Google Cloud

Professional Cloud Security Engineer

Certification exam guide

A Cloud Security Engineer allows organizations to design and implement secure workloads and infrastructure on Google Cloud. Through an understanding of security best practices and industry requirements, this individual designs, develops, and manages a secure solution by using Google security technologies. A Cloud Security Engineer is proficient in Identity and Access Management, defining the resource hierarchy and policies, using Google Cloud technologies to provide data protection, configuring network security defenses, monitoring environments for threats, configuring security automation, securing AI workloads, securing the software supply chain, and enforcing regulatory controls.

Section 1: Configuring access (~25% of the exam)

1.1 Managing Cloud Identity. Considerations include:

- Configuring Google Cloud Directory Sync and implement single sign-on (SSO) with a third-party identity provider.
- Managing a super administrator account.
- Automating the user lifecycle management process.
- Administering user accounts and groups programmatically.
- Configuring Workforce Identity Federation

1.2 Managing service accounts. Considerations include:

- Securing and protecting service accounts (including default service accounts).
- Identifying scenarios requiring service accounts.
- Creating, disabling, and authorizing service accounts.
- Securing, auditing, and mitigating the usage of service account keys.
- Managing and creating short-lived credentials.
- Configuring Workload Identity Federation.
- Managing service account impersonation.

1.3 Managing authentication. Considerations include:

- Creating a password and session management policy for user accounts.
- Setting up Security Assertion Markup Language (SAML) and OAuth.
- Configuring and enforcing 2-step verification.

1.4 Managing and implementing authorization controls. Considerations include:

- Managing privileged roles and separation of duties with Identity and Access Management (IAM) roles and permissions.
- Managing IAM and access control list (ACL) permissions.
- Granting permissions to different types of identities using IAM conditions and IAM deny policies.
- Defining access control at the organization, folder, project, and resource level using the principle of least privilege.
- Configuring Access Context Manager.
- Applying Policy Intelligence.
- Managing permissions through groups.
- Identifying use cases and configuring Privileged Access Manager.

1.5 Defining the resource hierarchy. Considerations include:

- Managing folders and projects at scale.
- Managing pre-built or custom organization policies for the organization, folders, and projects.
- Using the resource hierarchy for access control and permissions inheritance.

Section 2: Securing communications and establishing boundary protection (~22% of the exam)

2.1 Designing and configuring perimeter security. Considerations include:

- Configuring network perimeter controls (e.g., Cloud Next Generation Firewall [Cloud NGFW] rules and policies, Identity-Aware Proxy [IAP], load balancers, and Certificate Authority Service).
- Setting up application layer inspection on Cloud NGFW (e.g., layer 7).
- Differentiating between private and public IP addressing.
- Configuring web application firewalls (e.g., Google Cloud Armor).
- Deploying Secure Web Proxy.
- Configuring Cloud DNS security settings.
- Continually monitoring and restricting configured APIs.

2.2 Configuring boundary segmentation. Considerations include:

- Configuring security properties of a VPC network, VPC peering, Shared VPC, and firewall rules.
- Configuring network isolation and data encapsulation for N-tier applications.
- Identifying use cases and configuring VPC Service Controls.

2.3 Establishing private connectivity. Considerations include:

- Designing and configuring private connectivity between VPC networks and Google Cloud projects (Shared VPC, VPC peering, and Private Google Access for on-premises hosts).
- Designing and configuring private connectivity and encryption between data centers and VPC network (e.g., HA VPN, Cloud Interconnect).
- Establishing private connectivity between VPC and Google APIs (Private Google Access, Private Google Access for on-premises hosts, restricted Google access, Private Service Connect).
- Using Cloud NAT to enable outbound traffic.

Section 3: Ensuring data protection (~23% of the exam)

3.1 Protecting sensitive data and preventing data loss. Considerations include:

- Configuring Sensitive Data Protection (SDP) (e.g., discovering and redacting personally identifiable information (PII), configuring pseudonymization and format preserving encryption).
- Restricting access to Google Cloud data services (e.g., BigQuery, Cloud Storage, and Cloud SQL datastores).
- Securing secrets with Secret Manager.
- Protecting and managing compute instance metadata.

3.2 Managing encryption at rest, in transit, and in use. Considerations include:

- Identifying use cases for Google default encryption, customer-managed encryption keys (CMEK), and Cloud External Key Manager (EKM).
- Determining when to use software and hardware keys
- Creating and managing encryption keys for CMEK and EKM (e.g., key rotation and revocation, key import).
- Applying encryption methods to various use cases.
- Configuring object lifecycle policies for Cloud Storage.
- Enabling Confidential Computing.

3.3 Securing AI workloads. Considerations include:

- Implementing security and privacy controls for AI/ML systems to protect against unintentional exploitation of data or models.
- Determining security requirements for IaaS-hosted and PaaS-hosted training models.
- Implementing security controls for Gemini Enterprise Agent Platform.

Section 4: Managing operations (~19% of the exam)

4.1 Automating infrastructure and application security. Considerations include:

- Automating security scanning for Common Vulnerabilities and Exposures (CVEs) through a continuous integration and delivery (CI/CD) pipeline.
- Configuring Binary Authorization to secure GKE clusters or Cloud Run.
- Automating virtual machine and container image creation (e.g., hardening, maintenance, VM patch management).
- Managing policy and drift detection at scale (e.g., cloud security posture management, custom organization policies and custom modules for Security Health Analytics).

4.2 Configuring logging, monitoring, and detection. Considerations include:

- Configuring and analyzing network logs (Cloud Next Generation Firewall [Cloud NGFW], VPC flow logs, Packet Mirroring, Cloud Intrusion Detection System [Cloud IDS], Log Analytics).
- Designing an effective logging strategy.
- Logging, monitoring, responding to, and remediating security incidents.
- Designing secure access to logs.
- Exporting logs to external security systems.
- Configuring and analyzing Google Cloud Audit Logs and data access logs.
- Configuring log exports (log sinks and aggregated sinks).
- Configuring and monitoring Security Command Center.

Section 5: Supporting compliance requirements (~11% of the exam)

5.1 Adhering to regulatory and industry standards requirements for the cloud. Considerations include:

- Determining technical needs relative to compute, data, network, and storage.
- Evaluating the shared responsibility model.
- Configuring security controls within cloud environments to support compliance requirements (e.g., Assured Workloads, organizational policies, Access Transparency, Access Approval, regionalization of data and services).
- Determining the Google Cloud environment in scope for regulatory compliance.
- Mapping compliance requirements to Google Cloud services and security controls (e.g., network and access segmentation, audit log coverage).