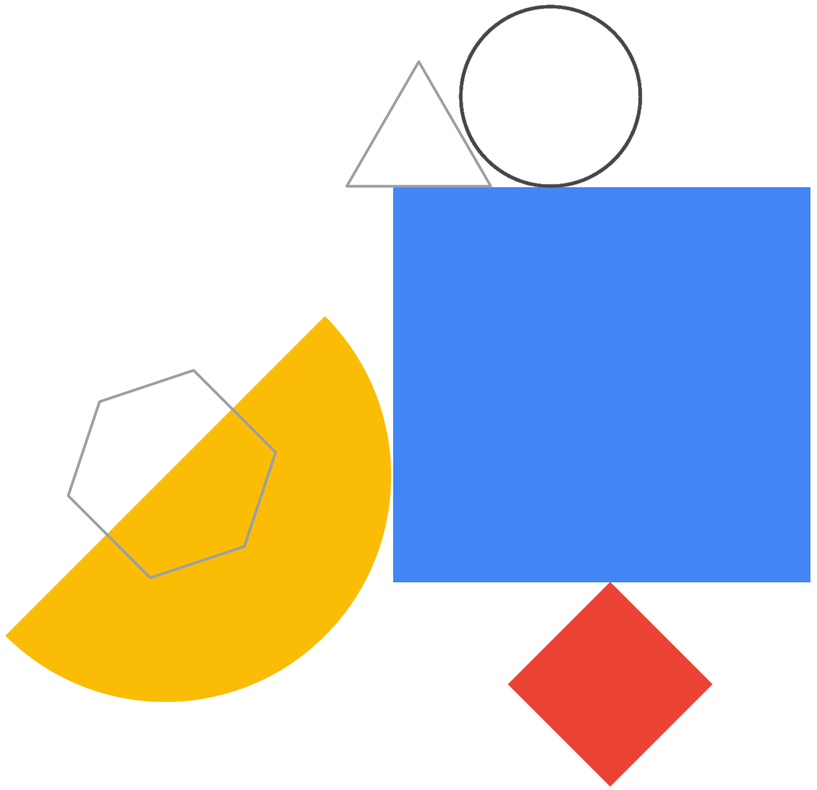
Google Cloud

Preparing for Your Professional Cloud Security Engineer Journey

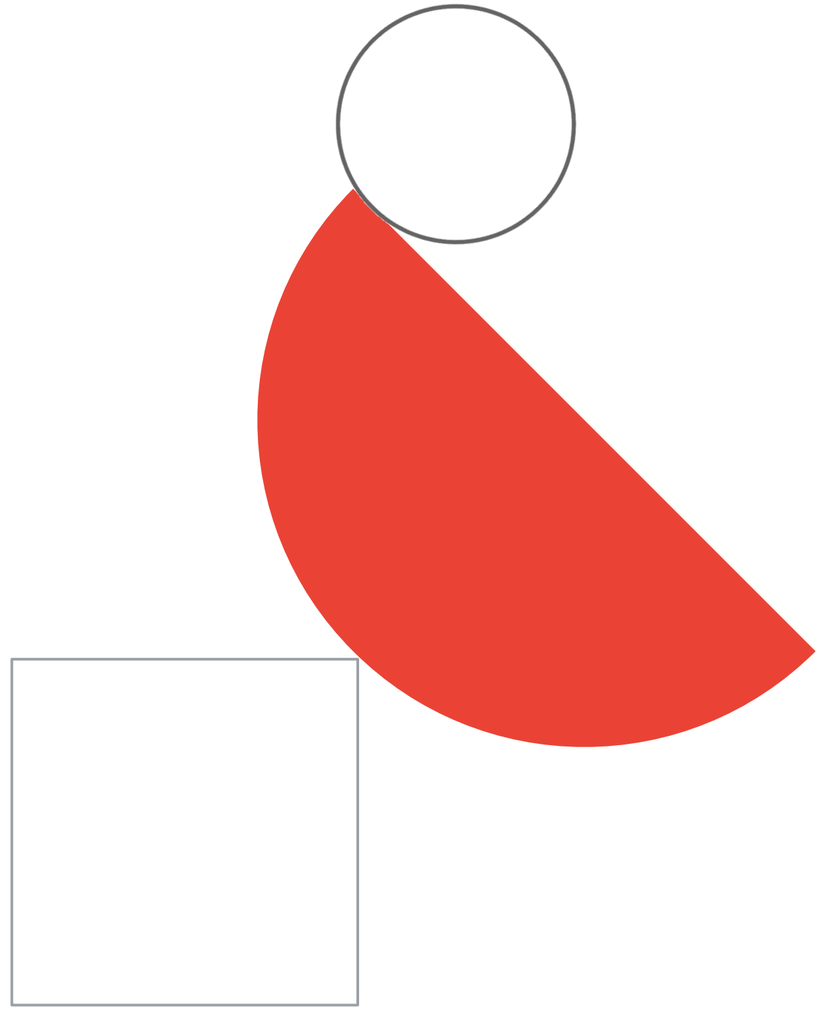


Course Workbook

Certification Exam Guide Sections

1	Configuring access within a cloud solution environment
2	Configuring network security
3	Ensuring data protection
4	Managing operations in a cloud solution environment
5	Ensuring compliance

Section 1:
Configuring access within a cloud solution environment



1.1 Diagnostic Question 01

Cymbal Bank has acquired a non-banking financial company (NBFC). This NBFC uses Active Directory as their central directory on an on-premises Windows Server. You have been tasked with migrating all the NBFC users and employee information to Cloud Identity.

What should you do?

