Google Cloud

Preparing for Your Professional Cloud Security Engineer Journey

Module 3: Ensuring Data Protection

Welcome to Module 3: Ensuring Data Protection.
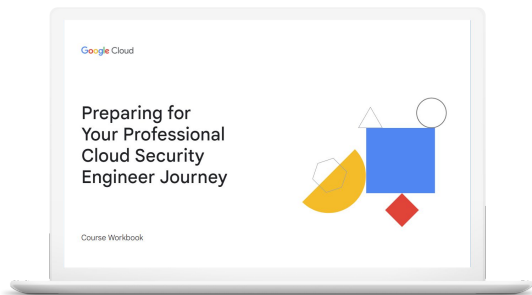
Review and study planning

Now let's review how to use these diagnostic questions to help you identify what to include in your study plan.

Your study plan:

Ensuring data protection

Google Cloud		
Preparing for Your Professional Cloud Security Engineer Journey		**3.1** Protecting sensitive data and preventing data loss
Course Workbook		**3.2** Managing encryption at rest, in transit, and in use

Google Cloud

We'll approach this review by looking at the key areas of this exam section and the questions you just answered about each one. We'll talk about where you can find out more about each area in the learning path for this certification and/or where to find the information in Google Cloud documentation. As we go through each one, take notes on the specific courses (and modules!), quests, and documentation pages you'll want to emphasize in your study plan.

3.1 | Protecting sensitive data and preventing data loss

Considerations include:

- Inspecting and redacting personally identifiable information (PII)
- Configuring pseudonymization
- Configuring format-preserving substitution
- Restricting access to BigQuery, Cloud Storage, and Cloud SQL datastores
- Securing secrets with Secrets Manager
- Protecting and managing compute instance metadata

As a Professional Cloud Security Engineer, you play a critical role in protecting sensitive data. This includes being able to configure and run data-loss prevention (DLP) software such as Google Cloud DLP. It also includes protecting sensitive data with encryption, access control, service perimeters, and secure techniques for data manipulation with such Google Cloud tools as VPC Service Controls and Secrets Manager.

Question 1 tested your knowledge of configuring DLP to automatically inspect and redact personally identifiable information (PII). Question 2 tested your knowledge of using DLP features. Question 3 asked you to secure access to BigQuery. Question 4 tested your understanding of using VPC Service Controls with Service perimeter bridges. Question 5 explored your understanding of Secrets Manager, and Question 6 asked you about VM metadata.

Diagnostic Question 01 Discussion

Cymbal Bank has hired a data analyst team to analyze scanned copies of loan applications. Because this is an external team, Cymbal Bank does not want to share the name, gender, phone number, or credit card numbers listed in the scanned copies. You have been tasked with hiding this PII information while minimizing latency.

What should you do?

A. Use the Cloud Data Loss Prevention (DLP) API to make redact image requests. Provide your project ID, built-in infoTypes, and the scanned copies when you make the requests.

B. Use the Cloud Vision API to perform optical code recognition (OCR) from scanned images. Redact the text using the Cloud Natural Language API with regular expressions.

C. Use the Cloud Vision API to perform optical code recognition (OCR) from scanned images. Redact the text using the Cloud Data Loss Prevention (DLP) API with regular expressions.

D. Use the Cloud Vision API to perform text extraction from scanned images. Redact the text using the Cloud Natural Language API with regular expressions.

Google Cloud

Feedback:
A. Correct! The DLP API can be directly used for image redaction. Built-in infoTypes already include name, gender, phone number, and credit card numbers.

B. Incorrect. The Cloud Vision API's OCR can be used to extract text from images but OCR does not redact the text. The Cloud Natural Language API also cannot help with text redaction. Use the DLP API for this.

C. Incorrect. The Cloud Vision API's OCR can be used to extract text from images and then you can redact the text using the DLP API, but this process adds a layer of latency because it involves two steps. You can create custom infoTypes with regular expressions, but these are recommended only in situations where standard infoTypes aren't supported, such as medical account numbers.

D. Incorrect. The Cloud Vision API's OCR can be used to extract text from images and then you can redact the text using DLP API, but this process adds a layer of latency because it involves two steps. The Cloud Natural Language API cannot help with text redaction. Use the DLP API for this.

