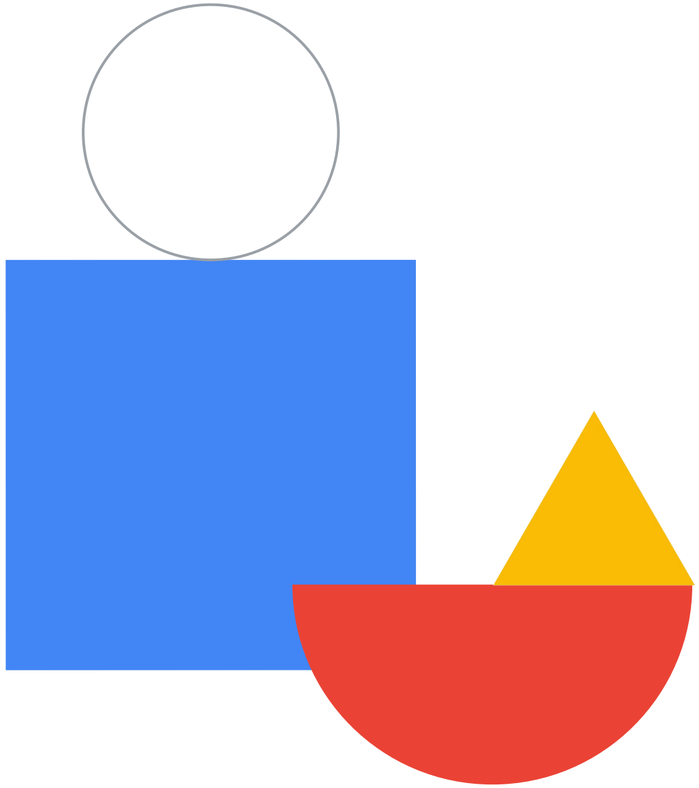
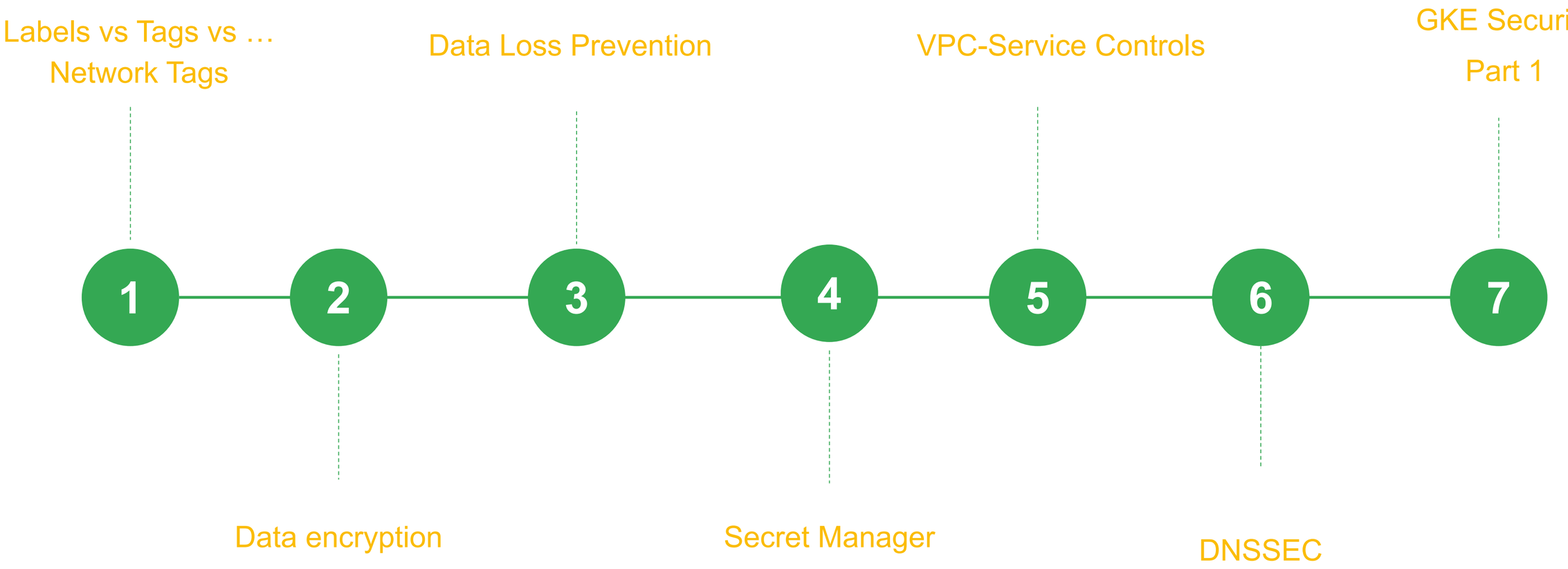
Google Cloud



Preparing for Your Professional Cloud Security Engineer Journey

Module 3: Ensuring Data Protection

Week 3 topics



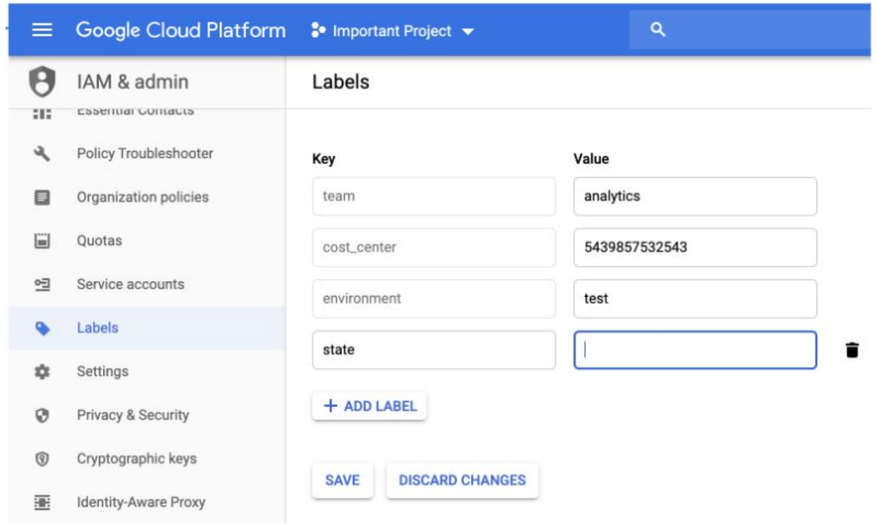
Labels vs Tags vs … Network Tags

What is cloud labeling?

Labeling cloud resources **helps the IT team understand cloud spend** at a granular level

Key features

- A label is a customer-defined key and value pair used to organize Google Cloud resources
- Labeling allows you to assign your own metadata to each taggable resource
- Labeling enables categorization of resources by purpose, owner, environment, etc.



Label requirements

- Each resource can have multiple labels, up to a maximum of 64.
- Each label must be a key-value pair.
- Keys have a minimum length of one character and a maximum length of 63 characters, and cannot be empty. Values can be empty, and have a maximum length of 63 characters.
- Keys and values can contain only lowercase letters, numeric characters, underscores, and dashes. All characters must use UTF-8 encoding, and international characters are allowed.
- The key portion of a label must be unique. However, you can use the same key with multiple resources.
- Keys must start with a lowercase letter or international character.

Common use of labels

- **Team labels**: Add labels based on team or cost center to distinguish resources owned by different teams (for example, team:research and team:analytics).
- **Cost center labels:** You can use this type of label for cost accounting, budgeting, or chargeback modeling (for example, product:costcenternumber, etc.).
- **Component labels**: For example, component:redis, component:frontend, component:ingest, and component:dashboard.
- **Environment or stage labels**: For example, environment:production and environment:test.
- **State labels**: For example, state:active, state:readytodelete, and state:archive.
- **VM labels**: A label can be attached to a VM.

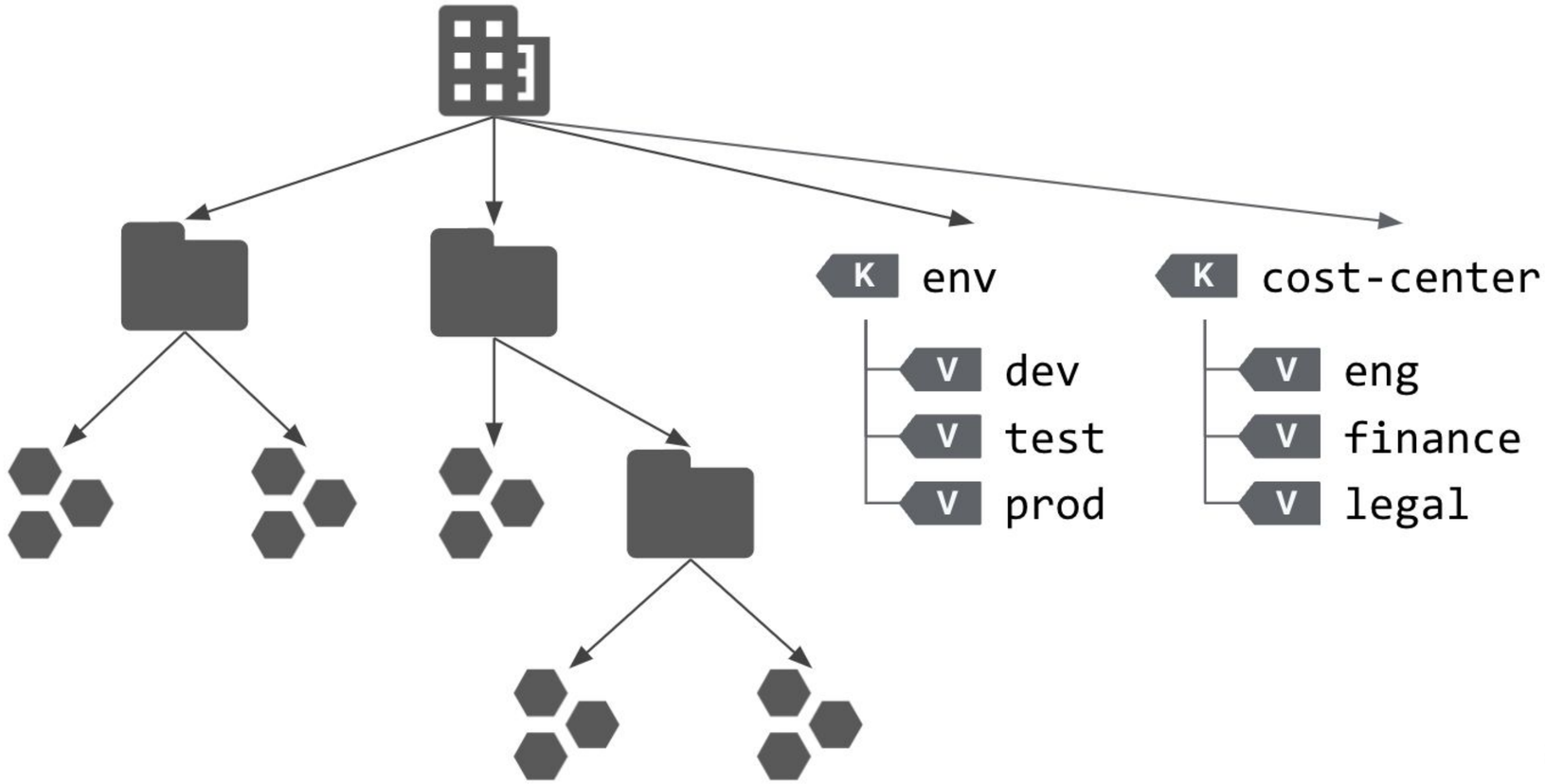
Exam Tip: *it's not recommended to create large numbers of unique labels, such as for timestamps or individual values of every API call.*

What are GCP Tags?

!!! NOT the same as “Network Tags” !!!

Tags are **resources** in the form of **key-value pairs** that can serve as **metadata** and be **associated with a resource**.

They can be **used to identify groups of related resources** (e.g., `env=prod`, `data-sensitivity=confidential`) and can also be **referenced in policies** (i.e IAM Policies, Organization Policies)



How are labels / tags / network tags different?

Labels have historically been the way to assign costs in GCP. Historically in GCP, Tags typically referred to 'Network Tags', which are one of the options (in parallel to Service Accounts) when designing firewall rules.
***Tags can be thought of as 'Labels v2'** in many ways and the below table clarifies the terminology in use*

Metadata type	Description
Tags	• Aka 'Labels v2' • Key-value pairs with robust permission model, inheritance and centralized management • Supported by many resources but only tags attached to Compute Engine instances and GCP projects will appear in the billing data. • Has to be defined in advance • Inheritance • Can be enforced through policy • Supported in BQ Billing Export and Asset Inventory
Labels	• Key value pairs - Supported by many resources. All attachable labels will appear in the billing data. • Free-form • Supported in BQ Billing export, Asset Inventory and Monitoring metrics
Network Tags	• For controlling GCP network traffic only.

