Summary

## <https://www.startcloudnow.com/google%20cloud.html>

<https://www.linkedin.com/pulse/my-review-professional-cloud-security-engineer-beta-exam-tzavelas/?trackingId=wfzSPQTlEQXGgzkRE6XWXA%3D%3D>

<https://github.com/sathishvj/awesome-gcp-certifications/blob/master/professional-cloud-security-engineer.md>

## VPC

Shared network. Service Control

Changes without blocking access to resource?

# Organization policies

Control creation of serviceaccount

# IAM

How to review accesses? Use role recommender.

**when to use service account**

Use service accounts for unattended scenarios.

Use service accounts to perform a transition between principals.

Don't use service accounts to access user data without the user's consent.

Don't use service accounts during development.

**Protect Service account**

[Best practices for securing service accounts  |  Cloud IAM Documentation  |  Google Cloud](https://cloud.google.com/iam/docs/best-practices-for-securing-service-accounts)

Don’t let user create service account key using org policy iam.disableServiceAccountKeyCreation and iam.disableServiceAccountKeyUpload

Don't use automatic role grants for default service accounts

Don't rely on access scopes when attaching a service account to a VM instance (because it is coarse-grained, not fine grained)

Avoid using groups for granting service accounts access to resources

Avoid using domain-wide delegation

Use Credential Access Boundaries to downscope access tokens (only for cloud storage)

Use role recommendations to identify unused permissions

Use lateral movement insights to limit lateral movement

## Protecting against privilege-escalation threats

Avoid letting users impersonate service accounts that are more privileged than the users themselves.

Avoid letting users change the IAM policies of service accounts that are more privileged than the users themselves.

Don't let users create or upload service account keys.

Don't grant access to service accounts at the Cloud project or folder level.

Don't run code from less protected sources on compute resources that have a privileged service account attached.

Limit shell access to VMs that have a privileged service account attached.

Limit metadata server access to selected users and processes.

## Protecting against spoofing threats

Don't allow attribute mappings to be modified.

Don't rely on attributes that aren't stable or authoritative.

## Protecting against information disclosure threats

Avoid disclosing confidential information in service account email addresses

## Protecting against non-repudiation threats

Enable data access logs for IAM APIs.

Ensure that CI/CD history can be correlated with Cloud Audit Logs.

**Choosing suitable IAM roles**

<https://cloud.google.com/iam/docs/job-functions/billing>

<https://cloud.google.com/iam/docs/job-functions/networking>

<https://cloud.google.com/iam/docs/job-functions/auditing>

**create short live service account credential**

grant the role to the account you will be creating the short live token.

So if SA1 create SA2 short live token, in SA2 iam policy need roles/iam.serviceAccountTokenCreator with member SA1.

**IAP**

TCP forwarding is use to allow user to access ssh rdp.

# DLP

Encryption to redact? Mask?

Table

Description automatically generated

Use rowsLimit and bytesLimitPerFile to sample data and use CloudStorageRegexFileSet limit scans

# Cloud Armor

The load balancer must be an external HTTP(S) load balancer.

The backend service's load balancing scheme must be EXTERNAL.

The backend service's protocol must be one of HTTP, HTTPS, or HTTP/2.

Have preview mode.

# VPC

Deploy private and subnet, in between virtual appliance route to monitor?

(use 1 vm with multiple NIC to different subnets.)

How to check rules that are conflict?

Firewall insights?

# Text Description automatically generated

Restricted.googleapis.com – ONLY SUPPORT services that supports VPC service controls

# kms

Cloud Build cannot use KMS. It encrypt the build-time persistent disk (PD) with an ephemeral key that is generated for each build. No configuration is required.

Generate DEK locally, generate new KEK in KMS to encrypt DEK, store both encrypted data and encrypted DEK

# Bigtable

Bigtable automatically replicate data over at least 2 geographic places

ISO 27017

# LB

A picture containing graphical user interface

Description automatically generated

Which one to use to remember client IP? Use TCP/UDP network load balancer and internal TCP/UDP load balancers.

Proxy-only subnets are only required for regional external HTTP(S) load balancers.

Firewall need ingress rule 130.211.0.0/22 35.191.0.0/16 for health check.

When delivering both secure and non-secure content over the same hostname, the client is directed to an edge server that can negotiate either HTTP or HTTPS. To make this work with Cloud CDN, you can reserve an IP address and bind the reserved IP address to both the HTTP and HTTPS frontend configuration in the external HTTP(S) load balancer.

**External HTTP Lb usecases:**

3 tier web service, multi region lb, Workloads with jurisdictional compliance, traffic management, lb for GKE (external), lb with request routing, lb for serverless services, lb with hybrid connectivity private service connect

**Internal HTTP LB usecases:**

3 tier web service, path-based routing, modernizing legacy services, private service connect

**External TCP/UDP usecases:**

Balance non-tcp traffic or balance other TCP port, ok to have SSL traffic decrypted by backends, acceptable for self managed cert, need **PRESERVE CLIENT IP**, need pass through lb instead of proxy.

SSL Proxy Load Balancing is intended for non-HTTP(S) traffic

# Logs

How to validate connection is working? (firewall logs? Flow logs?)

The Logs Viewer role doesn't let you read the Data Access audit logs that are in the \_Default bucket. To read these Data Access audit logs, you need the Private Logs Viewer role (roles/logging.privateLogViewer) for the appropriate log view.

The Logs Viewer role doesn't let you read logs that are stored in user-defined buckets; to read logs in user-defined buckets, you need the Logs View Accessor role (roles/logging.viewAccessor) for the appropriate log view.

# Compliance

Doc to see PCI?

# Private access

Have services except app engine, memcache, filestore and memorystore link

# Google Cloud Directory Sync (GCDS)

SSL

sync-cmd command

define google domain connection in Google Domain Configuration page

LDAP configuration page to define ldap server

General Settings to define type of object to sync

Org Units page to specify LDAP OU correspond to OU in google domain

# Cloud monitoring API

Use combiner field for combine conditions

Alerting policy can contain up to 6 conditions

Duration window refers to the length of time a condition must evaluate as true before triggering

Graphical user interface, text, application, email

Description automatically generated