Where to look:
- https://cloud.google.com/dlp/docs/concepts-image-redaction
- https://cloud.google.com/dlp/docs/redacting-sensitive-data-images
- https://cloud.google.com/dlp/docs/infotypes-reference

Content mapping:
- ILT course: **Security in Google Cloud**
  - M10 Content-related Vulnerabilities: Techniques and Best Practices

- On-demand course: **Mitigating Security Vulnerabilities on Google Cloud**
  - M2 Content-related Vulnerabilities: Techniques and Best Practices

Summary:
The Cloud Data Loss Prevention (DLP) API can redact images, documents, and text. It offers built-in and custom infoTypes that can help identify sensitive information. Using one of the supported programming languages, you can programmatically make redact image requests to the DLP API.

Diagnostic Question 02 Discussion

Cymbal Bank needs to statistically predict the days customers delay the payments for loan repayments and credit card repayments. Cymbal Bank does not want to share the exact dates a customer has defaulted or made a payment with data analysts. Additionally, you need to hide the customer name and the customer type, which could be corporate or retail.

How do you provide the appropriate information to the data analysts?

A. Generalize all dates to year and month with bucketing. Use the built-in infoType for customer name. Use a custom infoType for customer type with a custom dictionary.

B. Generalize all dates to year and month with bucketing. Use the built-in infoType for customer name. Use a custom infoType for customer type with regular expression.

C. Generalize all dates to year and month with date shifting. Use a predefined infoType for customer name. Use a custom infoType for customer type with a custom dictionary.

D. Generalize all dates to year and month with date shifting. Use a predefined infoType for customer name. Use a custom infoType for customer type with regular expression.

Google Cloud

Feedback:

A. Incorrect. Bucketing can reduce timestamps to smaller groups, but can also lose the sequence of events and time intervals. Generalizing all dates to year and month will also create difficulty for prediction, because the prediction must be in days. The usage of the built-in infoType for customer name and a custom infoType for customer type with a custom dictionary is correct, however.

B. Incorrect. Bucketing can reduce timestamps to smaller groups, but can also lose the sequence of events and time intervals. Generalizing all dates to year and month will also create difficulty for prediction, because the prediction must be in days. Usage of the built-in infoType for customer name is correct. Using a custom InfoType with regular expression will require additional filtering.

C. Correct! If your data is stored in a valid schema, date shifting will shift all dates logically. Built-in infoTypes allow a range of locale-specific and globally identifiable sensitive information pieces like email IDs and phone numbers. Custom dictionaries can be used with a custom infoType that contains predefined key-value pairs.

D. Incorrect. If your data is stored in a valid schema, date shifting will shift all dates logically. Usage of the built-in infoType for customer name is correct. Using a custom InfoType with regular expression will require additional filtering.

Where to look:
https://cloud.google.com/dlp/docs/concepts-date-shifting

https://cloud.google.com/dlp/docs/concepts-infotypes
https://cloud.google.com/dlp/docs/pseudonymization

Summary:
Date shifting and bucketing can help with date-time generalizing. Although bucketing can reduce the timestamp to smaller groups such as month or year, it can lose the sequence of events and time intervals. Date shifting shifts the date-time stamps while preserving the order and time intervals. The shifting period is different for different rows of data, so design the schema wisely.

Cloud DLP uses built-in and custom infoType detectors to scan images, documents, and text. Custom infoTypes can be dictionaries, regular expressions, or dictionaries extracted from BigQuery or Cloud Storage. Use dictionaries when you want to match a list of words or phrases, and use regular expressions when you want to detect matches based on a regex pattern.

Diagnostic Question 03 Discussion

Cymbal Bank stores customer information in a BigQuery table called 'Information,' which belongs to the dataset 'Customers.' Various departments of Cymbal Bank, including loan, credit card, and trading, access the information table. Although the data source remains the same, each department needs to read and analyze separate customers and customer-attributes. You want a cost-effective way to configure departmental access to BigQuery to provide optimal performance.

What should you do?

A. Create separate datasets for each department. Create views for each dataset separately. Authorize these views to access the source dataset. Share the datasets with departments. Provide the bigquery.dataViewer role to each department's required users.

B. Create an authorized dataset in BigQuery's Explorer panel. Write Customers' table metadata into a JSON file, and edit the file to add each department's Project ID and Dataset ID. Provide the bigquery.user role to each department's required users.