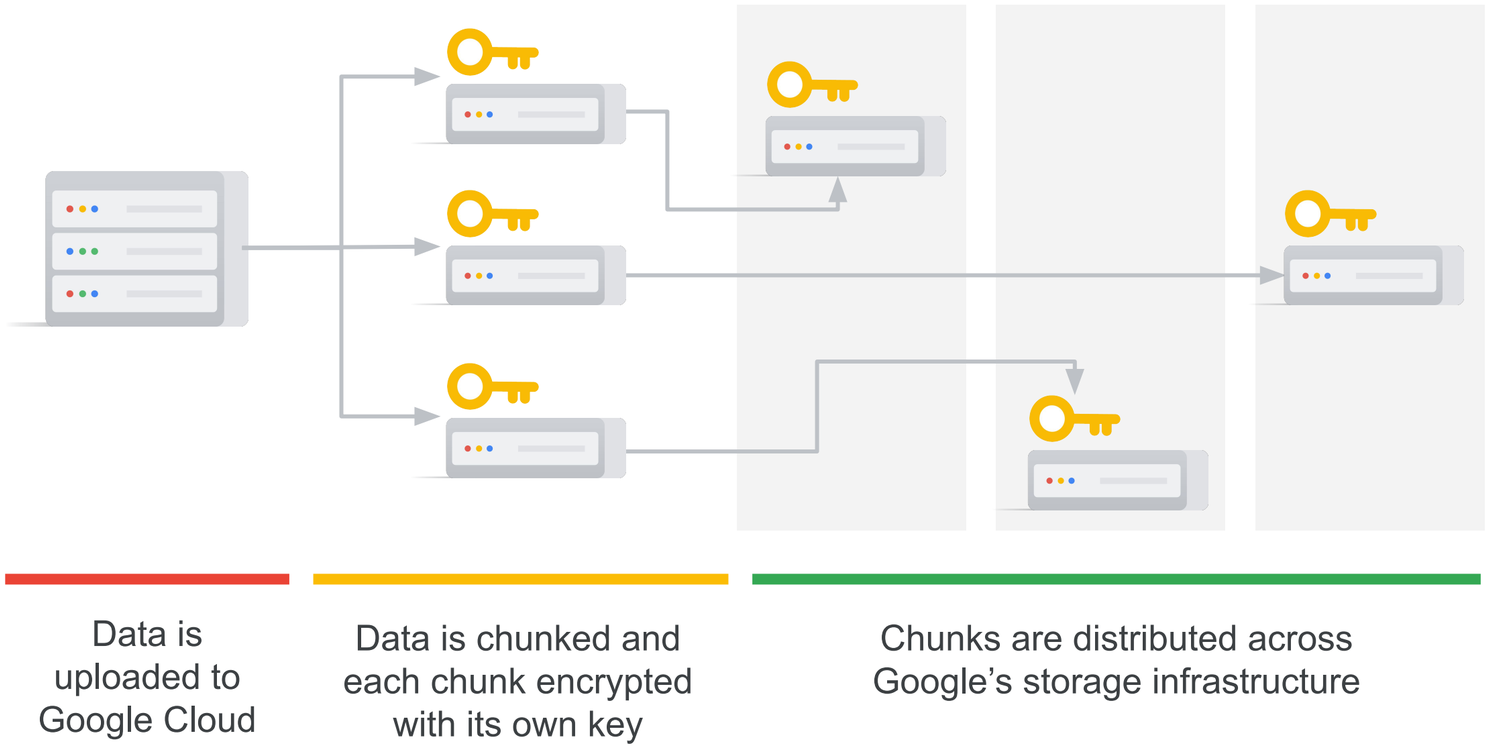
Data Encryption

Ensure data confidentiality with Google Cloud data encryption options

All data at rest is encrypted by default in Google Cloud using a multi-level encryption scheme.

You can take more control over encryption by using:

- Customer-managed encryption keys (CMEK)
- Customer-supplied encryption keys (CSEK)
- External key management (EKM)
- Cloud hosted security module (HSM)



Data encryption at rest options

DEFAULT ENCRYPTION

Google default data-at-rest encryption. Customer has no access to keys or control of key rotation.

CLOUD KMS

Customer can manage keys generated and stored by Google.

CLOUD HSM

Customer can manage keys generated by Google and stored in a Google owned and operated HSM.

CUSTOMER-SUPPLIED ENCRYPT. KEYS

Keys owned by customer and provided on each API call to be used ephemerally to access data.

HOSTED PRIVATE HSM

Select customers may use keys in their own HSM in a CoLo. Google does not have any control of the HSM.

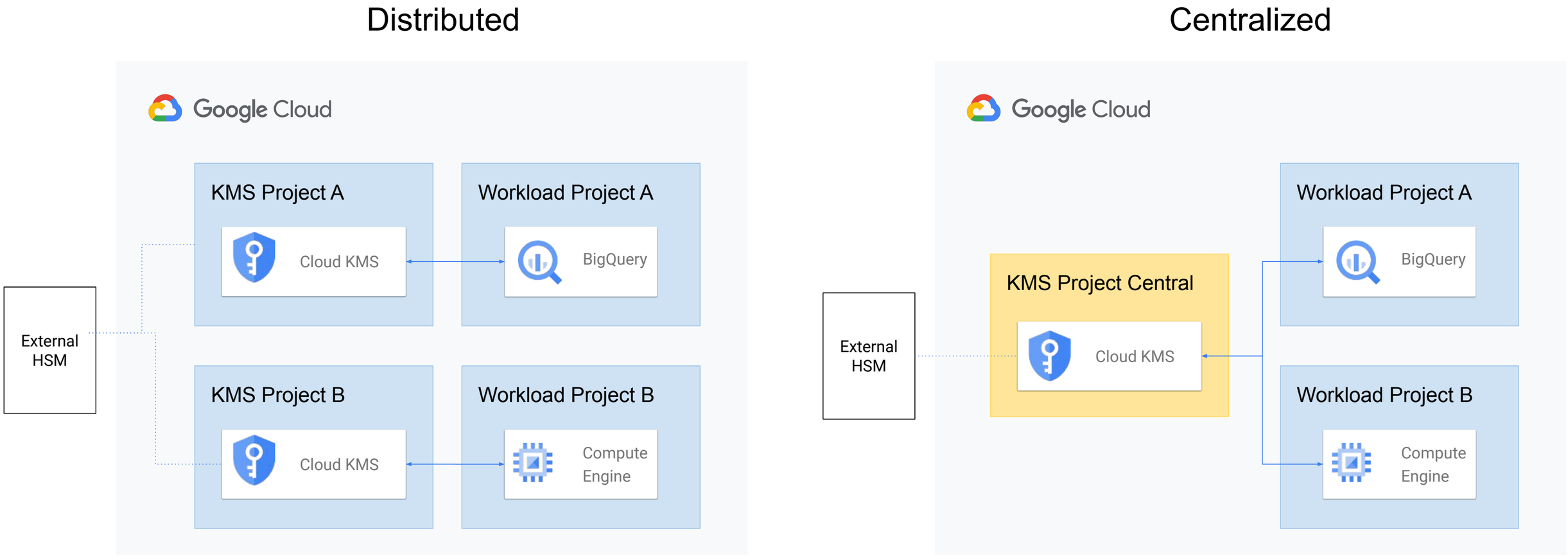
CLOUD EKM

Customer encrypts data-at-rest using a key residing outside of Google Cloud

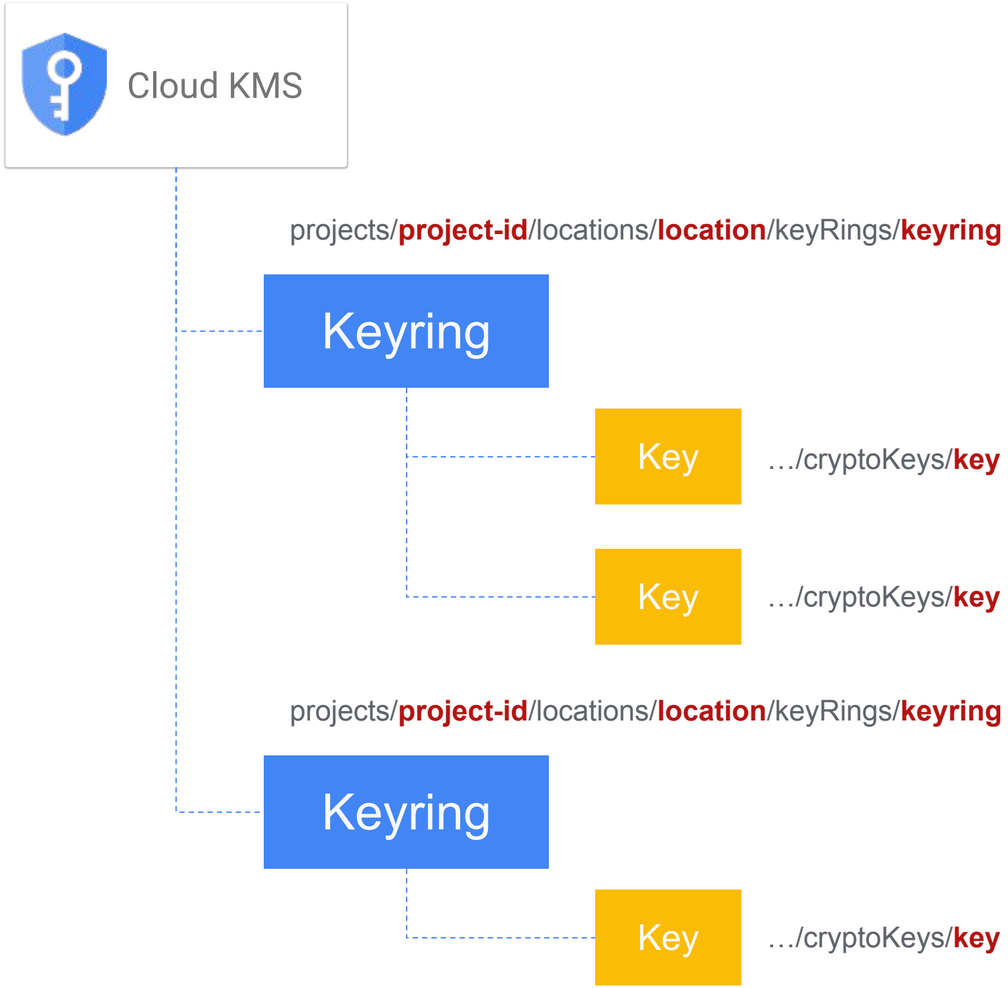
Fully automated management

Finer-grained customer control

Cloud KMS - Distributed vs Centralized



Keyrings and key hierarchy



Project to represent:

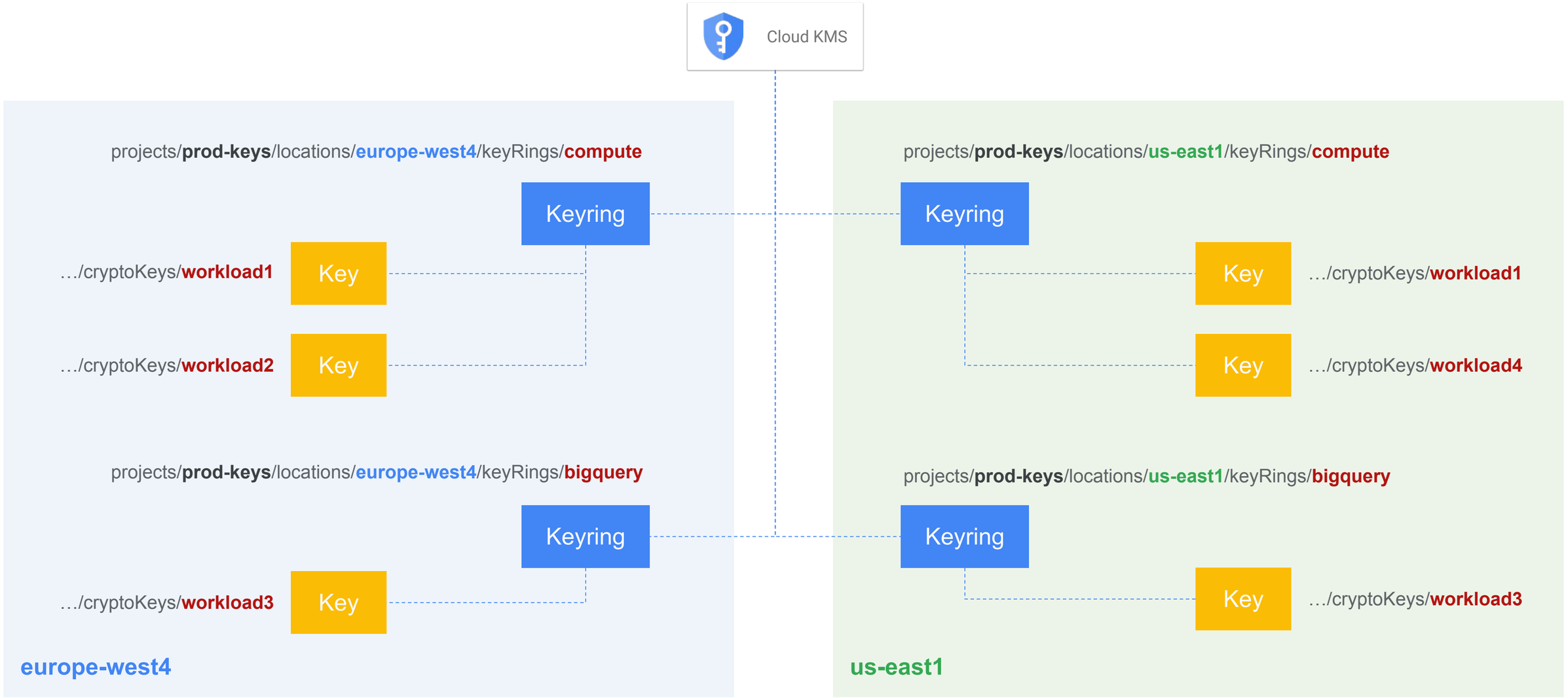
- Environment (e.g. prod and non-prod
- Legal entity

