud storage buckets update gs://my-bucket
--uniform-bucket-level-access
```

Q8: Deployment Manager changes are slow to roll out.

Answer:
Break templates into smaller, independent deployments, use --create-policy/--delete-policy flags for parallelism, and migrate high-churn resources to Terraform for better state mgmt.

Sample Points:

- Smaller deployments = faster changes.
- Use parallelism flags.

- Terraform better for iterative changes.
  Example Code:

```
gcloud deployment-manager deployments update my-deploy --async
```

Q9: IAM service account key leaked for a prod app.

Answer:
Immediately revoke the key, rotate application creds to Workload Identity or GCE default SA, audit Cloud Audit Logs for abuse, and set disableServiceAccountKeyCreation org policy.

Sample Points:

- Revoke/rotate quickly.
- Move to keyless auth.
- Lock down SA key creation.
  Example Code:

```
gcloud iam service-accounts keys delete KEY_ID
--iam-account=svc@proj.iam.gserviceaccount.com
```

Q10: Cloud Functions hitting outbound request timeouts to on-prem API.

Answer:
Use a Serverless VPC Connector + VPN/Interconnect to on-prem, raise function timeout up to 9min (2nd gen), and enable retries with exponential backoff.

Sample Points:

- VPC connector + hybrid link.
- Adjust timeout per runtime limits.
- Retries with backoff.
  Example Code:

```
gcloud functions deploy myfn --vpc-connector my-conn --timeout=540
```

Q11: GCE instance template update not reflected in MIG after `rolling-action start-update`.

Answer:
Ensure `instance-template` property actually changed, and that update policy is set to `OPPORTUNISTIC` or `PROACTIVE`. Check for stateful disks/metadata blocking recreation.
Sample Points:

- Template must differ to trigger update.
- Stateful MIG may block replace.
- Choose correct update policy.

Example Code:

```
gcloud compute instance-groups managed rolling-action start-update
mymig \
  --version=template=my-new-template
```

Q12: BigQuery query costs are high due to scanning entire tables.

Answer:
Partition tables by date, cluster by common filter column, and use SELECT only needed fields. Monitor via INFORMATION_SCHEMA.JOBS to find expensive queries.
Sample Points:

- Partition/cluster to limit scanned data.
- Avoid SELECT *.
- Monitor job stats regularly.

Example Code:

```
CREATE TABLE sales PARTITION BY DATE(ts) CLUSTER BY region AS SELECT
...
```

Q13: Cloud Armor policy needs to block `/admin` globally but allow from office IPs.

Answer:
Create a security policy with a rule matching /admin path, deny unless `src_ip` in office CIDR, place before default allow. Attach to backend service.

Sample Points:

- Path match + IP whitelist.
- Rule order matters.
- Attach at backend LB level.

Example Code:

```
gcloud compute security-policies rules create 1000
--security-policy=web \
  --expression="(request.path.startsWith('/admin') &&
!(inIpRange(origin.ip,'1.2.3.0/24')))" \
  --action=deny-403
```

Q14: GKE cluster upgrades are failing due to node pool drain timeouts.

Answer:
Increase maxUnavailable for faster draining, use PodDisruptionBudgets carefully, and check for long-running pods without termination handlers.

Sample Points:

- Tune surge/unavailable for upgrades.
- PDBs can block drains.

- Ensure terminationGracePeriodSeconds set.
  Example Code:

```
gcloud container clusters upgrade mycluster --node-pool np1
--max-unavailable 2
```

Q15: Cloud Storage signed URL should expire in 10 minutes and be GET-only.

Answer:
Generate signed URL with `--http-method GET` and `--expires-in 600`. Ensure bucket uniform access is enabled.
Sample Points:

- Method restriction for security.
- Short TTL minimizes exposure.
- Works with uniform access.
  Example Code:

```
gcloud storage sign-url gs://bucket/file.txt --http-method GET
--expires-in 600
```

Q16: You need to enforce CMEK for all BigQuery datasets.

Answer:
`Setanorg policy constraints/bigquery.requireCmek`, update datasets with `--default-kms-key`. Rotate KMS key per security compliance.
Sample Points:

- Org policy enforces CMEK org-wide.
- Assign default KMS key at dataset level.

- Rotate keys periodically.
  Example Code:

```
gcloud resource-manager org-policies enable-enforce
constraints/bigquery.requireCmek
```

Q17: Cloud Build deploys to GKE but fails with “image pull back-off” for private image.

Answer:
Grant the GKE node service account roles/artifactregistry.reader, ensure imagePullSecrets match the Artifact Registry auth, or use Workload Identity with GKE SA mapped to the builder SA.

Sample Points:

- Node SA must have registry read role.
- Ensure correct pull secret in namespace.
- Prefer Workload Identity for auth.
  Example Code:

```
gcloud projects add-iam-policy-binding $PROJ \
  --member=serviceAccount:node-sa@$PROJ.iam.gserviceaccount.com \
 --role=roles/artifactregistry.reader
```

Q18: Dataflow job stuck in draining state for hours.

Answer:
Jobs with large state or pending bundles drain slowly. Cancel if safe, snapshot state, and restart from snapshot. Avoid long-lived stateful DoFns unless necessary.

Sample Points:

- Large state slows drain.
- Use snapshots for resume.

- Refactor stateful transforms.
  Example Code:

```
gcloud dataflow jobs cancel JOB_ID
```

Q19: VPC Peering connection established but no traffic flows.

Answer:
Ensure both sides added matching routes, there's no overlapping CIDR, and firewall rules allow the traffic. Peering is non-transitive.
Sample Points:

- Peering requires both sides route config.
- No overlapping CIDR allowed.
- Firewall must allow source CIDR.
  Example Code:

```
gcloud compute networks peerings list --network myvpc
```

Q20: You must auto-start and stop dev GCE VMs outside office hours.

Answer:
Use Cloud Scheduler + Pub/Sub + Cloud Functions to call compute.instances.stop/start APIs. Tag instances with `AutoStop=true` and filter in function logic.
Sample Points:

- Scheduler triggers function.
- Tag filter for target instances.
- Least-privilege function SA.
  Example Code:

```
gcloud scheduler jobs create pubsub stop-dev\
--schedule "0 20 * * 1-5" --topic stop-vms
```

Q21: Cloud Logging ingestion cost is high from verbose GKE container logs.

Answer:

Use GKE logging filters to exclude noisy namespaces or drop debug level logs. Route selected logs to BigQuery/SIEM instead of full ingestion.

Sample Points:

- Filter at source for cost savings.
- Route critical logs only.
- Use exclusion filters.

Example Code:

```
gcloud logging sinks update default --exclusion-filter
'resource.labels.namespace_name="dev"'
```

Q22: Cloud Functions cold starts impact latency for a critical API.

Answer:

Switch to 2nd gen functions with min instances set >0, or migrate to Cloud Run with provisioned concurrency.

Sample Points:

- Min instances reduce cold starts.
- Cloud Run offers fine-grained scaling.
- Balance cost vs latency.

Example Code:

```
gcloud functions deploy api-fn --gen2 --min-instances1
```

Q23: Secret Manager secret must only be readable by a specific GKE namespace workload.

Answer:
Use Workload Identity + grant SA `roles/secretmanager.secretAccessor` only for that secret. Map namespace SA to GCP SA.
Sample Points:

- Granular secret IAM.
- Workload Identity mapping.
- Namespace isolation.

Example Code:

```
gcloud secrets add-iam-policy-binding my-secret \
  --member=serviceAccount:gke-sa@$PROJ.iam.gserviceaccount.com \
 --role=roles/secretmanager.secretAccessor
```

Q24: You must enforce org-wide block on external IPs for VMs.

Answer:
Apply org policy `constraints/compute.vmExternalIpAccess=DENY_ALL`. Allow exceptions only via folder/project policy override for bastions.
Sample Points:

- Org policy to block external IPs.
- Exception scoping by folder/project.
- Bastion pattern for external access.

Example Code:

```
gcloud resource-manager org-policies set-policy deny-extip.yaml
```

Q25: You want an automated daily export of billing data to BigQuery.

Answer:
Enable billing export to BigQuery in Cloud Console. Create dataset with CMEK if required. Partition table by usage_start_time for query efficiency.

Sample Points:

- Billing export native integration.
- Partition for cost queries.
- CMEK for compliance.

Example Code:

```
gcloud beta billing accounts links create --billing-account=XXXX\
--project=myproj --dataset=billing
```