C. Secure data with classification. Open the Data Catalog Taxonomies page in the Google Cloud Console. Create policy tags for required columns and rows. Provide the bigquery.user role to each department's required users. Provide policy tags access to each department separately.

D. Create separate datasets for each department. Create authorized functions in each dataset to perform required aggregations. Write transformed data to new tables for each department separately. Provide the bigquery.dataViewer role to each department's required users.

Google Cloud

Feedback:
A. Correct! Using authorized views is the right approach. Create a separate dataset for each department, and provide access to views containing filtered rows and columns.

B. Incorrect. There could be more tables or views in the 'Customers' dataset. Creating an authorized dataset will share all views inside it. The role bigquery.user is not sufficient because bigquery.dataViewer is required to query views.

C. Incorrect. Data classification could fit the scenario and add additional security on top of authorized views. However, authorized views have better performance and flexibility. The role bigquery.user is not sufficient because bigquery.dataViewer is required to query views.

D. Incorrect. Although authorized functions could fit the scenario with the help of user-defined functions (UDF), UDF execution is slower when compared to authorized views. Creating new tables would incur additional cost. Providing the bigquery.dataViewer role to each department's required users is correct.

Where to look:
- https://cloud.google.com/bigquery/docs/authorized-views
- https://cloud.google.com/bigquery/docs/authorized-datasets

Content mapping:

- ILT course: **Security in Google Cloud**
  - M6 Securing Cloud Data: Techniques and Best Practices

- On-demand course: **Security Best Practices in Google Cloud**
  - M2 Securing Cloud Data: Techniques and Best Practices

Summary:
Authorized views and data classification are two approaches for row-level security. Data classification helps with creating policies to access columns and rows. These policies can be assigned to users through Identity and Access Management (IAM). Authorized views help with providing limited control over the data. Both data classification and authorized views let you slice tables and provide different levels of access to BigQuery users.

Diagnostic Question 04 Discussion

Your colleague at Cymbal Bank is a cloud security engineer. She sketches out the following solution to manage her team's access to application security keys:

1 - Create 2 projects
- Project A: Cloud Storage to store secrets
- Project B: Cloud KMS to manage encryption keys

2 - Store each secret individually in Cloud Storage

3 - Rotate secrets and encryption keys regularly

4 - Protect each bucket by using encryption with Cloud KMS

What (if any) step does not follow Google Cloud's best practices for secret management?

A. Your colleague should have created one project for the Cloud Storage bucket and one to store the KMS encryption keys. Two projects create an unnecessary burden of IAM management.

B. Your colleague should cluster her secrets together in Cloud Storage. That way that can be easily accessed by applications.

C. It is not recommended to use Cloud KMS keys to encrypt buckets. Default management is safer and more reliable.

D. Your colleague's proposal follows Google Cloud's best practices.

Google Cloud

Feedback:
A. Incorrect. Google Cloud' s best practices recommend you create one project for the Cloud Storage bucket and one to store the KMS encryption keys.

B. Incorrect. You should store secrets individually in Cloud Storage.

C. Incorrect. Cloud KMS is the recommended solution for encrypting buckets.

D. Correct! Your colleague's proposal follows Google Cloud's best practices for managing access to application security keys.

Where to look:
https://cloud.google.com/secret-manager/docs

Content mapping:
- ILT course: **Security in Google Cloud**
  - M6 Securing Cloud Data: Techniques and Best Practices

- On-demand course: **Security Best Practices in Google Cloud**
  - M2 Securing Cloud Data: Techniques and Best Practices

Summary: Secret Manager allows you to store, manage, and access secrets as binary blobs or text strings. With the appropriate permissions, you can view the contents of the secret. Secret Manager works well for storing configuration

information such as database passwords, API keys, or TLS certificates needed by an application at runtime.

Cymbal Bank has a Cloud SQL instance that must be shared with an external agency. The agency's developers will be assigned roles and permissions through a Google Group in Identity and Access Management (IAM). The external agency is on an annual contract and will require a connection string, username, and password to connect to the database.

How would you configure the group's access?

A. Use Secret Manager. Use the duration attribute to set the expiry period to one year. Add the secretmanager.secretAccessor role for the group that contains external developers.

B. Use Cloud Key Management Service. Use the destination IP address and Port attributes to provide access for developers at the external agency. Remove the IAM access after one year and rotate the shared keys. Add cloudkms.cryptoKeyEncryptorDecryptor role for the group that contains the external developers.