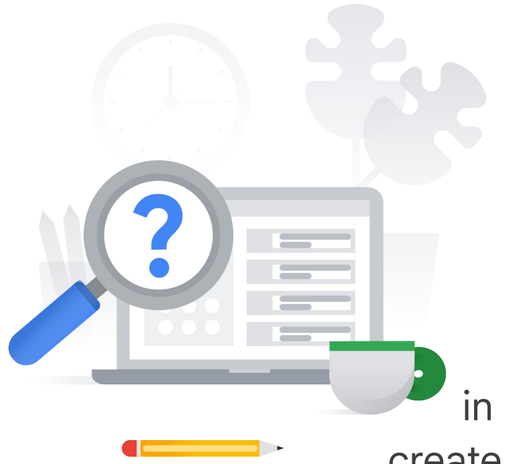
A. Run Microsoft System Center Configuration Manager (SCCM) on a Compute Engine instance. Leave the channel unencrypted because you are in a secure Google Cloud environment. Deploy Google Cloud Directory Sync on the Compute Engine instance. Connect to the on-premises Windows Server environment from the instance, and migrate users to Cloud Identity.

B. Run Configuration Manager on a Compute Engine instance. Copy the resulting configuration file from this machine onto a new Compute Engine instance to keep the production environment separate from the staging environment. Leave the channel unencrypted because you are in a secure Google Cloud environment. Deploy Google Cloud Directory Sync on this new instance. Connect to the on-premises Windows Server environment from the new instance, and migrate users to Cloud Identity.

C. Use Cloud VPN to connect the on-premises network to your Google Cloud environment. Select an on-premises domain-joined Windows Server. On the domain-joined Windows Server, run Configuration Manager and Google Cloud Directory Sync. Use Cloud VPN's encrypted channel to transfer users from the on-premises Active Directory to Cloud Identity.

D. Select an on-premises domain-joined Windows Server. Run Configuration Manager on the domain-joined Windows Server, and copy the resulting configuration file to a Compute Engine instance. Run Google Cloud Directory Sync on the Compute Engine instance over the internet, and use Cloud VPN to sync users from the on-premises Active Directory to Cloud Identity.

1.1 Diagnostic Question 02



Cymbal Bank has certain default permissions and access for their analyst, finance, and teller teams. These teams are organized into groups that have a set of role-based IAM permissions assigned to them. After a recent acquisition of a small bank, you find that the small bank directly assigns permissions to their employees in IAM. You have been tasked with applying Cymbal Bank's organizational structure to the small bank. Employees will need access to Google Cloud services.

What should you do?

A. Leave all user permissions as-is in the small bank's IAM. Use the Directory API in the Google Workspace Admin SDK to create Google Groups. Use a Python script to allocate users to the Google Groups.

B. Reset all user permissions in the small bank's IAM. Use Cloud Identity to create dynamic groups for each of the bank's teams. Use the dynamic groups' metadata field for team type to allocate users to their appropriate group with a Python script.

C. Reset all user permissions in the small bank's IAM. Use Cloud Identity to create the required Google Groups. Upgrade the Google Groups to Security Groups. Use a Python script to allocate users to the groups.

D. Reset all user permissions in the small bank's IAM. Use the Directory API in the Google Workspace Admin SDK to create Google Groups. Use a Python script to allocate users to the groups.

1.1 Configuring Cloud Identity

Courses

[Security in Google Cloud](#)
- M2 Cloud Identity

[Managing Security in Google Cloud](#)
- M2 Cloud Identity

Documentation

[Active Directory user account provisioning | Identity and access management | Google Cloud](#)

[What is Configuration Manager? - Google Workspace Admin Help](#)

[Manage membership automatically with dynamic groups - Google Workspace Admin Help](#)

[Creating and updating a dynamic group | Cloud Identity](#)

[Create and manage groups using APIs - Google Workspace Admin Help](#)

1.2 Diagnostic Question 03

Cymbal Bank leverages Google Cloud storage services, an on-premises Apache Spark Cluster, and a web application hosted on a third-party cloud. The Spark cluster and web application require limited access to Cloud Storage buckets and a Cloud SQL instance for only a few hours per day. You have been tasked with sharing credentials while minimizing the risk that the credentials will be compromised.

What should you do?

A. Create a service account with appropriate permissions. Authenticate the Spark Cluster and the web application as direct requests and share the service account key.

B. Create a service account with appropriate permissions. Have the Spark Cluster and the web application authenticate as delegated requests, and share the short-lived service account credential as a JWT.

C. Create a service account with appropriate permissions. Authenticate the Spark Cluster and the web application as a delegated request, and share the service account key.

D. Create a service account with appropriate permissions. Have the Spark Cluster and the web application authenticate as a direct request, and share the short-lived service account credentials as XML tokens.

1.2 Diagnostic Question 04

Cymbal Bank recently discovered service account key misuse in one of the teams during a security audit. As a precaution, going forward you do not want any team in your organization to generate new external service account keys. You also want to restrict every new service account's usage to its associated Project.

What should you do?

A. Navigate to Organizational policies in the Google Cloud Console. Select your organization. Select `iam.disableServiceAccountKeyCreation`. Customize the **applied to** property, and set **Enforcement** to 'On'. Click Save. Repeat the process for `iam.disableCrossProjectServiceAccountUsage`.

B. Run the `gcloud resource-manager org-policies enable-enforce` command with the constraints iam.disableServiceAccountKeyCreation, and `iam.disableCrossProjectServiceAccountUsage` and the Project IDs you want the constraints to apply to.