Keyring to represent:

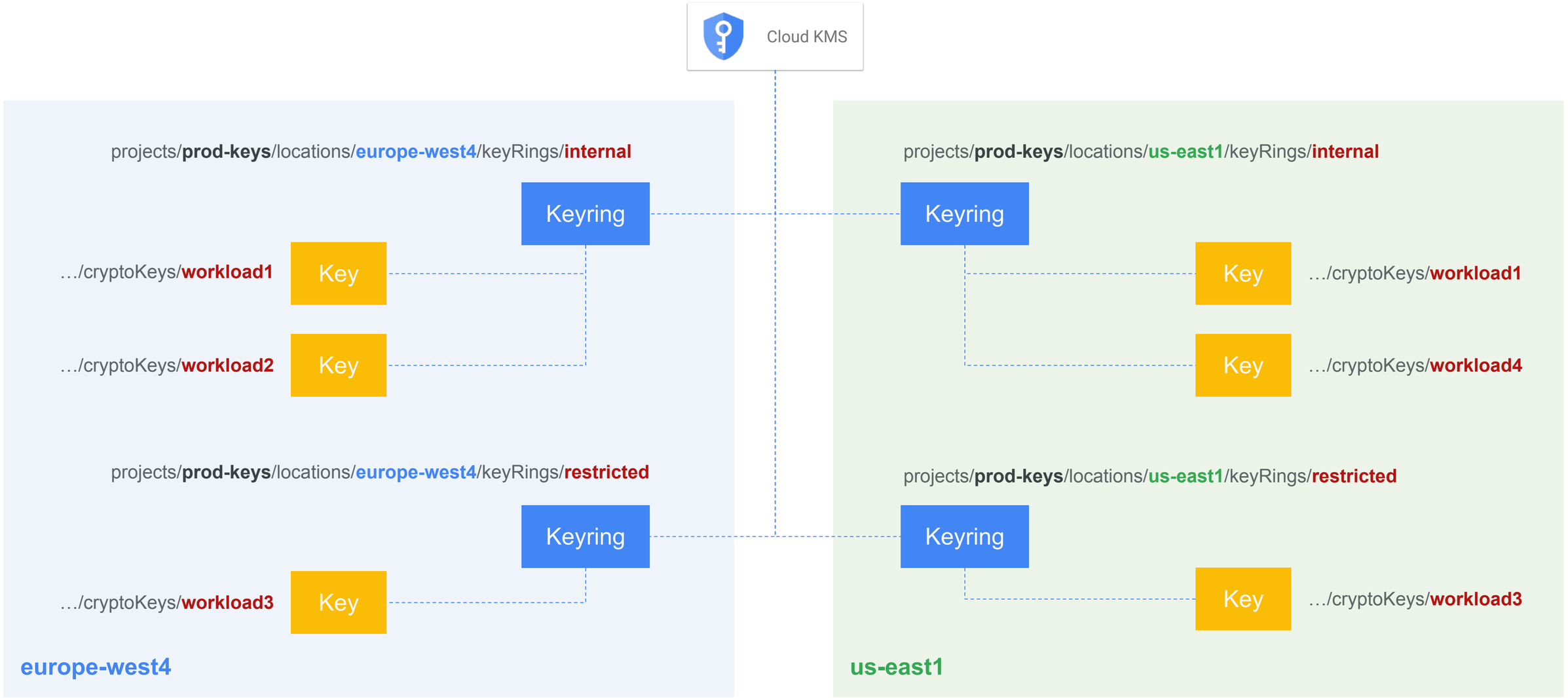
- Location
- Security classification
- Legal entity (if not split on project level)
- Service (e.g. GCE, GCS, BQ)

Key for every workload.

Example: Service split



Example: Data classification split



3.2 Diagnostic Question 09 Discussion

Cymbal Bank has an equated monthly installment (EMI) application. This application must comply with PCI-DSS standards because it stores credit card information. For additional security, you use asymmetric keys to encrypt the data and rotate the keys at fixed intervals. Cymbal Bank has recently migrated to Google Cloud, and you need to set up key rotation.

How would you configure Cloud Key Management Service (KMS)?

A. Use manual key rotation and assign yourself the cloudkms.cryptoKeyEncrypterDecrypter role.

B. Use automatic key rotation and assign yourself the cloudkms.cryptoKeyEncrypterDecrypter role.

C. Use automatic key rotation and assign yourself the cloudkms.admin role.

D. Use manual key rotation and assign yourself the cloudkms.admin role.

3.2 Diagnostic Question 09 Discussion

Cymbal Bank has an equated monthly installment (EMI) application. This application must comply with PCI-DSS standards because it stores credit card information. For additional security, you use asymmetric keys to encrypt the data and rotate the keys at fixed intervals. Cymbal Bank has recently migrated to Google Cloud, and you need to set up key rotation.

How would you configure Cloud Key Management Service (KMS)?

A. Use manual key rotation and assign yourself the cloudkms.cryptoKeyEncrypterDecrypter role.

B. Use automatic key rotation and assign yourself the cloudkms.cryptoKeyEncrypterDecrypter role.

C. Use automatic key rotation and assign yourself the cloudkms.admin role.

D. Use manual key rotation and assign yourself the cloudkms.admin role.

3.2 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.

3.2 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.

3.2 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?

3.2 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.

What should you do?

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.

4.2 Diagnostic Question 03 Discussion

Cymbal Bank wants to use Cloud Storage and BigQuery to store safe deposit usage data. Cymbal Bank needs a cost-effective approach to auditing only Cloud Storage and BigQuery data access activities.

How would you use Cloud Audit Logs to enable this analysis?

A. Enable Data Access Logs for ADMIN_READ, DATA_READ, and DATA_WRITE at the service level for BigQuery and Cloud Storage.

B. Enable Data Access Logs for ADMIN_READ, DATA_READ, and DATA_WRITE at the organization level.

C. Enable Data Access Logs for ADMIN_READ, DATA_READ, and DATA_WRITE for Cloud Storage. All Data Access Logs are enabled for BigQuery by default.

D. Enable Data Access Logs for ADMIN_READ, DATA_READ, and DATA_WRITE for BigQuery. All Data Access Logs are enabled for Cloud Storage by default.

4.2 Diagnostic Question 03 Discussion

Cymbal Bank wants to use Cloud Storage and BigQuery to store safe deposit usage data. Cymbal Bank needs a cost-effective approach to auditing only Cloud Storage and BigQuery data access activities.

How would you use Cloud Audit Logs to enable this analysis?

A. Enable Data Access Logs for ADMIN_READ, DATA_READ, and DATA_WRITE at the service level for BigQuery and Cloud Storage.

B. Enable Data Access Logs for ADMIN_READ, DATA_READ, and DATA_WRITE at the organization level.

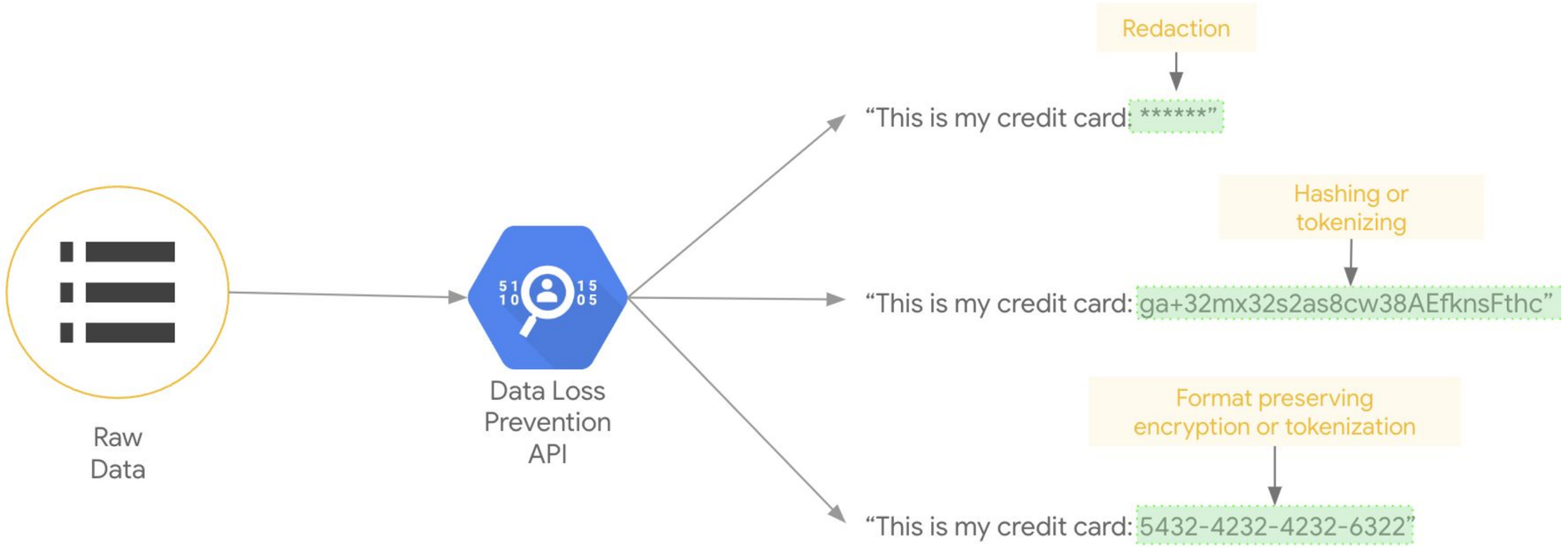
C. Enable Data Access Logs for ADMIN_READ, DATA_READ, and DATA_WRITE for Cloud Storage. All Data Access Logs are enabled for BigQuery by default.

D. Enable Data Access Logs for ADMIN_READ, DATA_READ, and DATA_WRITE for BigQuery. All Data Access Logs are enabled for Cloud Storage by default.

Cloud DLP

Cloud DLP (Data Loss Prevention)

Provides programmatic access to a powerful detection engine for PII Data



Hello, My Name is Thomas Anderson. I received a message that my account has been closed. Can you please reopen my account? Do you need my SSN: 123-45-6789. Please call +1-727-555-1212 or email thomas.anderson@example.org.

Hello, My Name is Thomas Anderson. I received a message that my account has been closed. Can you please reopen my account? Do you need my [redacted]-6789. Ple[redacted]555-1212 or [redacted]ple.org.

De-identification
(Data Masking)

Easy to use transformations
Redaction, masking, pseudonymization, tokenization, format-preserving encryption, date-shifting and more.

Handle structured and unstructured data
Apply transforms to an entire column or based on classified data in a “blob of text” or both.

Mask images
Generate redacted images based on findings or remove all text.