C. Use Secret Manager. Use the resource attribute to set a key-value pair with key as duration and values as expiry period one year from now. Add secretmanager.viewer role for the group that contains external developers.

D. Use Secret Manager for the connection string and username, and use Cloud Key Management Service for the password. Use tags to set the expiry period to the timestamp one year from now. Add secretmanager.secretVersionManager and secretmanager.secretAccessor roles for the group that contains external developers.

Google Cloud

Feedback:
A. Correct! Secret Manager supports time types such as absolute time duration to invoke and revoke access. The Secret Assessor role is required to read the stored secrets in Secret Manager.

B. Incorrect. You can use Cloud KMS to configure and manage Google-managed, customer-managed, and customer-supplied encryption keys. With Cloud KMS, developers will be able to decrypt shared information. Using IP address and Port ranges is incorrect because users are available as a group in IAM.

C. Incorrect. Secret Manager supports time types such as absolute time duration to invoke and revoke access. However, the Viewer role for Secret Manager does not allow users to use secrets.

D. Incorrect. You can use Cloud KMS to configure and manage Google-managed, customer-managed, and customer-supplied encryption keys. All details should be stored only in Secret Manager for our scenario. With Cloud KMS, developers will be able to decrypt shared information.

Where to look:
https://cloud.google.com/secret-manager/docs/access-control

Content mapping:
- ILT course: **Security in Google Cloud**

- ○ M7 Application Security: Techniques and Best Practices

- ● On-demand course: **Security Best Practices in Google Cloud**
  - ○ M3 Application Security: Techniques and Best Practices

Summary:
Secret Manager helps save confidential details such as passwords and URLs. You can provide access to secrets using IAM. Secret Manager lets organizations share configured secrets instead of confidential information with developers. Cloud KMS is used for storing encryption keys that are either managed by Google or by the customer.

Cloud KMS lets you share symmetric and asymmetric keys. Cloud KMS can be used to encrypt/decrypt data, but that will expose critical information to developers in plain text.

Diagnostic Question 06 Discussion

Cymbal Bank wants to deploy an n-tier web application. The frontend must be supported by an App Engine deployment, an API with a Compute Engine instance, and Cloud SQL for a MySQL database. This application is only supported during working hours, App Engine is disabled, and Compute Engine is stopped. How would you enable the infrastructure to access the database?

How would you enable the infrastructure to access the database?

A. Use VM metadata to read the current machine's IP address, and use a gcloud command to add access to Cloud SQL. Store Cloud SQL's connection string and password in Cloud Key Management Service. Store the Username in Project metadata.

B. Use Project metadata to read the current machine's IP address, and use a startup script to add access to Cloud SQL. Store Cloud SQL's connection string in Cloud Key Management Service, and store the password in Secret Manager. Store the Username in Project metadata.

C. Use Project metadata to read the current machine's IP address and use a gcloud command to add access to Cloud SQL. Store Cloud SQL's connection string and username in Cloud Key Management Service, and store the password in Secret Manager.

D. Use VM metadata to read the current machine's IP address and use a startup script to add access to Cloud SQL. Store Cloud SQL's connection string, username, and password in Secret Manager.

Google Cloud

Feedback:
A. Incorrect. Using a gcloud command would require manual intervention or an external trigger. Storing Cloud SQL's connection string and password in Cloud KMS would allow users to decrypt sensitive information. Storing the username in Project metadata is incorrect because it potentially shares the username with more users than required.

B. Incorrect. Using a startup script to add the VM's IP address to Cloud SQL is the correct choice. However, storing Cloud SQL's connection string and password in Cloud KMS would allow users to decrypt sensitive information. Storing the username in Project metadata is incorrect because it potentially shares the username with more users than required.

C. Incorrect. VM metadata should be used to read the current session, which can fetch the IP address. Using a gcloud command would require manual intervention or an external trigger. Storing Cloud SQL's connection string and password in Cloud KMS would allow users to decrypt sensitive information. Storing the password in Secret Manager is the right choice, however.

D. Correct! Using the VM's metadata is the correct approach because the current machine will be able to provide its IP address, and requests will stay inside the host VM. A startup script can read a VM session and fetch the IP address. It can additionally configure the IP address to access Cloud SQL. Storing all data in Secret Manager lets you share sensitive information without revealing its text.