C. Navigate to Organizational policies in the Google Cloud Console. Select your organization. Select `iam.disableServiceAccountKeyCreation`. Under Policy Enforcement, select **Merge with parent**. Click **Save**. Repeat the process for `iam.disableCrossProjectServiceAccountLienRemoval`.

D. Run the `gcloud resource-manager org-policies` allow command with the boolean `constraints iam.disableServiceAccountKeyCreation` and `iam.disableCrossProjectServiceAccountUsage` with Organization ID.

1.2 Managing service accounts

Courses

Security in Google Cloud
- M3 Identity and Access Management (IAM)
- M5 Securing Compute Engine: Techniques and Best Practices
- M8 Securing Kubernetes: Techniques and Best Practices

Managing Security in Google Cloud
- M3 Identity and Access Management (IAM)

Security Best Practices in Google Cloud
- M1 Securing Compute Engine: Techniques and Best Practices
- M4 Securing Kubernetes: Techniques and Best Practices

Skill Badges

Google Cloud

Ensure Access and Identity in Google Cloud Quest

Documentation

Creating short-lived service account credentials | Cloud IAM Documentation

Restricting service account usage | Resource Manager Documentation | Google Cloud

1.3 Diagnostic Question 05

Cymbal Bank publishes its APIs through Apigee. Cymbal Bank has recently acquired ABC Corp, which uses a third-party identity provider. You have been tasked with connecting ABC Corp's identity provider to Apigee for single sign-on (SSO). You need to set up SSO so that Google is the service provider. You also want to monitor and log high-risk activities.

Which two choices would you select to enable SSO?

A. Use openssl to generate public and private keys. Store the public key in an X.509 certificate, and encrypt using RSA or DSA for SAML. Sign in to the Google Admin console, and under **Security**, upload the certificate.

B. Use openssl to generate a private key. Store the private key in an X.509 certificate, and encrypt using AES or DES for SAML. Sign in to the Google Workspace Admin Console and upload the certificate.

C. Use openssl to generate public and private keys. Store the private key in an X.509 certificate, and encrypt using AES or DES for SAML. Sign in to the Google Admin console, and under Security, upload the certificate.

D. Review Network mapping results, and assign SSO profiles to required users.

E. Review Network mapping results, and assign SAML profiles to required users.

1.3 Diagnostic Question 06

Cymbal Bank's Mobile Development Team has an AI Platform instance in a Google Cloud Project. An auditor needs to record the AI Platform jobs and models, along with their usage. You need to assign permissions to the external auditors so that they can view the models and jobs but not retrieve specific details on any of them.

What should you do?

A. Create a custom role for auditors at the Organization level. Create a JSON file with required permissions ml.models.list and ml.jobs.list. Use `gIAM roles create role-id -- organization organization-id --file=json-file-path.`

B. Create a custom role for auditors at the Project level. Create a YAML file with required permissions `ml.models.list` and `ml.jobs.list`. Use `gIAM roles create role-id --project project-id --file=yaml-file-path.`

C. Create a custom role for auditors at the Project level. `Use gIAM roles create role-name --project project-id --permissions= ml.models.get, ml.jobs.get.`

D. Create a custom role for auditors at the Organization level. Create a JSON file with required permissions `ml.models.list` and `ml.jobs.list`. Use `gIAM role create role-id --organization organization-id --file=json-file-path.`

1.3 Managing authentication

Courses

[Security in Google Cloud](#)
- M2 Cloud Identity
- M3 Identity and Access Management (IAM)

[Managing Security in Google Cloud](#)
- M2 Cloud Identity
- M3 Identity and Access Management (IAM)

Skill Badges

Google Cloud

[Ensure Access and Identity in Google Cloud Quest](#)

Documentation

[SAML overview | Apigee X | Google Cloud](#)

[Set up single sign-on for managed Google Accounts using third-party Identity providers - Google Workspace Admin Help](#)

[Assign SSO profile to organizational units or groups - Google Workspace Admin Help](#)

[Network Mapping results - Google Workspace Admin Help](#)

[Creating and managing custom roles | Cloud IAM Documentation](#)

[Understanding IAM custom roles | Cloud IAM Documentation | Google Cloud](#)

[Understanding roles | Cloud IAM Documentation](#)

1.4 Diagnostic Question 07

Cymbal Bank's organizational hierarchy divides the Organization into departments. The Engineering Department has a 'product team' folder. This folder contains folders for each of the bank's products. Each product folder contains one Google Cloud Project, but more may be added. Each project contains an App Engine deployment.

Cymbal Bank has hired a new technical product manager and a new web developer. The technical product manager must be able to interact with and manage all services in projects that roll up to the Engineering Department folder. The web developer needs read-only access to App Engine configurations and settings for a specific product.

How should you provision the new employees' roles into your hierarchy following principles of least privilege?

A. Assign the Project Editor role in each individual project to the technical product manager. Assign the Project Editor role in each individual project to the web developer.

B. Assign the Project Owner role in each individual project to the technical product manager. Assign the App Engine Deployer role in each individual project to the web developer.

C. Assign the Project Editor role at the Engineering Department folder level to the technical product manager. Assign the App Engine Deployer role at the specific product's folder level to the web developer.

D. Assign the Project Editor role at the Engineering Department folder level to the technical product manager. Create a Custom Role in the product folder that the web developer needs access to. Add the appengine.versions.create and appengine.versions.delete permissions to that role, and assign it to the web developer.

1.4 Diagnostic Question 08

Cymbal Bank's organizational hierarchy divides the Organization into departments. The Engineering Department has a 'product team' folder. This folder contains folders for each of the bank's products. One folder titled "analytics" contains a Google Cloud Project that contains an App Engine deployment and a Cloud SQL instance.