ID	Job Title	Phone	Comments
359740	Senior Engineer	307-964-0673	Please email them at jane@imadethisup.com
981587	VP, Engineer	713-910-6787	none
394091	Lawyer	692-398-4146	Updated phone to: 692-398-4146
986941	Senior Ops Manager	294-967-5508	none
490456	Junior Ops Manager	791-954-3281	Tried to verify account with their SSN 222-44-5555

De-ID: Tokenization

	A	B	C
1	userid	transaction_date	data1
2	jane@example.org	12/29/2018	Hello my email is jane@example.org
3	maria@example.org	9/12/2018	I am having trouble with my order
4	robert@example.org	2/14/2019	My payment card is 4111-1111-1111-1111

Tokenize

Inspect & Redact

Row	userid	transaction_date	data1
1	T1(32):Af9BFf7tF/2g34w9egkb0LGhZAraIw==	2020-02-07	Hello my email is [EMAIL_ADDRESS]
2	T1(32):AUiIUzf+N62KzhGtNhWQTG3cDtCn1w==	2019-05-30	Hello my email is [EMAIL_ADDRESS]
3	T1(32):Afouix9iCzsLcaOpHbKLIVmt6TrJbQ==	2018-05-01	I am having trouble with my order
4	T1(32):AYTj/bMivbZ37dAME+IQ4wb/cTLmfA==	2019-05-07	I am having trouble with my order
5	T1(32):AYPpVAWy34Ymeuv7OdV0utN626zq6Q==	2018-05-27	Hello my email is [EMAIL_ADDRESS]
6	T1(32):ASUkwQG7s2abH/k0ksD8q1fkv8fc6Q==	2018-11-30	Hello my email is [EMAIL_ADDRESS]
7	T1(32):ARQctEZGZHBSQNbVOpbue5hnETA9MQ==	2017-11-16	I am having trouble with my order
8	T1(32):AfhP78xsIReCqTl++ugYM5oCRfyZ4g==	2019-04-24	Hello my email is [EMAIL_ADDRESS]
9	T1(32):AXielhmrk8g8B17l2CPddl3JGjaBug==	2018-05-06	I am having trouble with my order
10	T1(32):AeKYHtMlCimEl+mBLfUTN7FdrRSOcg==	2018-07-06	My payment card is [CREDIT_CARD_NUMBER]
11	T1(32):AY58OJ6Z5y4ul4L93VVD2Efr9oLVag==	2019-12-27	Hello my email is [EMAIL_ADDRESS]
12	T1(32):AQW7f/9IEpEXIO7Eb3wEaEv7eZJHQA==	2019-02-22	My payment card is [CREDIT_CARD_NUMBER]

```
1 SELECT
2   userid,
3   COUNT(*) AS icount
4 FROM `deid-demo-lock1.webinar_06.*`
5 GROUP BY userid
6 ORDER BY icount DESC
```

Run | Save query | Save view | Schedule

Query results | SAVE RESULTS | EXPLO

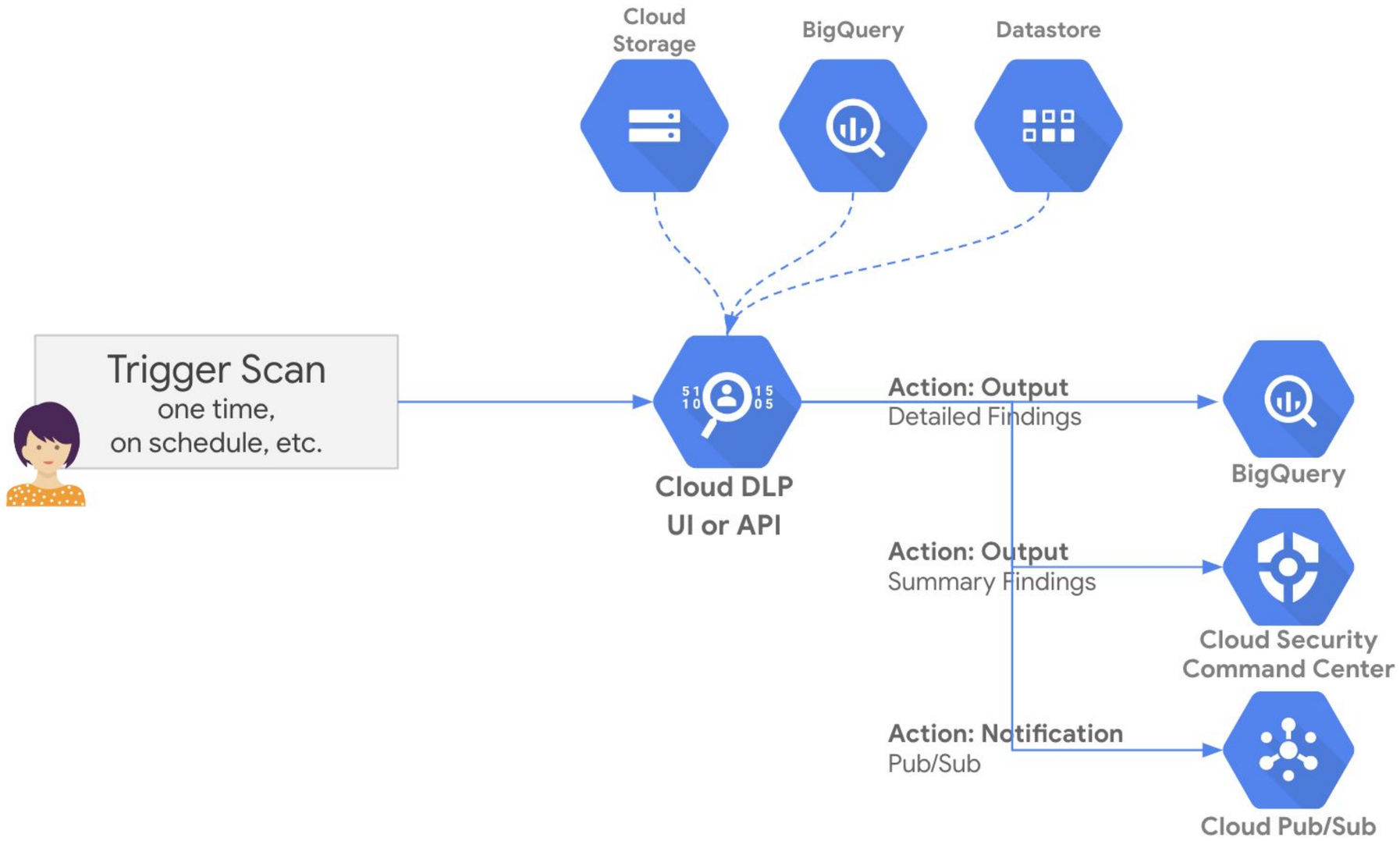
Query complete (1.4 sec elapsed, 16 KB processed)

Job information | Results | JSON | Execution details

Row	userid	icount
1	T1(32):AQW7f/9IEpEXIO7Eb3wEaEv7eZJHQA==	37
2	T1(32):AW3Rdxj4c8TmtFY6C7O7dDAOrMsAMg==	36
3	T1(32):AeB3rNiUQV9ZrpaKAaqcHWc1eRNx5Q==	4
4	T1(32):AWKK2qv/Sq7WBu2cfMUWZ3jNrwA1Iw==	4
5	T1(32):AWtHJzvZxid5n+l6C0jY42xWdHfXPQ==	4

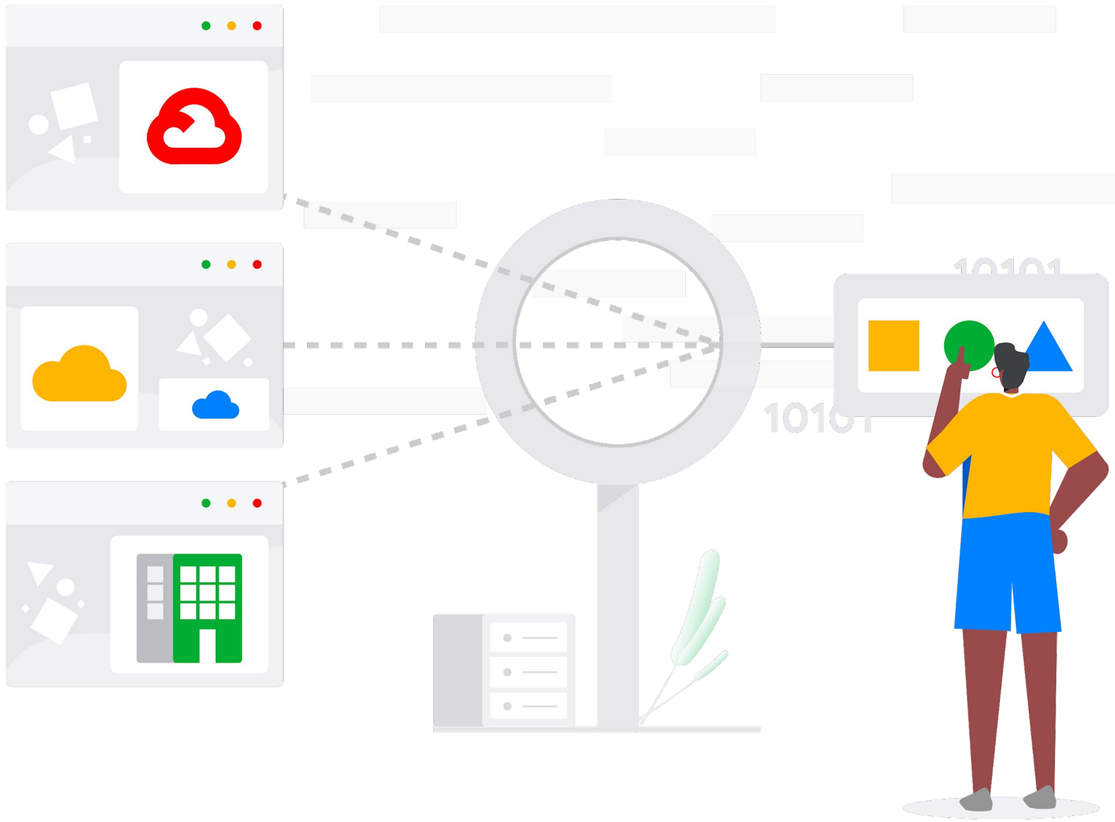
Tokens keep referential integrity

Implementing Cloud DLP



DLP Examples

- Use native inspection jobs to scan data at-rest in Cloud Storage, BigQuery, Datastore
- Use API “content” and “hybrid” methods to scan data at-rest on-prem, in other clouds, and in non-native storage systems (e.g. mysql running in a VM).
- Use API “content” and “hybrid” methods to scan data in motion via an Envoy filter/proxy or in custom applications



5.1 Diagnostic Question 02 Discussion

You are designing a web application for Cymbal Bank so that customers who have credit card issues can contact dedicated support agents. Customers may enter their complete credit card number when chatting with or emailing support agents. You want to ensure compliance with PCI-DSS and prevent support agents from viewing this information in the most cost-effective way.

What should you do?

A. Use customer-supplied encryption keys (CSEK) and Cloud Key Management Service (KMS) to detect and encrypt sensitive information.

B. Detect sensitive information with Cloud Natural Language API.

C. Use customer-managed encryption keys (CMEK) and Cloud Key Management Service (KMS) to detect and encrypt sensitive information.

D. Implement Cloud Data Loss Prevention using its REST API.

5.1 Diagnostic Question 02 Discussion

You are designing a web application for Cymbal Bank so that customers who have credit card issues can contact dedicated support agents. Customers may enter their complete credit card number when chatting with or emailing support agents. You want to ensure compliance with PCI-DSS and prevent support agents from viewing this information in the most cost-effective way.

What should you do?

A. Use customer-supplied encryption keys (CSEK) and Cloud Key Management Service (KMS) to detect and encrypt sensitive information.

B. Detect sensitive information with Cloud Natural Language API.

C. Use customer-managed encryption keys (CMEK) and Cloud Key Management Service (KMS) to detect and encrypt sensitive information.

D. Implement Cloud Data Loss Prevention using its REST API.

3.1 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.

3.1 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.

3.1 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.

3.1 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.

3.1 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.

3.1 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.

3.2 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.

3.2 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?