Where to look:
https://cloud.google.com/compute/docs/metadata/overview#vm_metadata_uses

Content mapping:
- ILT course: **Security in Google Cloud**
  - M5 Securing Compute Engine: Techniques and Best Practices
  - M7 Application Security: Techniques and Best Practices

- On-demand course: **Security Best Practices in Google Cloud**
  - M1 Securing Compute Engine: Techniques and Best Practices
  - M3 Application Security: Techniques and Best Practices

Summary:
Every virtual machine (VM) instance stores its metadata on a metadata server. The metadata server is particularly useful when used in combination with startup and shutdown scripts because you can use the metadata server to programmatically get unique information about a VM, without additional authorization. Secret Manager helps save confidential details such as passwords and URLs. You can provide access to secrets using IAM. Secret Manager lets organizations share configured secrets instead of confidential information with developers.

3.1 | Protecting sensitive data and preventing data loss

Courses

Security in Google Cloud
- M5 Securing Compute Engine: Techniques and Best Practices
- M6 Securing Cloud Data: Techniques and Best Practices
- M7 Application Security: Techniques and Best Practices
- M10 Content-Related Vulnerabilities: Techniques and Best Practices

Security Best Practices in Google Cloud
- M1 Securing Compute Engine: Techniques and Best Practices
- M2 Securing Cloud Data: Techniques and Best Practices
- M3 Application Security: Techniques and Best Practices

Mitigating Security Vulnerabilities in Google Cloud
- M2 Content-Related Vulnerabilities: Techniques and Best Practices

Documentation

Image inspection and redaction | Data Loss Prevention Documentation | Google Cloud

Redacting sensitive data from images | Data Loss Prevention Documentation | Google Cloud

InfoType detector reference | Data Loss Prevention Documentation | Google Cloud

Pseudonymization | Data Loss Prevention Documentation | Google Cloud

Authorized views | BigQuery | Google Cloud

Authorized datasets | BigQuery | Google Cloud

Sharing across perimeters with bridges | VPC Service Controls | Google Cloud

Creating a perimeter bridge | VPC Service Controls | Google Cloud

Context-aware access with ingress rules | VPC Service Controls | Google Cloud

Frequently asked questions | IAM Documentation

Access control with IAM | Secret Manager Documentation | Google Cloud

About VM metadata | Compute Engine Documentation | Google Cloud

---

Let's take a moment to consider resources that can help you build your knowledge and skills in this area.

The concepts in the diagnostic questions we just reviewed are covered in these modules and in this documentation. Reviewing the documentation is highly recommended. You'll find this list in your workbook so you can take a note of what you want to include later when you build your study plan. Based on your experience with the diagnostic questions, you may want to include some or all of these.

- https://cloud.google.com/dlp/docs/concepts-image-redaction
- https://cloud.google.com/dlp/docs/redacting-sensitive-data-images
- https://cloud.google.com/dlp/docs/infotypes-reference
- https://cloud.google.com/dlp/docs/pseudonymization
- https://cloud.google.com/bigquery/docs/authorized-views
- https://cloud.google.com/bigquery/docs/authorized-datasets
- https://cloud.google.com/vpc-service-controls/docs/share-across-perimeters
- https://cloud.google.com/vpc-service-controls/docs/create-perimeter-bridges
- https://cloud.google.com/vpc-service-controls/docs/context-aware-access
- https://cloud.google.com/iam/docs/faq#how_do_i_grant_permissions_to_resources_in_my_project_to_someone_who_is_not_part_of_my_organization
- https://cloud.google.com/secret-manager/docs/access-control
- https://cloud.google.com/compute/docs/metadata/overview#vm_metadata_uses

3.2 | Managing encryption at rest, in transit, and in use

Considerations include:

- Understanding use cases for Google default encryption, Customer-Managed Encryption Keys (CMEK), Customer-Supplied Encryption Keys (CSEK), Cloud External Key Manager (EKM), and Cloud HSM
- Creating and managing encryption keys for CMEK, CSEK, and EKM
- Applying Google's encryption approach to use cases
- Configuring object lifecycle policies for Cloud Storage
- Enabling confidential computing
- Encryption in transit

Google Cloud

A Professional Cloud Security Engineer should also have a clear understanding of the considerations involved in managing encryption at rest, and be able to apply Google's encryption approach to a variety of use cases. You should be familiar with Customer-Managed Encryption Keys (CMEK), Customer-Supplied Encryption Keys (CSEK), Cloud External Key Manager (EKM), and Cloud HSM.