A team needs specific access to this project. The team lead needs full administrative access to App Engine and Cloud SQL. A developer must be able to configure and manage all aspects of App Engine deployments. There is also a code reviewer who may periodically review the deployed App Engine source code without making any changes.

What types of permissions would you provide to each of these users?

A. Create custom roles for all three user types at the "analytics" folder level. For the team lead, provide all appengine.* and cloudsql.* permissions. For the developer, provide appengine.applications.* and appengine.instances.* permissions. For the code reviewer, provide the appengine.instances.* permissions.

B. Assign the basic 'App Engine Admin' and 'Cloud SQL Admin" roles to the team lead. Assign the 'App Engine Admin' role to the developer. Assign the 'App Engine Code Viewer' role to the code reviewer. Assign all these permissions at the analytics project level.

C. Create custom roles for all three user types at the project level. For the team lead, provide all appengine.* and cloudsql.* permissions. For the developer, provide appengine.applications.* and appengine.instances.* permissions. For the code reviewer, provide the appengine.instances.* permissions.

D. Assign the basic 'Editor' role to the team lead. Create a custom role for the developer. Provide all appengine.* permissions to the developer. Provide the predefined 'App Engine Code Viewer' role to the code reviewer. Assign all these permissions at the "analytics" folder level.

1.4 Managing and implementing authorization controls

Courses

[Security in Google Cloud](#)
- M3 Identity and Access Management (IAM)

[Managing Security in Google Cloud](#)
- M3 Identity and Access Management (IAM)

Skill Badges

Google Cloud

[Ensure Access and Identity in Google Cloud Quest](#)

Documentation

[Access control for projects with IAM | Resource Manager Documentation | Google Cloud](#)

[Access control for organizations with IAM | Resource Manager Documentation | Google Cloud](#)

[Access control for folders with IAM | Resource Manager Documentation | Google Cloud](#)

[Understanding roles | Cloud IAM Documentation](#)

[Understanding roles | Cloud IAM Documentation](#)

1.5 Diagnostic Question 09

Cymbal Bank is divided into separate departments. Each department is divided into teams. Each team works on a distinct product that requires Google Cloud resources for development.

How would you design a Google Cloud organization hierarchy to best match Cymbal Bank's organization structure and needs?

A. Create an Organization node. Under the Organization node, create Department folders. Under each Department, create Product folders. Under each Product, create Teams folders. In the Teams folder, add Projects.

B. Create an Organization node. Under the Organization node, create Department folders. Under each Department, create Product folders. Add Projects to the Product folders.

C. Create an Organization node. Under the Organization node, create Department folders. Under each Department, create Teams folders. Add Projects to the Teams folders.

D. Create an Organization node. Under the Organization node, create Department folders. Under each Department, create a Teams folder. Under each Team, create Product folders. Add Projects to the Product folders.

1.5 Diagnostic Question 10

Cymbal Bank has a team of developers and administrators working on different sets of Google Cloud resources. The Bank's administrators should be able to access the serial ports on Compute Engine Instances and create service accounts. Developers should only be able to access serial ports.

How would you design the organization hierarchy to provide the required access?

A. Deny Serial Port Access and Service Account Creation at the Organization level. Create an 'admin' folder and set enforced: false for constraints/compute.disableSerialPortAccess. Create a new 'dev' folder inside the 'admin' folder, and set enforced: false for constraints/iam.disableServiceAccountCreation. Add developers to the 'dev' folder, and add administrators to the 'admin' folder.

B. Deny Serial Port Access and Service Account Creation at the organization level. Create a 'dev' folder and set enforced: false for constraints/compute.disableSerialPortAccess. Create a new 'admin' folder inside the 'dev' folder, and set enforced: false for constraints/iam.disableServiceAccountCreation. Add developers to the 'dev' folder, and add administrators to the 'admin' folder.

C. Deny Serial Port Access and Service Account Creation at the organization level. Create a 'dev' folder and set enforced: true for constraints/compute.disableSerialPortAccess and enforced: true for constraints/iam.disableServiceAccountCreation. Create a new 'admin' folder inside the 'dev' folder, and set enforced: false for constraints/iam.disableServiceAccountCreation. Add developers to the 'dev' folder, and add administrators to the 'admin' folder.

D. Allow Serial Port Access and Service Account Creation at the organization level. Create a 'dev' folder and set enforced: true for constraints/iam.disableServiceAccountCreation. Create another 'admin' folder that inherits from the parent inside the organization node. Add developers to the 'dev' folder, and add administrators to the 'admin' folder.

1.5 Defining resource hierarchy

Courses

[Security in Google Cloud]
- M2 Cloud Identity
- M3 Identity and Access Management (IAM)

[Managing Security in Google Cloud]
- M2 Cloud Identity
- M3 Identity and Access Management (IAM)