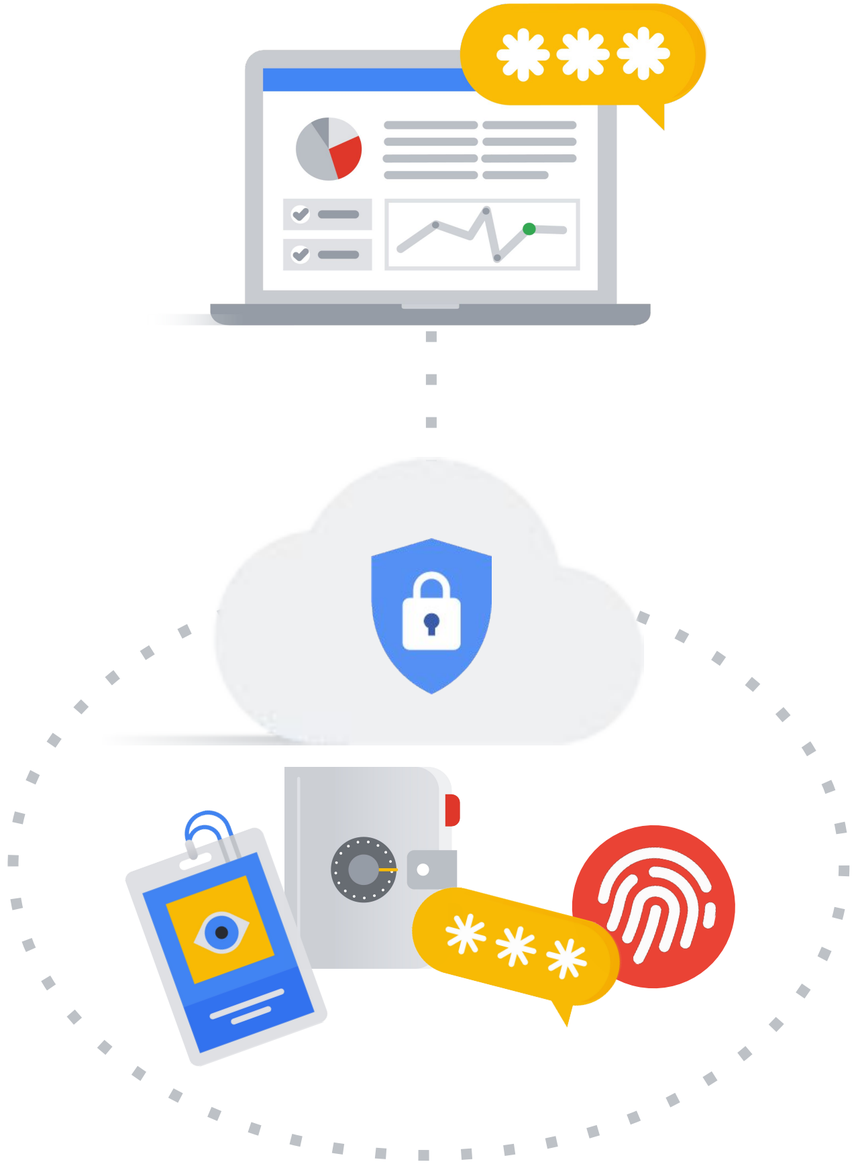
A. Import the spreadsheets to BigQuery, and create separate tables for Sales and Marketing. Set table expiry rules to 365 days for both tables. Create jobs scheduled to run every quarter for Marketing and every month for Sales.

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.

Secret Manager



Protect secret key-value data with Secret Manager

Exam Tip: *Secret Manager (or other specialized service like Hashicrop Vault) is a preferred method of storing secrets. You should NOT use source code repos / environment variables / config files for this purpose!*

When to use (or do not use) Secret Manager

Use Secret Manager to store...

- Credentials
- API tokens
- Base64 encoded private keys
- Certificates
- Other ASCII text secrets

Do not use Secret Manager to store...

- Dynamic secrets
- AES symmetric key
- Dynamic secrets and short-term credentials automatically generated
- Secrets that scale with O(users) like user login data
- SA keys

3.1 Diagnostic Question 05 Discussion

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.

3.1 Diagnostic Question 05 Discussion

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.

3.1 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.

3.1 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.

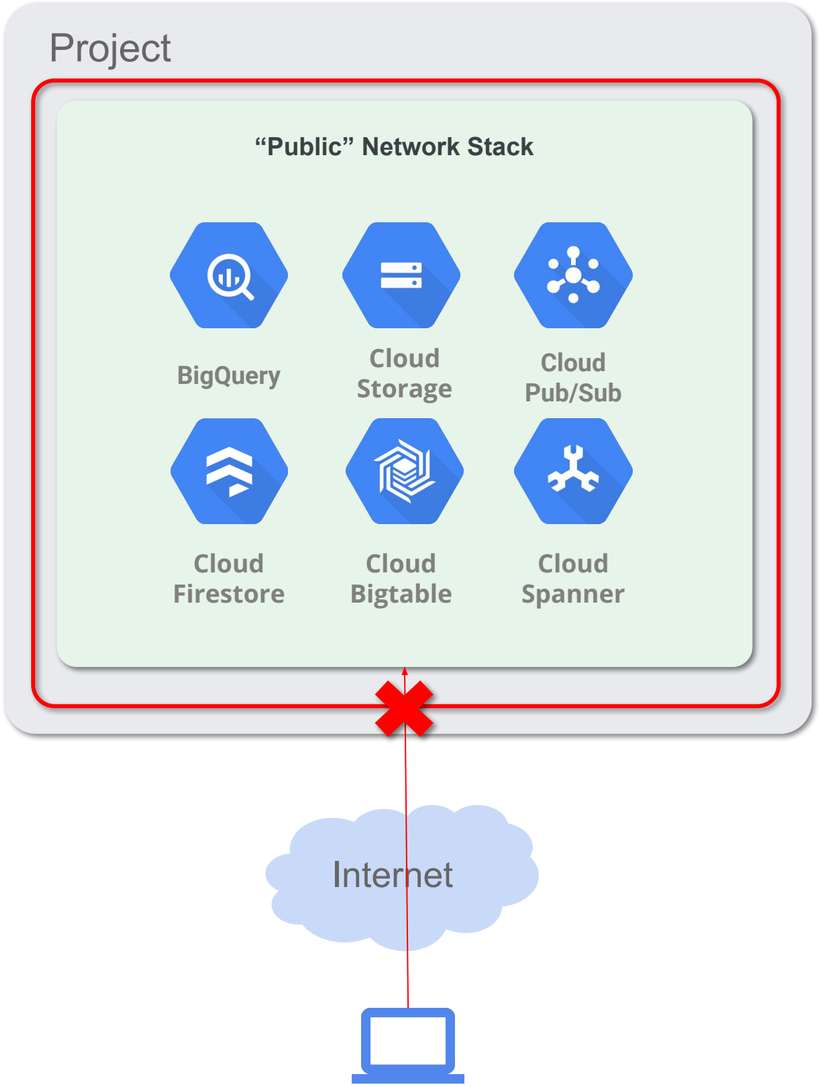
C. Use Project metadata to read the current machine's IP address and use a gcloud command to add access to Cloud SQL. Store Cloud SQL's connection string and username in Cloud Key Management Service, and store the password in Secret Manager.

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.

VPC Service Controls

Why is VPC Service Control needed?

- Key use-case: **Mitigate data exfiltration risks**
- Google Managed Services run on a **‘Public” network stack**, i.e. outside of your VPC network and its APIs are publically accessible.
- **Firewall rules cannot** be used to provide more granular access control to these services.
- VPC Service Controls provides **an additional layer of security defense** for Google Cloud services that is independent of Identity and Access Management (IAM).
- VPC Service Controls enables **broader context-based perimeter security**, including controlling data egress across the perimeter.



VPC Service Controls versus Firewall Policies

	Firewall Policies	VPC Service Control
Control path	VM ⟷ VM VM ⟷ Internet VM ⟷ On-premises	Google Cloud Service ⟷ VM Google Cloud Service ⟷ Internet Google Cloud Service ⟷ On-premise Google Cloud Service ⟷ Google Cloud Service
Conditions	5-tuple VM tags VM service accounts	VPC network Google Cloud project Service accounts Internet IPs
Policies apply to	VMs in a VPC network VMs grouped by tag VMs grouped by service account	API based resources grouped by project

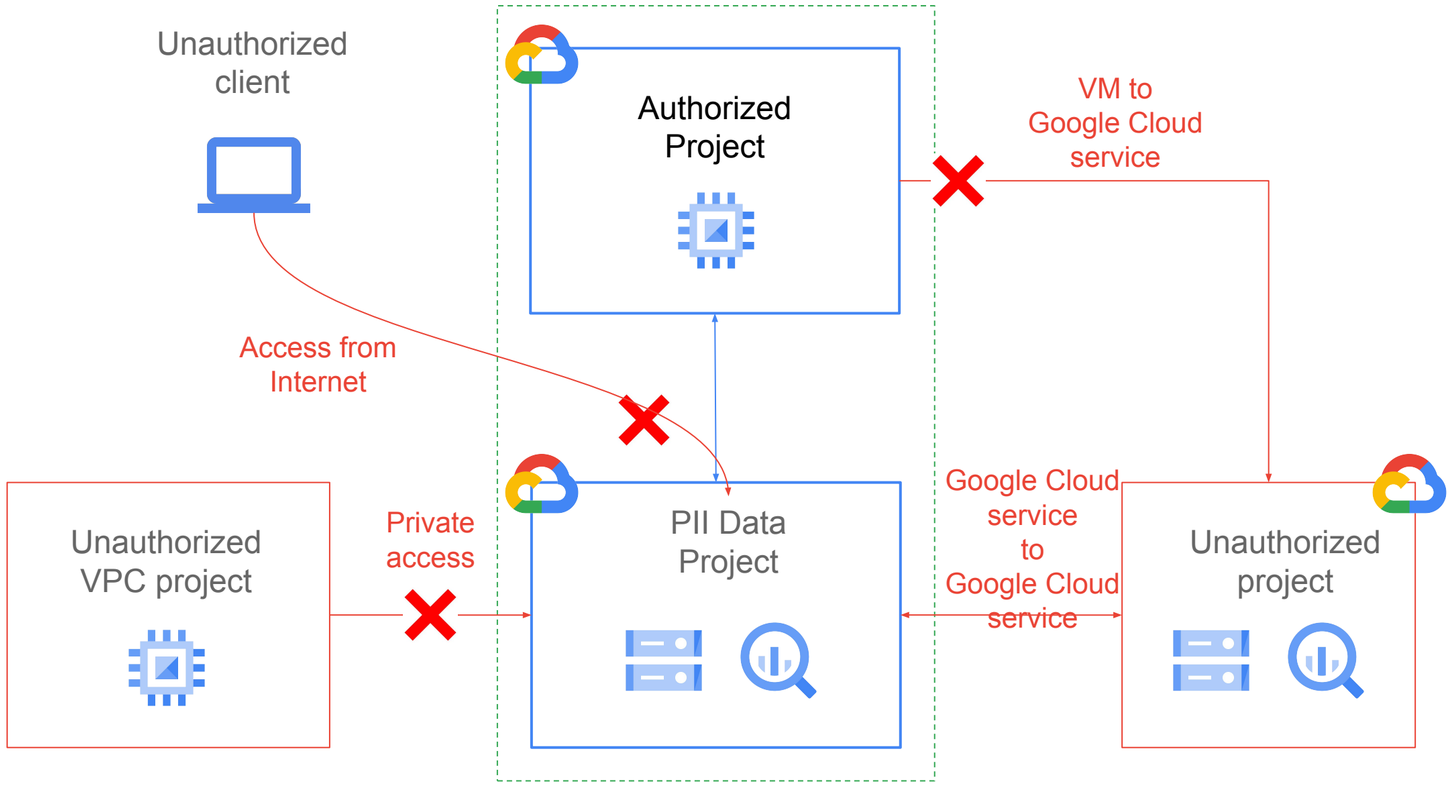
Protect against data exfiltration with

VPC Service Controls

Service perimeter

Extend perimeter security to managed Google Cloud services

- Control VM-to-service and service-to-service paths.
- Ingress: prevent access from the unauthorized networks.
- Egress: prevent copying of data to unauthorized Google Cloud Projects.
- Project-level granularity.