Question 7 tested your knowledge of Cloud Storage object lifecycle management. Question 8 asked you to identify the steps necessary to apply encryption settings. Question 9 asked you to configure Cloud KMS for key rotation. Question 10 tested your understanding of confidential VMs and their benefits.

| Diagnostic Question 07 Discussion

Cymbal Bank calculates employee incentives on a monthly basis for the sales department and on a quarterly basis for the marketing department. The incentives are released with the next month's salary. Employee's performance documents are stored as spreadsheets, which are retained for at least one year for audit. You want to configure the most cost-effective storage for this scenario.

What should you do?

A. Import the spreadsheets to BigQuery, and create separate tables for Sales and Marketing. Set table expiry rules to 365 days for both tables. Create jobs scheduled to run every quarter for Marketing and every month for Sales.

B. Upload the spreadsheets to Cloud Storage. Select the Nearline storage class for the sales department and Coldline storage for the marketing department. Use object lifecycle management rules to set the storage class to Archival after 365 days. Process the data on BigQuery using jobs that run monthly for Sales and quarterly for Marketing.

C. Import the spreadsheets to Cloud SQL, and create separate tables for Sales and Marketing. For Table Expiration, set 365 days for both tables. Use stored procedures to calculate incentives. Use App Engine cron jobs to run stored procedures monthly for Sales and quarterly for Marketing.

D. Import the spreadsheets into Cloud Storage and create NoSQL tables. Use App Engine cron jobs to run monthly for Sales and quarterly for Marketing. Use a separate job to delete the data after 1 year.

Google Cloud

Feedback:
A. Incorrect. Although this solution works, it is not the most cost-effective. Use BigQuery if you need a high-performance solution to disburse salary immediately after processing. Use Cloud Storage and load external data into BigQuery to lower the cost.

B. Correct! Cloud Storage storage classes let you lower the storage cost for data that you access less frequently and don't require for real-time applications. Use object lifecycle rules to change storage classes and expire data. For processing, use BigQuery, which has a free daily quota.

C. Incorrect. Cloud SQL is a more expensive choice than Cloud Storage storage classes. App Engine has a free quota that can be used to run your cron jobs, but your solutions need to run once a month and once a quarter. App Engine is good for scenarios that require web availability or high availability.

D. Incorrect. Use Datastore for NoSQL transactional applications or semi-structured information such as categories, subcategories, product descriptions, logs, and variable sensor data. Using Datastore for highly structured information is possible, but is not the product use case. You will also need to run additional infrastructure to manipulate all aspects of data.

Where to look:
● https://cloud.google.com/storage/docs/storage-classes

- https://cloud.google.com/storage/docs/lifecycle

Content mapping:
- ILT course: **Security in Google Cloud**
  - M6 Securing Cloud Data: Techniques and Best Practices

- On-demand course: **Security Best Practices in Google Cloud**
  - M2 Securing Cloud Data: Techniques and Best Practices

Summary:
Cloud Storage lets you use storage classes that are less expensive than standard storage. These storage classes use low-performance HDDs compared to standard SDDs. The cost-performance trade-off lets you build low-cost, resilient applications that still have the fastest read access and lowest latency in the cloud space. Cloud Storage object lifecycle rules let you change storage classes or set expiration rules to further reduce storage costs.

Diagnostic Question 08 Discussion

Cymbal Bank uses Google Kubernetes Engine (GKE) to deploy its Docker containers. You want to encrypt the boot disk for a cluster running a custom image so that the key rotation is controlled by the Bank. GKE clusters will also generate up to 1024 randomized characters that will be used with the keys with Docker containers.

What steps would you take to apply the encryption settings with a dedicated hardware security layer?

A. In the Google Cloud console, navigate to Google Kubernetes Engine. Select your cluster and the boot node inside the cluster. Enable customer-managed encryption. Use Cloud HSM to generate random bytes and provide an additional layer of security.

B. Create a new GKE cluster with customer-managed encryption and HSM enabled. Deploy the containers to this cluster. Delete the old GKE cluster. Use Cloud HSM to generate random bytes and provide an additional layer of security.