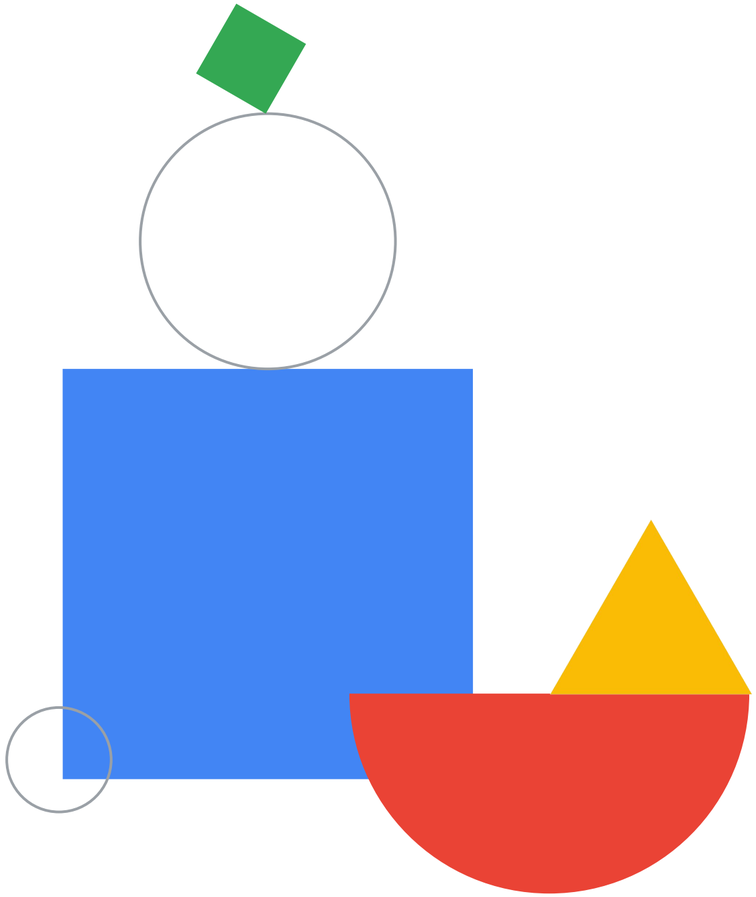
Documentation

[Understanding hierarchy evaluation | Resource Manager Documentation | Google Cloud]

[Creating and managing organizations | Resource Manager Documentation | Google Cloud]

[Best practices for enterprise organizations | Documentation | Google Cloud]

Google Cloud



Section 2: Configuring network security

2.1 Diagnostic Question 01

Cymbal Bank has published an API that internal teams will use through the HTTPS load balancer. You need to limit the API usage to 200 calls every hour. Any exceeding usage should inform the users that servers are busy.

Which gcloud command would you run to throttle the load balancing for the given specification?

A. gcloud compute security-policies rules create priority
--security-policy sec-policy
--src-ip-ranges=source-range
--action=throttle
--rate-limit-threshold-count=200
--rate-limit-threshold-interval-sec=3600
--conform-action=allow
--exceed-action=deny-429
--enforce-on-key=HTTP-HEADER

B. gcloud compute security-policies rules create priority
--security-policy sec-policy
--src-ip-ranges=source-range
--action=throttle
--rate-limit-threshold-count=200
--rate-limit-threshold-interval-sec=60
--conform-action=deny
--exceed-action=deny-404
--enforce-on-key=HTTP-HEADER

C. gcloud compute security-policies rules create priority
--security-policy sec-policy
--src-ip-ranges=source-range
--action=rate-based-ban
--rate-limit-threshold-count=200
--rate-limit-threshold-interval-sec=3600
--conform-action=deny
--exceed-action=deny-403
--enforce-on-key=HTTP-HEADER

D. gcloud compute security-policies rules create priority
--security-policy sec-policy
--src-ip-ranges="<source range>"
--action=rate-based-ban
--rate-limit-threshold-count=200
--rate-limit-threshold-interval-sec=3600
--conform-action=allow
--exceed-action=deny-500
--enforce-on-key=IP

2.1 Diagnostic Question 02

Cymbal Bank is releasing a new loan management application using a Compute Engine managed instance group. External users will connect to the application using a domain name or IP address protected with TLS 1.2. A load balancer already hosts this application and preserves the source IP address. You are tasked with setting up the SSL certificate for this load balancer.

What should you do?

A. Create a Google-managed SSL certificate. Attach a global dynamic external IP address to the internal HTTPS load balancer. Validate that an existing URL map will route the incoming service to your managed instance group backend. Load your certificate and create an HTTPS proxy routing to your URL map. Create a global forwarding rule that routes incoming requests to the proxy.

B. Create a Google-managed SSL certificate. Attach a global static external IP address to the external HTTPS load balancer. Validate that an existing URL map will route the incoming service to your managed instance group backend. Load your certificate and create an HTTPS proxy routing to your URL map. Create a global forwarding rule that routes incoming requests to the proxy.

C. Import a self-managed SSL certificate. Attach a global static external IP address to the TCP Proxy load balancer. Validate that an existing URL map will route the incoming service to your managed instance group backend. Load your certificate and create a TCP proxy routing to your URL map. Create a global forwarding rule that routes incoming requests to the proxy.

D. Import a self-managed SSL certificate. Attach a global static external IP address to the SSL Proxy load balancer. Validate that an existing URL map will route the incoming service to your managed instance group backend. Load your certificate and create an SSL proxy routing to your URL map. Create a global forwarding rule that routes incoming requests to the proxy.

2.1 Diagnostic Question 03

Your organization has a website running on Compute Engine. This instance only has a private IP address. You need to provide SSH access to an on-premises developer who will debug the website from the authorized on-premises location only.

How do you enable this?

A. Set up Cloud VPN. Set up an unencrypted tunnel to one of the hosts in the network. Create outbound or egress firewall rules. Use the private IP address to log in using a gcloud ssh command.

B. Use SOCKS proxy over SSH. Set up an SSH tunnel to one of the hosts in the network. Create the SOCKS proxy on the client side.

C. Use the default VPC's firewall. Open port 22 for TCP protocol using the Google Cloud Console.

D. Use Identity-Aware Proxy (IAP). Set up IAP TCP forwarding by creating ingress firewall rules on port 22 for TCP using the gcloud command.