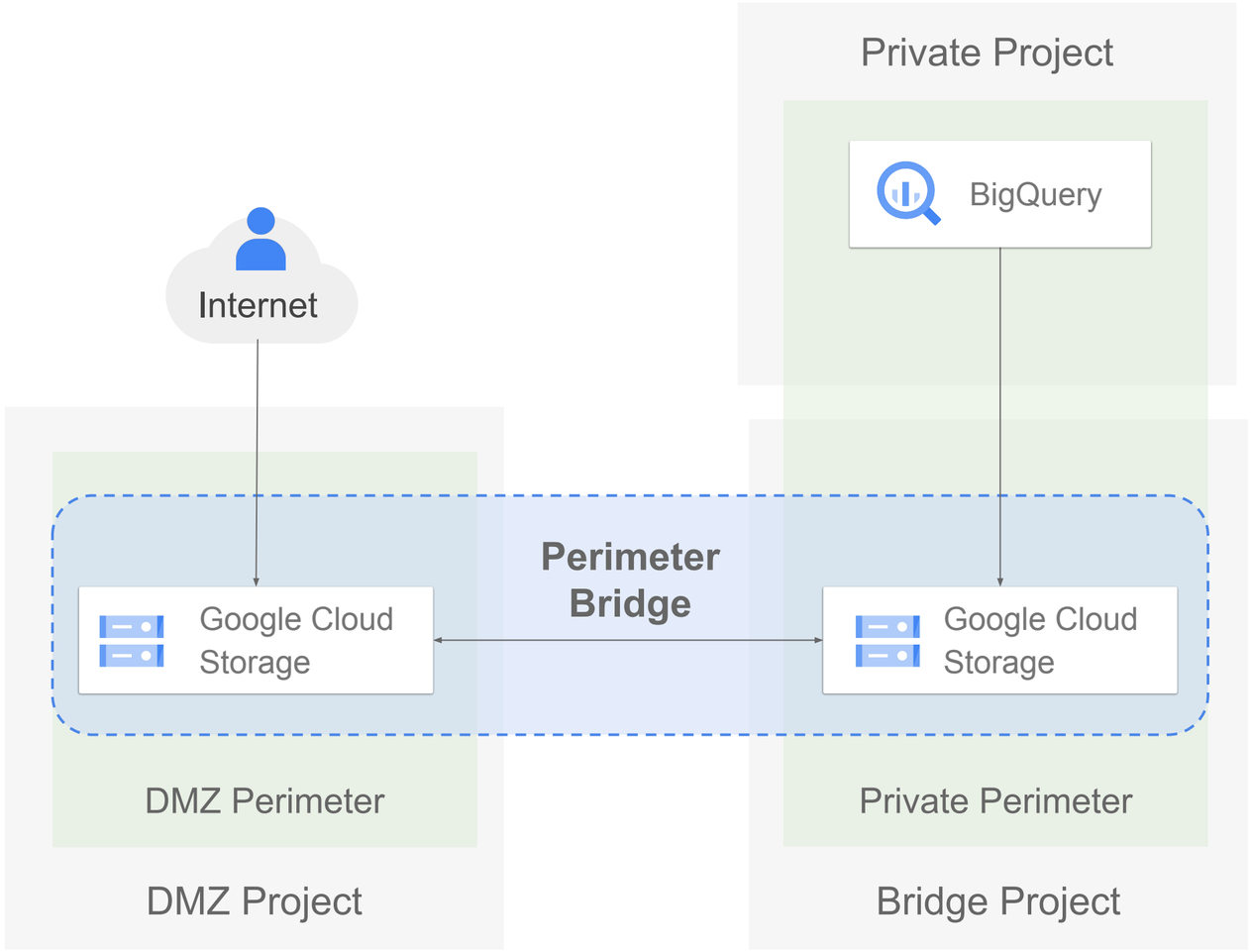


VPC Service Controls - Perimeter Bridge

Perimeter Bridge

Share data across Service Perimeters

- Allows communication between Google Cloud resources across Service Perimeters.
- A Google Cloud project can belong to only one Service Perimeter but can be a part of multiple Perimeter Bridges.
- Only the Service Perimeter determines the security policies for a Project.



2.5 Diagnostic Question 09 Discussion

Cymbal Bank requires that access to the Cloud Storage buckets in a project is restricted to ensure that the only way the buckets or objects within can be accessed is via users (who also have the necessary IAM role or ACL access to the bucket or object) first connecting to a VM running in a VPC in the project via SSH. You also want to ensure that users and service accounts are blocked from access to other Google Cloud APIs in the same project from VMs in the project VPCs, regardless of whether they have access via Identity and Access Management (IAM) roles.

Select the approach that can accomplish this with minimal configuration effort and complexity.

A. Create a VPC service controls service perimeter that includes the project and restricts access to Cloud Storage APIs, and enable VPC accessible services configuring Cloud Storage APIs as accessible.

B. Create a VPC service controls service perimeter that includes the project and restricts access to Cloud Storage APIs.

C. Create a VPC service controls service perimeter that includes an ingress rule for all users ingressFrom.identityType: ANY_USER_ACCOUNT; ingressFrom.sources.resource set to the project full path; ingressTo.operations.serviceName set to storage.googleapis.com; ingressTo.operations.methodSelectors.permission set to google.storage.buckets.get; and ingressTo.resources set to \"*\"

D. Update the IAM role bindings for all users with access to the buckets to add an IAM condition of the access level attribute type.

2.5 Diagnostic Question 09 Discussion

Cymbal Bank requires that access to the Cloud Storage buckets in a project is restricted to ensure that the only way the buckets or objects within can be accessed is via users (who also have the necessary IAM role or ACL access to the bucket or object) first connecting to a VM running in a VPC in the project via SSH. You also want to ensure that users and service accounts are blocked from access to other Google Cloud APIs in the same project from VMs in the project VPCs, regardless of whether they have access via Identity and Access Management (IAM) roles.

Select the approach that can accomplish this with minimal configuration effort and complexity.

A. **Create a VPC service controls service perimeter that includes the project and restricts access to Cloud Storage APIs, and enable VPC accessible services configuring Cloud Storage APIs as accessible.**

B. Create a VPC service controls service perimeter that includes the project and restricts access to Cloud Storage APIs.

C. Create a VPC service controls service perimeter that includes an ingress rule for all users ingressFrom.identityType: ANY_USER_ACCOUNT; ingressFrom.sources.resource set to the project full path; ingressTo.operations.serviceName set to storage.googleapis.com; ingressTo.operations.methodSelectors.permission set to google.storage.buckets.get; and ingressTo.resources set to \"*\"

D. Update the IAM role bindings for all users with access to the buckets to add an IAM condition of the access level attribute type.

2.5 Diagnostic Question 10 Discussion

Cymbal Bank has a set of VPC service control service perimeters around several projects with BigQuery datasets, and each project is in a separate service perimeter. You want to restrict access to these projects' BigQuery datasets to VMs in the VPCs of one of these projects (project P1,) and a small set of users should have external access from a combination of a specific IP range, geo-location, and device type.

Select the configuration that satisfies these requirements with minimal configuration.

A. Create a service perimeter bridge connecting the service perimeters of all the projects.

B. Create a service perimeter bridge connecting the service perimeters of all the projects, and update all the service perimeters to add an access level providing the external access for the specified users.

C. Update the service perimeter configurations for all the projects to add an ingress rule with an access level to provide the external access for the specified users.

D. Update the service perimeter configurations for all the projects to add an ingress rule to provide external access for the specified users and add another ingress rule to provide access from the VPCs of the specified project P1.

2.5 Diagnostic Question 10 Discussion

Cymbal Bank has a set of VPC service control service perimeters around several projects with BigQuery datasets, and each project is in a separate service perimeter. You want to restrict access to these projects' BigQuery datasets to VMs in the VPCs of one of these projects (project P1,) and a small set of users should have external access from a combination of a specific IP range, geo-location, and device type.

Select the configuration that satisfies these requirements with minimal configuration.

A. Create a service perimeter bridge connecting the service perimeters of all the projects.

B. Create a service perimeter bridge connecting the service perimeters of all the projects, and update all the service perimeters to add an access level providing the external access for the specified users.

C. Update the service perimeter configurations for all the projects to add an ingress rule with an access level to provide the external access for the specified users.

D. Update the service perimeter configurations for all the projects to add an ingress rule to provide external access for the specified users and add another ingress rule to provide access from the VPCs of the specified project P1.

3.1 Diagnostic Question 04 Discussion

Cymbal Bank has two vendors who need to collaborate on the same files and images, and each vendor is represented by Google Groups. Each vendor will perform different sets of transformations on these files. Cymbal Bank has provided a perimeter network with lower trust where Projects for the two vendors are also hosted along with a Project 'ForVendors,' which contains the files and images in Cloud Storage.

How would you configure access in the vendor Projects so that vendors can't communicate with each other, but can still copy the data from the bank's Cloud Storage bucket?

A. Use VPC Service Controls with Service perimeter bridges. Use the `gcloud access-context-manager perimeters` command and use project IDs of two vendors with –resources while the 'ForVendors' project is selected. Use Identity and Access Management (IAM) to provide appropriate permissions.

B. Use VPC Service Controls with Context-aware access with ingress rules. Use the command `gcloud access-context-manager perimeters update` and set ingress rules for the vendor projects. Use IAM to provide appropriate permissions.

C. Use VPC Service Controls with Service perimeter bridges. Use the command `gcloud access-context-manager perimeters` and use project IDs of each vendor and bank project with --resources separately. Use IAM to provide appropriate permissions.

D. Use VPC Service Controls with Context-aware access with ingress rules. Use the command `gcloud access-context-manager perimeters update` and set ingress rules for the bank's bucket in the vendor's Cloud Storage buckets separately. Use IAM to provide appropriate permissions.

3.1 Diagnostic Question 04 Discussion

Cymbal Bank has two vendors who need to collaborate on the same files and images, and each vendor is represented by Google Groups. Each vendor will perform different sets of transformations on these files. Cymbal Bank has provided a perimeter network with lower trust where Projects for the two vendors are also hosted along with a Project 'ForVendors,' which contains the files and images in Cloud Storage.

How would you configure access in the vendor Projects so that vendors can't communicate with each other, but can still copy the data from the bank's Cloud Storage bucket?

A. Use VPC Service Controls with Service perimeter bridges. Use the `gcloud access-context-manager perimeters` command and use project IDs of two vendors with –resources while the 'ForVendors' project is selected. Use Identity and Access Management (IAM) to provide appropriate permissions.

B. Use VPC Service Controls with Context-aware access with ingress rules. Use the command `gcloud access-context-manager perimeters update` and set ingress rules for the vendor projects. Use IAM to provide appropriate permissions.

C. Use VPC Service Controls with Service perimeter bridges. Use the command `gcloud access-context-manager perimeters` and use project IDs of each vendor and bank project with --resources separately. Use IAM to provide appropriate permissions.

D. Use VPC Service Controls with Context-aware access with ingress rules. Use the command `gcloud access-context-manager perimeters update` and set ingress rules for the bank's bucket in the vendor's Cloud Storage buckets separately. Use IAM to provide appropriate permissions.

DNSSEC

DNSSEC (DNS Security)

- Prevents DNS poisoning/spoofing through strong **authentication/**establishing trust relationship between domain registrar and server providing the DNS service (DNS host)
- **Enable:** first enable in Cloud DNS, then add DS record in registrar
- **Disable:** disable in registrar (remove DS record). Once the record cache is expired, disable it in Cloud DNS
- **TTL:** avoid TTL for DS longer than 259200 seconds (3 days)
- Know how to “Migrate or transfer DNSSEC-enabled zones”

2.2 Diagnostic Question 04 Discussion

Cymbal Bank has two engineering teams (T1 and T2) working on two different Projects (P1 and P2). Both P1 and P2 use custom VPCs. T2 needs to request and verify DNS records for T1's domain that are internal to P1's Compute Engine Instance. After the records are verified, T2 will access and look up more records in this Compute Engine Instance.

How would you enable the lookup access to ensure that the requests are always authenticated and are protected against exfiltration?

A. Create a forwarding zone with P1 and P2's VPCs in the VPC network list. Add P2's IP addresses in the private forwarding targets list. Then enable DNSSEC with `gcloud dns managed-zones update zone-name -dnssec-state` on.

B. Create a peering zone. Set P1 as producer network and P2 as consumer network. Then enable DNSSEC with `gcloud dns managed-zones update zone-name -dnssec-state` on.

C. Create a managed reverse lookup private zone with P1 and P2's VPCs in the VPC network list. Keep visibility as private. Add the required domain names in dns-names while creating the managed zone.

D. Create a cross-project binding zone by creating a private zone with the URL of P2's VPC network. Then enable DNSSEC with `gcloud dns managed-zones update zone-name -dnssec-state` on.

2.2 Diagnostic Question 04 Discussion

Cymbal Bank has two engineering teams (T1 and T2) working on two different Projects (P1 and P2). Both P1 and P2 use custom VPCs. T2 needs to request and verify DNS records for T1's domain that are internal to P1's Compute Engine Instance. After the records are verified, T2 will access and look up more records in this Compute Engine Instance.

How would you enable the lookup access to ensure that the requests are always authenticated and are protected against exfiltration?

A. Create a forwarding zone with P1 and P2's VPCs in the VPC network list. Add P2's IP addresses in the private forwarding targets list. Then enable DNSSEC with `gcloud dns managed-zones update zone-name -dnssec-state` on.

B. Create a peering zone. Set P1 as producer network and P2 as consumer network. Then enable DNSSEC with `gcloud dns managed-zones update zone-name -dnssec-state` on.

C. Create a managed reverse lookup private zone with P1 and P2's VPCs in the VPC network list. Keep visibility as private. Add the required domain names in dns-names while creating the managed zone.

D. Create a cross-project binding zone by creating a private zone with the URL of P2's VPC network. Then enable DNSSEC with `gcloud dns managed-zones update zone-name -dnssec-state` on.