C. Create a new key ring using Cloud Key Management Service. Extract this key to a certificate. Use the kubectl command to update the Kubernetes configuration. Validate using MAC digital signatures, and use a startup script to generate random bytes.

D. Create a new key ring using Cloud Key Management Service. Extract this key to a certificate. Use the Google Cloud Console to update the Kubernetes configuration. Validate using MAC digital signatures, and use a startup script to generate random bytes.

Google Cloud

Feedback:
A. Incorrect. A Kubernetes cluster can be accessed through the kubectl command. Usage of Cloud HSM is correct.

B. Correct! Building a new cluster and deleting the old one is the solution. Cloud HSM provides an additional layer of dedicated hardware security and generates random bytes of up to 1024 characters.

C. Incorrect. Validating using MAC digital signatures is not helpful because they are used to verify messages. However, a startup script can be used to generate a random sequence.

D. Incorrect. The Google Cloud console cannot be used to edit a Kubernetes configuration. Validating using MAC digital signatures is not helpful because they are used to verify messages. However, a startup script can be used to generate a random sequence.

Where to look:
- https://cloud.google.com/kubernetes-engine/docs/how-to/using-cmek#boot-disks
- https://cloud.google.com/kubernetes-engine/docs/how-to/custom-boot-disks
- https://cloud.google.com/kms/docs/using-other-products#cmek_integrations

Content mapping:

- ILT course: **Security in Google Cloud**
  - M5 Securing Compute Engine: Techniques and Best Practices
  - M6 Securing Cloud Data: Techniques and Best Practices
  - M8 Securing Google Kubernetes Engine

- On-demand course: **Security Best Practices in Google Cloud**
  - M1 Securing Compute Engine: Techniques and Best Practices
  - M2 Securing Cloud Data: Techniques and Best Practices
  - M4 Securing Google Kubernetes Engine

- Quest: Ensure Access & Identity in Google Cloud

Summary:
All Google Cloud resources default to have data encrypted at rest. You can use Google-Managed Encryption Keys to further encrypt GKE clusters, Compute Engine instance boot disks, Cloud Storage, and BigQuery. You can use a Customer-Supplied Encryption Key to replace the Google keys with your own keys. Alternatively, you could use Customer-Managed Encryption Keys to rotate keys.

Diagnostic Question 09 Discussion

You have recently joined Cymbal Bank as a cloud security engineer. You want to encrypt a connection from a user on the internet to a VM in your development project. This is at the layer 3/4 (network/transport) level and you want to set up user configurable encryption for the in transit network traffic.

What architecture choice best suits this use case?

A. Set up an IPsec tunnel. This will allow you to create L3/L4 encryption between a user and a VM instance in her project.

B. Set up transport layer security (TLS). This will encrypt data sent to the Google Front End, and in turn, your VM. This is not setup by default.

C. Set up a managed SSL certificate by configuring a load balancer. By default, this will encrypt at the L3/L4 layer.

D. Set up app layer transport security (ALTS). This is a mutual authentication and transport encryption system developed by Google. This is configured for L3/L4 network connections.

Google Cloud

Feedback:
A. Correct! IPsec tunnels are used to make connections at the L3 layer, and they are encrypted by one VPN gateway and decrypted by the other VPN gateway.

B. Incorrect. The TLS protocol operates at layers 4 through 7 (transport - application).

C. Incorrect. SSL proxy load balancing operates at layer 4.

D. Incorrect. App layer transport security (ALTS) is a mutual authentication and transport encryption system developed by Google and operates at the application layer (7).

Where to look:
https://cloud.google.com/network-connectivity/docs/vpn/concepts/overview#ipsec_and_ike_support

Content mapping:
- ILT course: **Security in Google Cloud**
  - M4 Configuring Virtual Private Cloud for Isolation and Security

- On-demand course: **Security Best Practices in Google Cloud**
  - M4 Configuring Virtual Private Cloud for Isolation and Security

Summary:

Adding IPsec encryption to your in-transit traffic is important for meeting your data encryption and other compliance needs, especially if you must connect to a third-party service provider.

| Diagnostic Question 10 Discussion

Cymbal Bank needs to migrate existing loan processing applications to Google Cloud. These applications transform confidential financial information. All the data should be encrypted at all stages, including sharing between sockets and RAM. An integrity test should also be performed every time these instances boot. You need to use Cymbal Bank's encryption keys to configure the Compute Engine instances.