2.1 Designing network security

Courses

Networking in Google Cloud

- M2 Controlling Access to VPC Networks
- M4 Load balancing

Security in Google Cloud

- M4 Configuring VPC for Isolation and Security
- M7 Application Security: Techniques and Best Practices
- M9 Protecting Against DDoS Attacks

Networking in Google Cloud: Defining and implementing networks

- M2 Controlling Access to VPC Networks
- M4 Load balancing

Managing Security in Google Cloud

- M4 Configuring VPC for Isolation and Security

Security Best Practices in Google Cloud

- M3 Application Security: Techniques and Best Practices

Mitigating Security Vulnerabilities in Google Cloud

- M1 Protecting Against DDoS Attacks

Skill Badges

Google Cloud

Build and Secure Networks in Google Cloud Quest

Google Cloud

Ensure Access and Identity in Google Cloud Quest

Documentation

gcloud compute security-policies rules update | Cloud SDK Documentation

gcloud compute security-policies | Cloud SDK Documentation

Setting up an global external HTTP(S) load balancer (classic) with a Compute Engine backend | Load Balancing | Google Cloud

Using Google-managed SSL certificates | Load Balancing

Using IAP for TCP forwarding | Identity-Aware Proxy | Google Cloud

Securely connecting to VM instances | Compute Engine Documentation | Google Cloud

2.2 Diagnostic Question 04

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 05

Cymbal Bank needs to connect its employee MongoDB database to a new human resources web application on the same network. Both the database and the application are autoscaled with the help of Instance templates. As the Security Administrator and Project Editor, you have been tasked with allowing the application to read port 27017 on the database.

What should you do?

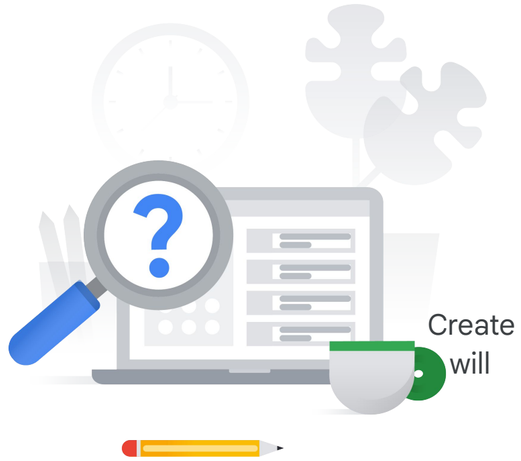
A. Create service accounts for the application and database. Create a firewall rule using:
gcloud compute firewall-rules create ALLOW_MONGO_DB
--network network-name
--allow TCP:27017
--source-service-accounts web-application-service-account
--target-service-accounts database-service-account

B. Create service accounts for the application and database. Create a firewall rule using:
gcloud compute firewall-rules create ALLOW_MONGO_DB
--network network-name
--allow ICMP:27017
--source-service-accounts web-application-service-account
--target-service-accounts database-service-account

C. Create a user account for the database admin and a service account for the application. Create a firewall rule using:
gcloud compute firewall-rules create ALLOW_MONGO_DB
--network network-name
--allow TCP:27017
--source-service-accounts web-application-service-account
--target-service-accounts database-admin-user-account

D. Create user accounts for the application and database. Create a firewall rule using:
gcloud compute firewall-rules create ALLOW_MONGO_DB
--network network-name
--deny UDP:27017
--source-service-accounts web-application-user-account
--target-service-accounts database-admin-user-account

2.2 Diagnostic Question 06



Cymbal Bank has designed an application to detect credit card fraud that will analyze sensitive information. The application that's running on a Compute Engine instance is hosted in a new subnet on an existing VPC. Multiple teams who have access to other VMs in the same VPC must access the VM. You want to configure the access so that unauthorized VMs or users from the internet can't access the fraud detection VM.

What should you do?

A. Use subnet isolation. Create a service account for the fraud detection VM. Create one service account for all the teams' Compute Engine instances that will access the fraud detection VM. Create a new firewall rule using:
gcloud compute firewall-rules create ACCESS_FRAUD_ENGINE
--network <network name>
--allow TCP:80
--source-service-accounts <one service account for all teams>
--target-service-accounts <fraud detection engine's service account>

B. Use target filtering. Create two tags called 'app' and 'data'. Assign the 'app' tag to the Compute Engine instance hosting the Fraud Detection App (source), and assign the 'data' tag to the other Compute Engine instances (target). Create a firewall rule to allow all ingress communication on this tag.

C. Use subnet isolation. Create a service account for the fraud detection engine. Create service accounts for each of the teams' Compute Engine instances that will access the engine. Add a firewall rule using:
gcloud compute firewall-rules create ACCESS_FRAUD_ENGINE
--network <network name>
--allow TCP:80
--source-service-accounts <list of service accounts>
--target-service-accounts <fraud detection engine's service account>

D. Use target filtering. Create a tag called 'app', and assign the tag to both the source and the target. Create a firewall rule to allow all ingress communication on this tag.

2.2 Configuring network segmentation

Courses

Networking in Google Cloud

- M2 Controlling Access to VPC Networks

Security in Google Cloud

- M4 Configuring VPC for Isolation and Security

Networking in Google Cloud: Defining and implementing networks

- M2 Controlling Access to VPC Networks

Managing Security in Google Cloud

- M4 Configuring VPC for Isolation and Security

Skill Badges

Google Cloud

Build and Secure Networks in Google Cloud Quest

Documentation

DNS zones overview | Google Cloud

Using firewall rules | VPC | Google Cloud

Best practices and reference architectures for VPC design

Best practices and reference architectures for VPC design

Best practices for securing service accounts | Cloud IAM Documentation

2.3 Diagnostic Question 07

The data from Cymbal Bank's loan applicants resides in a shared VPC. A credit analysis team uses a CRM tool hosted in the App Engine standard environment. You need to provide credit analysts with access to this data. You want the charges to be incurred by the credit analysis team.