Kubernetes Engine Security Best Practices - Part 1

Container-Optimized OS

Default for Kubernetes Engine

Minimal footprint

- Based on Chromium OS
- Optimized for Kubernetes Engine and Compute Engine
- Unnecessary packages removed

OS security features:

- Locked-down firewall
- Read-only filesystem where possible
- Limited user access
- Disabled root login

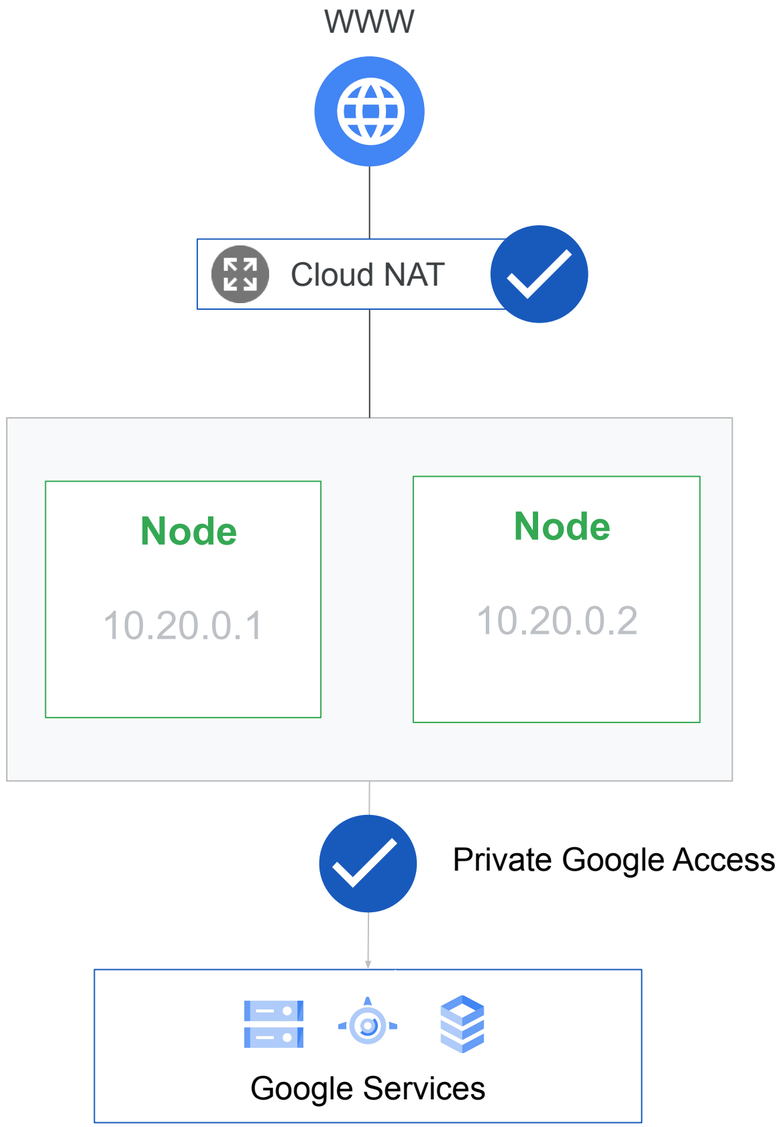
Hardened kernel with security features:

- Opt-in to auto-upgrade OS on nodes during maintenance window
- Integrity Measurement Architecture (IMA)
- Audit, Kernel Page Table Isolation (KPTI)
- Linux Security Modules (LSMs) from Chromium OS

Private clusters

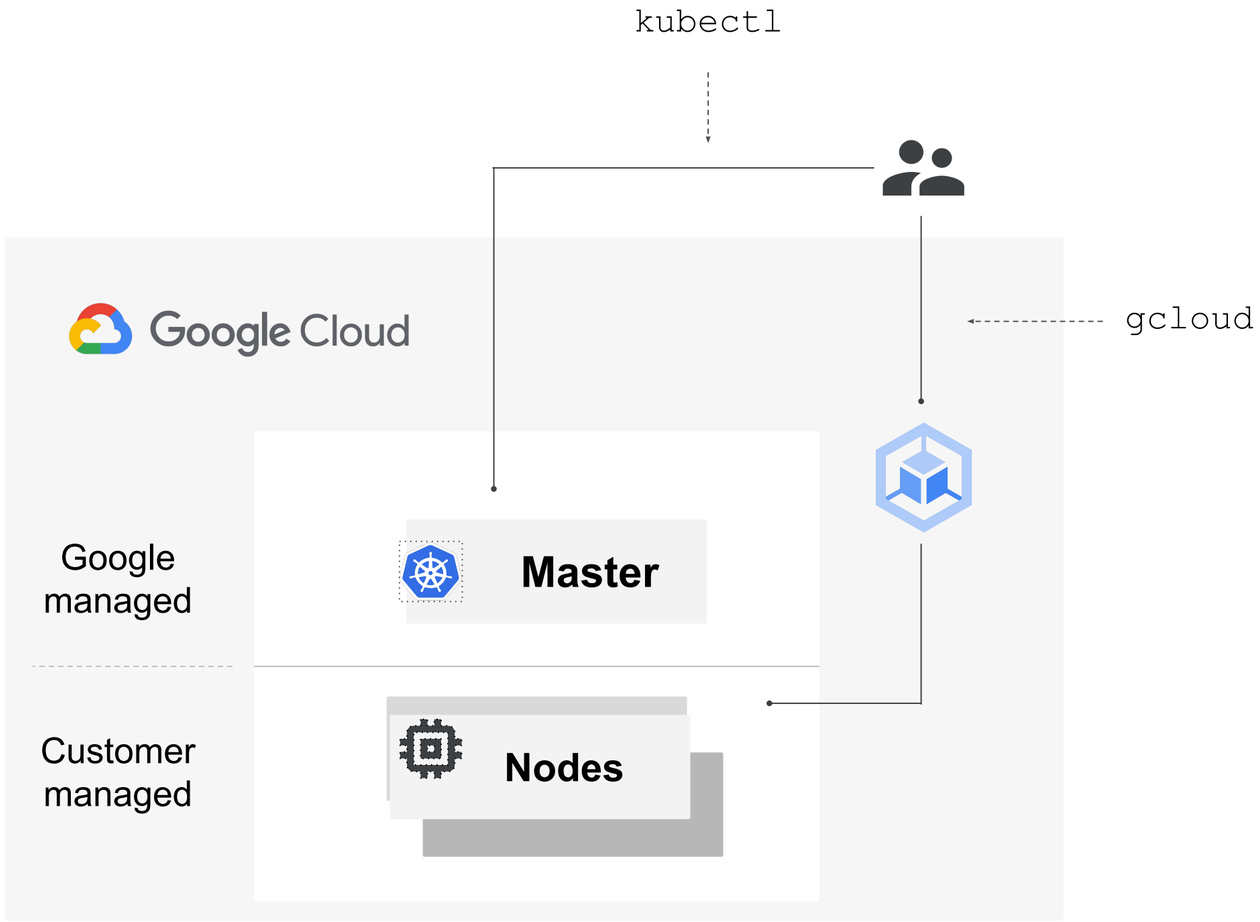
Private clusters isolate nodes from having inbound and outbound connectivity to the public internet

- Nodes have only private IP addresses
- Nodes use Private Google Access to communicate with Google APIs
- Nodes can use Cloud NAT to reach the internet
- Control Plane gets an additional private endpoint for the cluster nodes to talk to the control plane.



Automatic control plane and node upgrade

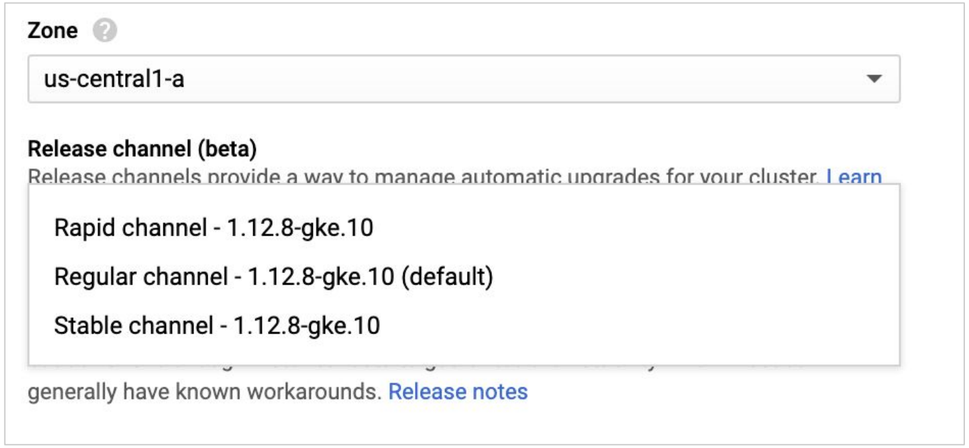
- GKE is **a managed service** and we keep the cluster control plane up-to-date and secure
- Cluster control planes are **always upgraded** on a regular basis, regardless of whether the cluster is enrolled in a release channel or not
  - Automatic upgrades can be controlled by defining maintenance windows and exclusions
  - Manual upgrades/downgrades possible
- Control plane is not 100% accessible during upgrades unless the cluster is *regional*
  - Regional masters are upgraded by rolling update and the uptime SLO is 99.95%



Auto Upgrade and Risk Tolerance Profiles for Enterprise Customers

Release Channels: Chrome-like, automated updates. Choose a release cadence and feature set to match risk preference.

```
gcloud alpha container clusters create [CLUSTER_NAME] --release-channel rapid
```