A. Create a Confidential VM instance with Customer-Supplied Encryption Keys. In Cloud Logging, collect all logs for sevLaunchAttestationReportEvent.

B. Create a Shielded VM instance with Customer-Supplied Encryption Keys. In Cloud Logging, collect all logs for earlyBootReportEvent.

C. Create a Confidential VM instance with Customer-Managed Encryption Keys. In Cloud Logging, collect all logs for earlyBootReportEvent.

D. Create a Shielded VM instance with Customer-Managed Encryption Keys. In Cloud Logging, collect all logs for sevLaunchAttestationReportEvent.

What should you do?

Google Cloud

Feedback:
A. Correct! Use Customer-Supplied Encryption Keys because you need to use your own encryption keys. Confidential VMs have a unique launch attestation event that can be read from Cloud Logging.

B. Incorrect. Although using Customer-Supplied Encryption Keys is the correct choice, earlyBootReportEvent is not the parameter for booting. Use the launch attestation event from Cloud Logging.

C. Incorrect. Customer-Managed Encryption Keys will only let you manage key rotation, but you need to use your own encryption keys. Use the launch attestation event from Cloud Logging because earlyBootReportEvent is not the parameter for booting.

D. Incorrect. Customer-Managed Encryption Keys only let you manage key rotation, but you need to use your own encryption keys. However, Confidential VMs have a unique launch attestation event that can be read from Cloud Logging, so sevLaunchAttestationReportEvent is the correct choice.

Where to look:
https://cloud.google.com/compute/confidential-vm/docs/about-cvm

Content mapping:
● ILT course: **Security in Google Cloud**

- ○ M5 Securing Compute Engine: Techniques and Best Practices

- ● On-demand course: **Security Best Practices in Google Cloud**
  - ○ M1 Securing Compute Engine: Techniques and Best Practices

Summary:
Confidential VMs use AMD's Secure Encrypted Virtualization, which keeps data encrypted in RAM. They can be managed using Customer-Supplied or Customer-Managed Encryption Keys. These instances contain dedicated AES engines that encrypt data as it flows out of sockets and decrypt data when it is read.

When restarting, Confidential VMs generate a unique log called Launch Attestation. Cloud Logging can be used to filter the logs and collect sevLaunchAttestationReportEvent.

3.2 | Managing encryption at rest, in transit, and in use

Courses

Security in Google Cloud
- M4 Configuring Virtual Private Cloud for Isolation and Security
- M5 Securing Compute Engine: Techniques and Best Practices
- M6 Securing Cloud Data: Techniques and Best Practices
- M8 Securing Google Kubernetes Engine

Managing Security in Google Cloud
- M4 Configuring Virtual Private Cloud for Isolation and Security

Security Best Practices in Google Cloud
- M1 Securing Compute Engine
- M2 Securing Cloud Data
- M4 Securing Google Kubernetes Engine

Skill Badges

Google Cloud

Ensure Access and Identity in Google Cloud Quest

Documentation

Storage classes | Google Cloud

Object Lifecycle Management | Cloud Storage

Use customer-managed encryption keys (CMEK) | Kubernetes Engine Documentation | Google Cloud

Configuring a custom boot disk | Kubernetes Engine Documentation | Google Cloud

Using Cloud KMS with other products

Rotating keys | Cloud KMS Documentation

Confidential VM and Compute Engine | Google Cloud

Let's take a moment to consider resources that can help you build your knowledge and skills in this area.

The concepts in the diagnostic questions we just reviewed are covered in these modules and in this documentation. Reviewing the documentation is highly recommended. You'll find this list in your workbook so you can take a note of what you want to include later when you build your study plan. Based on your experience with the diagnostic questions, you may want to include some or all of these.

- https://cloud.google.com/storage/docs/storage-classes
- https://cloud.google.com/storage/docs/lifecycle
- https://cloud.google.com/kubernetes-engine/docs/how-to/using-cmek#boot-disks
- https://cloud.google.com/kubernetes-engine/docs/how-to/custom-boot-disks
- https://cloud.google.com/kms/docs/using-other-products#cmek_integrations
- https://cloud.google.com/kms/docs/rotating-keys
- https://cloud.google.com/compute/confidential-vm/docs/about-cvm