What should you do?

A. Add egress firewall rules to allow TCP and UDP ports for the App Engine standard environment in the Shared VPC network. Create either a client-side connector in the Service Project or a server-side connector in the Host Project using the IP Range or Project ID of the target VPC. Verify that the connector is in a READY state. Create an egress rule on the Shared VPC network to allow the connector using Network Tags or IP ranges.

B. Add egress firewall rules to allow SSH and/or RDP ports for the App Engine standard environment in the Shared VPC network. Create a client-side connector in the Service Project using the IP range of the target VPC. Verify that the connector is in a READY state. Create an egress rule on the Shared VPC network to allow the connector using Network Tags or IP ranges.

C. Add ingress firewall rules to allow NAT and Health Check ranges for the App Engine standard environment in the Shared VPC network. Create a client-side connector in the Service Project using the Shared VPC Project ID. Verify that the connector is in a READY state. Create an ingress rule on the Shared VPC network to allow the connector using Network Tags or IP ranges.

D. Add ingress firewall rules to allow NAT and Health Check ranges for App Engine standard environment in the Shared VPC network. Create a server-side connector in the Host Project using the Shared VPC Project ID. Verify that the connector is in a READY state. Create an ingress rule on the Shared VPC network to allow the connector using Network Tags or IP ranges.

2.3 Diagnostic Question 08

Cymbal Bank's Customer Details API runs on a Compute Engine instance with only an internal IP address. Cymbal Bank's new branch is co-located outside the Google Cloud points-of-presence (PoPs) and requires a low-latency way for its on-premises apps to consume the API without exposing the requests to the public internet.

Which solution would you recommend?

A. Use a Content Delivery Network (CDN). Establish direct peering with one of Google's nearby edge-enabled PoPs.

B. Use Carrier Peering. Use a service provider to access their enterprise grade infrastructure to connect to the Google Cloud environment.

C. Use Partner Interconnect. Use a service provider to access their enterprise grade infrastructure to connect to the Google Cloud environment.

D. Use Dedicated Interconnect. Establish direct peering with one of Google's nearby edge-enabled PoPs.

2.3 Diagnostic Question 9

An external audit agency needs to perform a one-time review of Cymbal Bank's Google Cloud usage. The auditors should be able to access a Default VPC containing BigQuery, Cloud Storage, and Compute Engine instances where all the usage information is stored. You have been tasked with enabling the access from their on-premises environment, which already has a configured VPN.

What should you do?

A. Use a Cloud VPN tunnel. Use your DNS provider to create DNS zones and records for private.googleapis.com. Connect the DNS provider to your on-premises network. Broadcast the request from the on-premises environment. Use a software-defined firewall to manage incoming and outgoing requests.

B. Use Partner Interconnect. Configure an encrypted tunnel in the auditor's on-premises environment. Use Cloud DNS to create DNS zones and A records for private.googleapis.com.

C. Use a Cloud VPN tunnel. Use Cloud DNS to create DNS zones and records for *.googleapis.com. Set up on-premises routing with Cloud Router. Use Cloud Router custom route advertisements to announce routes for Google Cloud destinations.

D. Use Direct Interconnect. Configure a VLAN in the auditor's on-premises environment. Use Cloud DNS to create DNS zones and records for restricted.googleapis.com and private.googleapis.com. Set up on-premises routing with Cloud Router. Add custom static routes in the VPC to connect individually to BigQuery, Cloud Storage, and Compute Engine instances.

2.3 Diagnostic Question 10

An external audit agency needs to perform a one-time review of Cymbal Bank's Google Cloud usage. The auditors should be able to access a Default VPC containing BigQuery, Cloud Storage, and Compute Engine instances where all the usage information is stored. You have been tasked with enabling the access from their on-premises environment, which already has a configured VPN.

What should you do?

A. Cloud DNS, subnet primary IP address range for nodes, and subnet secondary IP address range for pods and services in the cluster

B. Cloud VPN, subnet secondary IP address range for nodes, and subnet secondary IP address range for pods and services in the cluster

C. Nginx load balancer, subnet secondary IP address range for nodes, and subnet secondary IP address range for pods and services in the cluster

D. Cloud NAT gateway, subnet primary IP address range for nodes, and subnet secondary IP address range for pods and services in the cluster

2.3 Establish private connectivity

Courses

Networking in Google Cloud

- M5 Hybrid Connectivity
- M7 Network Design and Deployment

Security in Google Cloud

- M4 Configuring VPC for Isolation and Security
- M5 Securing Compute Engine: Techniques and Best Practices