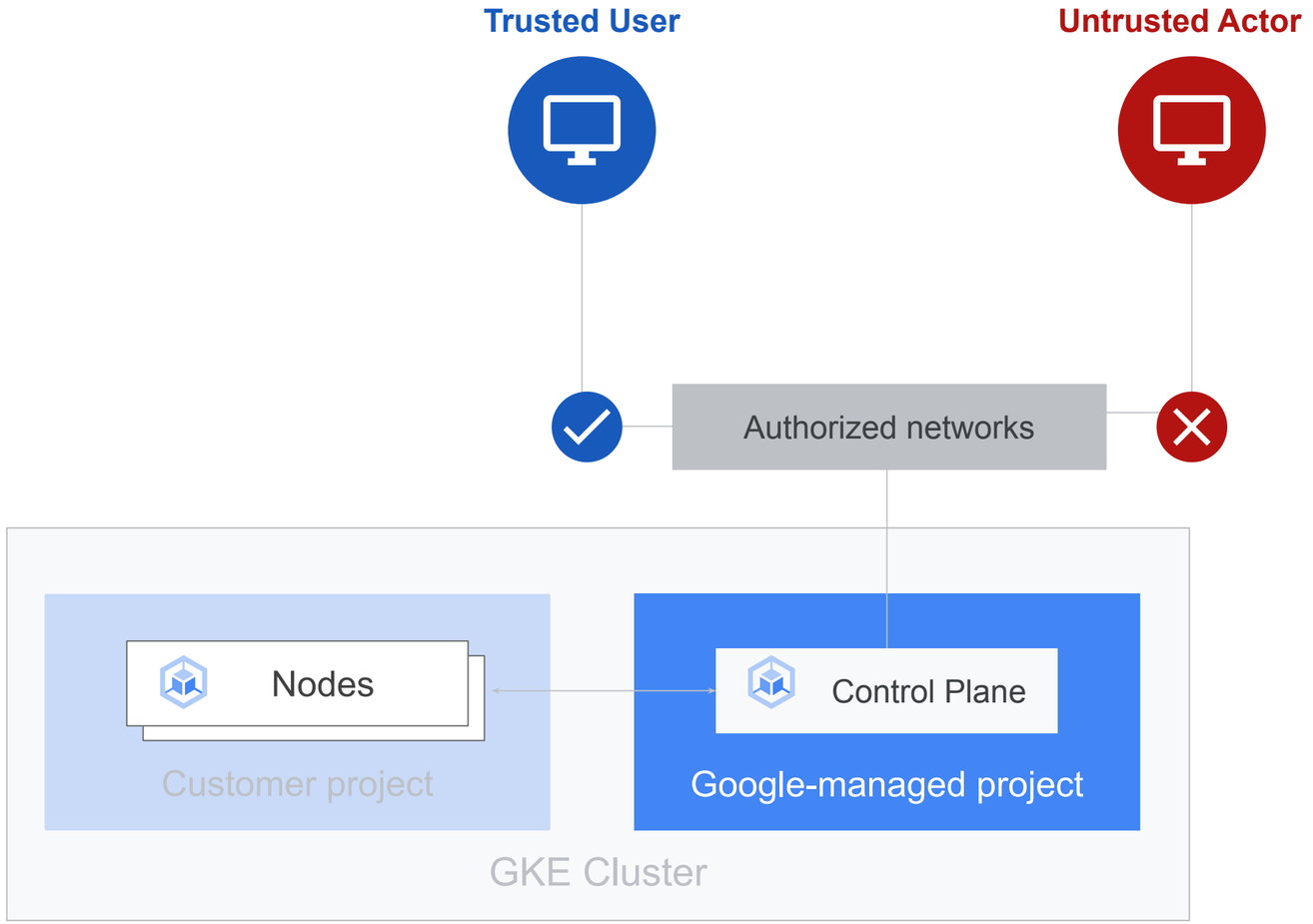


https://cloud.google.com/kubernetes-engine/docs/how-to/node-auto-upgrades

https://cloud.google.com/kubernetes-engine/docs/concepts/release-channels

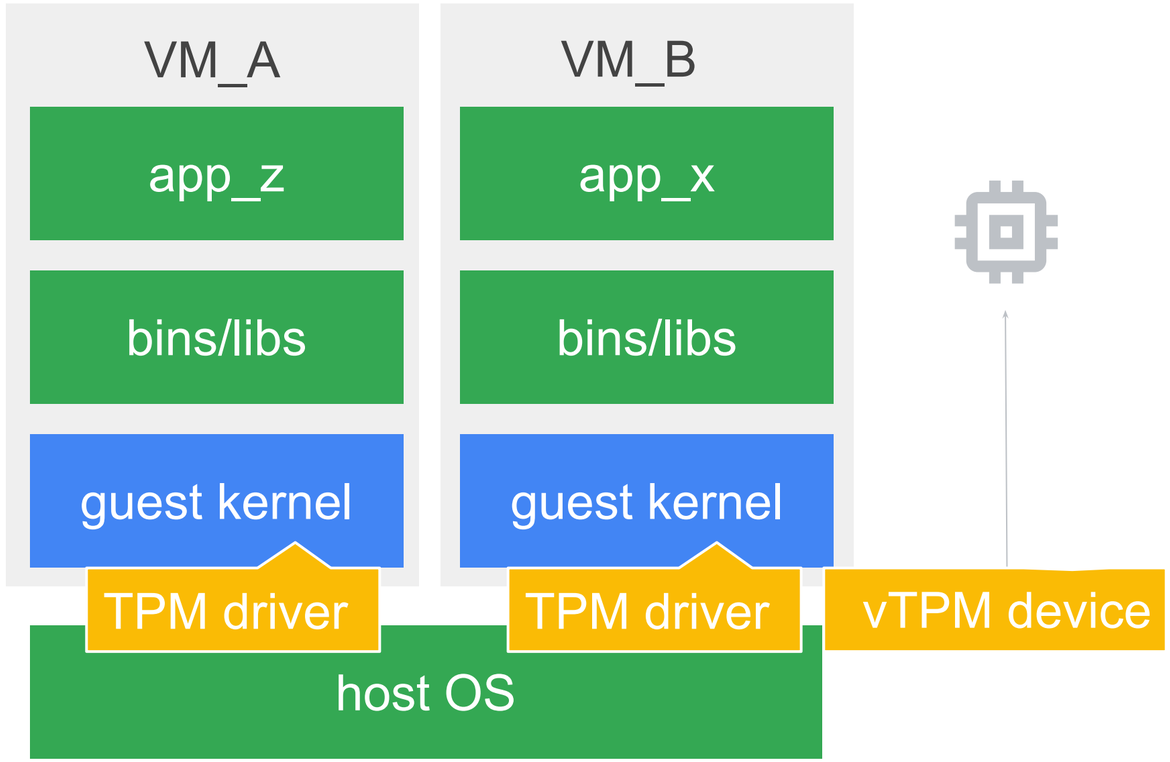
Authorized networks

- Authorized networks restrict access to the control plane to trusted CIDR ranges. Mandatory for private clusters.
- By default nodes and pods ranges are allowed.
- Google recommends activating it for all clusters.
- Control plane access via public IP can be disabled (recommended). This is called Private endpoint.



Shielded Nodes

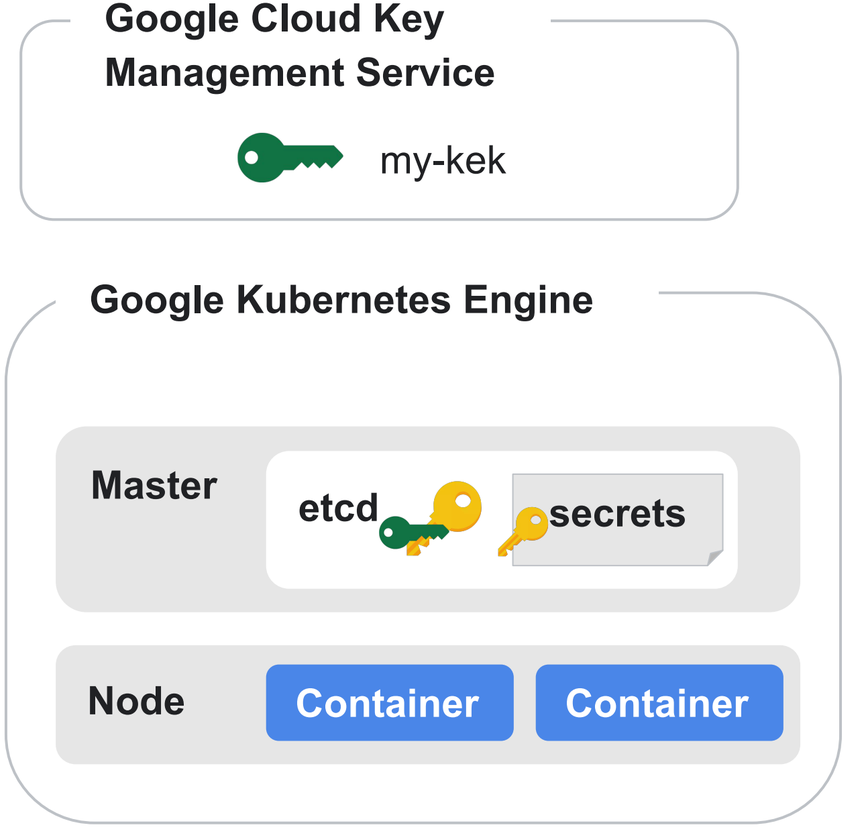
- Built on top of **Compute Engine Shielded VMs**
- Now on by default
- Limits the ability of an attacker to impersonate a node in your cluster
- Verifies:
  - Node is a virtual machine running in Google's data center
  - Node is part of the Managed Instance Group (MIG) provisioned for the cluster
  - The kubelet is being provisioned a certificate for the node on which it is running.



GKE Secret management

Enable Application Layer Encryption for sensitive data

- Application-layer Secrets Encryption provides an additional layer of security for sensitive data, such as Secrets, stored in etcd.
- Data in etcd, such as secrets, are encrypted locally with a data encryption key (DEK)
- The data encryption key is also stored in etcd, but encrypted with a key encryption key (KEK) in Cloud KMS, via a KMS plugin



Use Secret Manager or third-party tool like Vault to store and manage your GKE Secrets

IAM: Use default roles as a starting point

These roles are available by default for Kubernetes Engine users.

Kubernetes Engine Admin	Full permissions to manage container clusters **and Kubernetes API objects.**
Kubernetes Engine **Cluster** Admin	Full permissions to manage container clusters, **but not Kubernetes API objects.**
Kubernetes Engine **Cluster** Viewer	Read-only access to view and list clusters
Kubernetes Engine Developer	Full permissions to manage Kubernetes API objects, **but not the container clusters.**
Kubernetes Engine Viewer	Provides read-only access to Kubernetes API objects.

What can I do with RBAC?

IAM is great. However, RBAC at the cluster level allows for much more granular authorization control.

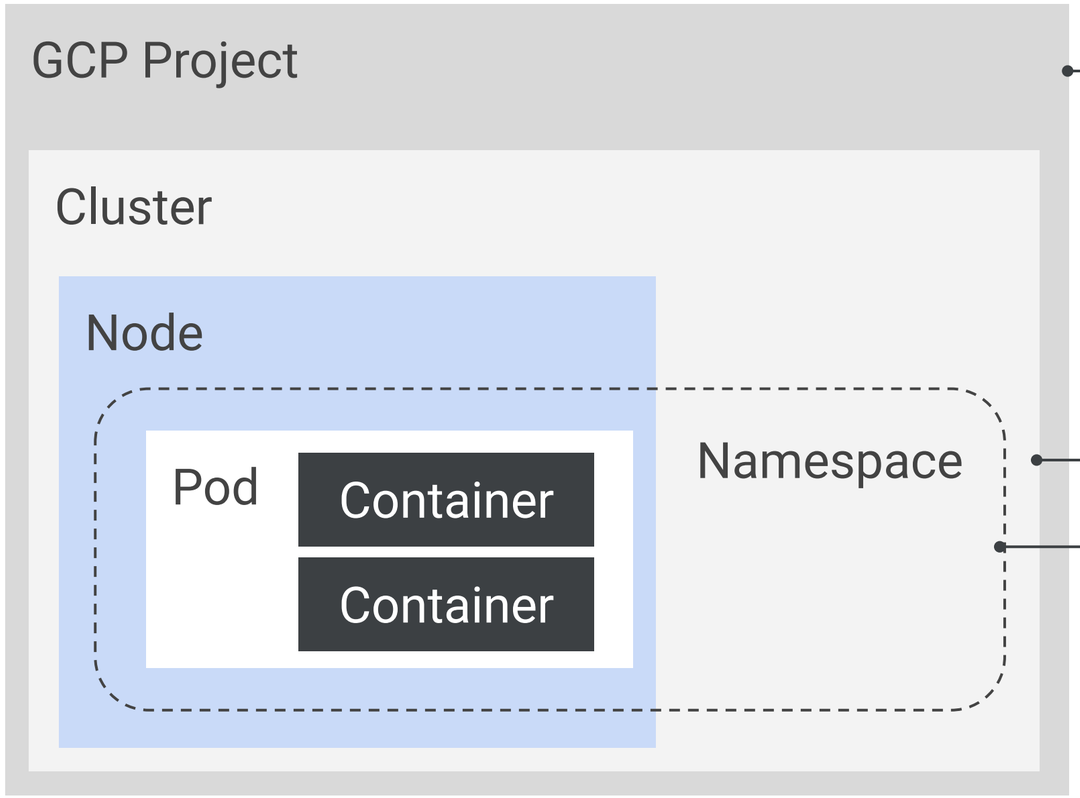
Secure your cluster by granting privileged operations (accessing secrets, for example) only to admin users.

Enforce user-based authentication and authorization **by the cluster**.

Limit resource creation (such as pods, persistent volumes, deployments) to specific namespaces.

Have users and pods only see resources in their authorized namespace. This allows you to isolate resources within your organization (for example, between development teams).

GKE: Using IAM and RBAC



Use IAM at the project level
Set roles for

- Cluster Admin: manage clusters
- Container Developer: API access within clusters

Use RBAC at the cluster and namespace level
Set permissions on individual clusters and namespaces

Additional content

QUIZ week 3

(the one we went through during the meeting)

Reminder:

- NOT as complex as questions on the exam
- Technical knowledge validation (No business context)

Additional content 1

[READING]

- Overview of VPC Service Controls
- Cloud DLP: Classification, redaction, and de-identification
- DLP: Transformation methods
- DLP: Format-preserving encryption
- DLP: what are infoTypes and infoType detectors?
- How to secure DLP resources using VCP-SC (Service Controls)
- BigQuery: Authorized Views
- Data encryption options
- Envelope encryption
- Customer-Supplied Encryption Keys - CSEK
- Customer-managed encryption keys - CMEK
- Key rotation
- Cloud Key Management Service deep dive - lengthy, but important
- Best practices to securely authenticate applications in Google Cloud
- Application auth methods - have a look at different options
- GCS Object Lifecycle Management
- GCS Retention policies and retention policy locks
- Confidential Computing overview

Additional content 2

- What is Confidential Computing: https://cloud.google.com/blog/products/identity-security/confidential-computing-data-encryption-during-processing
- DLP: https://cloud.google.com/blog/products/identity-security/google-cloud-dlp-can-modify-data-to-protect-it
- Three pseudonymization methods available in Cloud DLP
- BigQuery encryption
- BigQuery - CMEK
- What is VM Metadata?
- Cloud External Key Manager and hosted private HSM
- Overview of Secret Manager, best practices and secret rotation.
- How to use and lock GCS Retention Policies
- KMS Key versions
- [Cloud DLP] Hybrid scenarios
- [Recommended] Secret Manager best practices

[VIDEOS]

- Cloud DLP: inspection of PII data and de-identification: De-identification and inspection templates with Cloud DLP

Additional content 3

- Pseudo-anonymization technique and other interesting capabilities of DLP: How to use tokenization with Cloud DLP
- [Cloud DLP] Managing sensitive data in hybrid environments
- Great intro into Secret Manager: Manage your Cloud Run secrets securely with Secret Manager
- Securing GCP Projects with VPC Service Controls: VPC-SC explained in 3 minutes.
- Preventing Data Exfiltration on GCP (Cloud Next '19): structured approach to misconfigured policies, leaked credentials, broad privileges, malicious insiders, compromised code etc.
  a. Great intro to VPC-SC
  b. VERY USEFUL VIDEO!!!! 42 mins, but SO useful!

[PODCASTS]

- Confidentially Speaking
- Confidentially Speaking 2: Cloudful of Secrets
- Data Security in the Cloud

[DEEP DIVES]

- Secrets in serverless - 2.0 (comparison of KMS vs Secret Manager for storing secrets).
- Encryption at rest in GCP.
- Encryption in transit in GCP.

Make sure to…

Enjoy the journey as much as the destination!