Networking in Google Cloud: Hybrid Connectivity and Network Management

- M1 Hybrid Connectivity
- M3 Network Design and Deployment

Managing Security in Google Cloud

- M4 Configuring VPC for Isolation and Security

Security Best Practices in Google Cloud

- M1 Securing Compute Engine: Techniques and Best Practices

Skill Badges

Google Cloud

Build and Secure Networks in Google Cloud Quest

Google Cloud

Ensure Access and Identity in Google Cloud Quest

Documentation

Configuring Serverless VPC Access | Google Cloud

Overview of VPC Service Controls | Google Cloud

Choosing a Network Connectivity product | Google Cloud

Private Google Access | VPC

Manage zones | Cloud DNS

Private Google Access for on-premises hosts | VPC

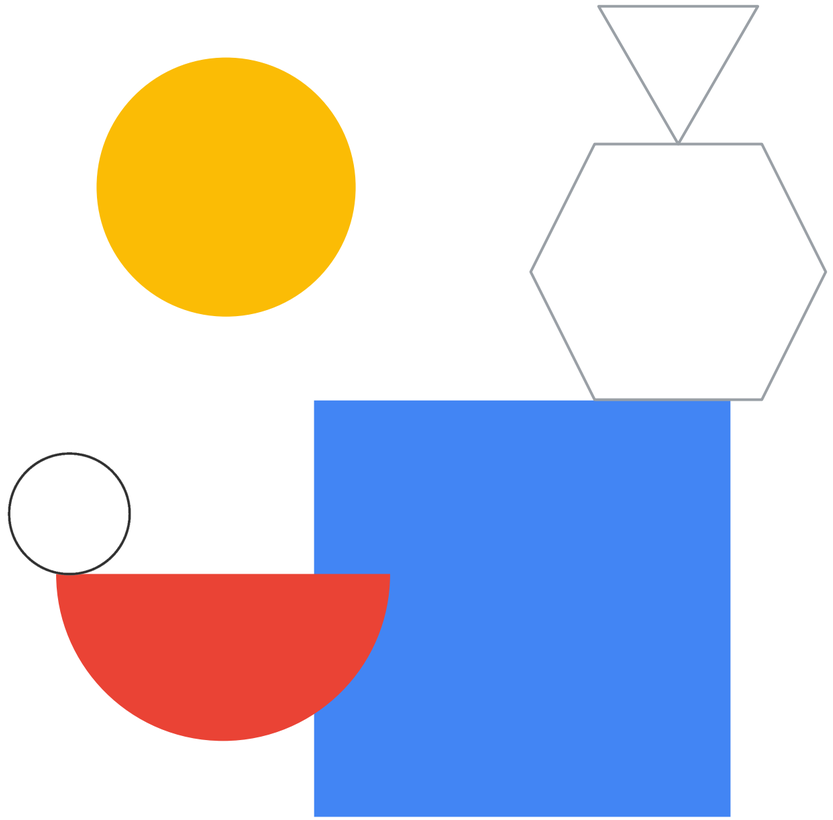
Simplifying cloud networking for enterprises: announcing Cloud NAT and more | Google Cloud Blog

Example GKE setup | Cloud NAT

Cloud NAT overview

Google Cloud

Section 3:
Ensuring data protection



3.1 Diagnostic Question 01

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 02

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

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 04

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 05

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

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 Protecting sensitive data

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
- M7 Application Security: Techniques and Best Practices
- M10 Content-Related Vulnerabilities: Techniques and Best Practices

[Managing Security in Google Cloud]

- M4 Configuring Virtual Private Cloud for Isolation and Security

[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]

- M3 Monitoring, Logging, Auditing, and Scanning

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 | Cloud IAM Documentation]

[Access control with IAM | Secret Manager Documentation | Google Cloud]

[About VM metadata | Compute Engine Documentation | Google Cloud]

3.2 Diagnostic Question 07

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 08

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 09

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 10

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.

3.2 Managing encryption at rest

Courses

Security in Google Cloud
- M5 Securing Compute Engine: Techniques and Best Practices
- M6 Securing Cloud Data: 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

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

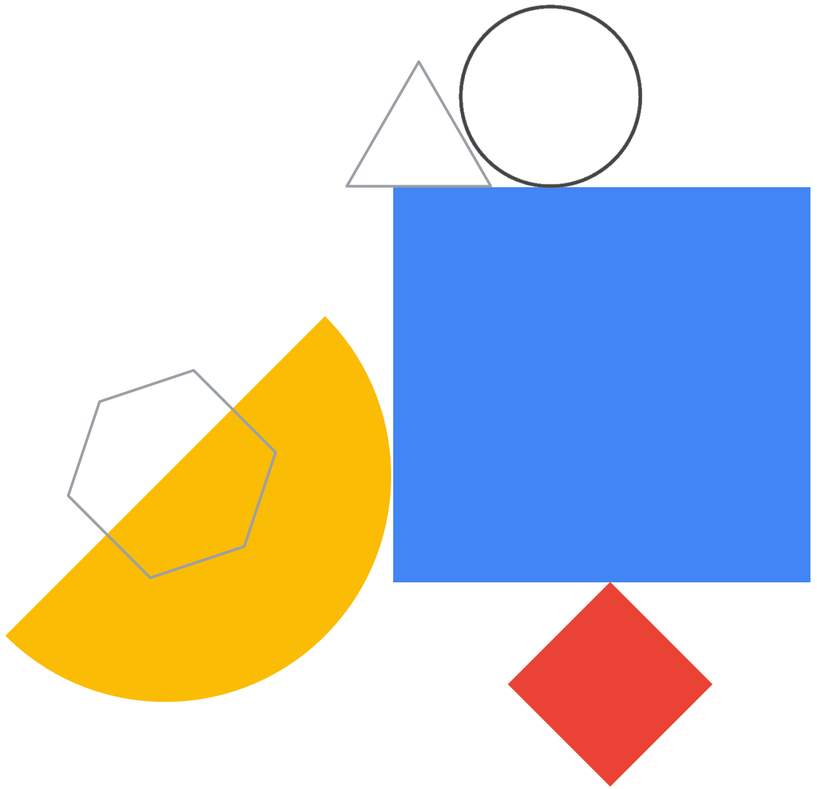
Using Cloud KMS with other products

Rotating keys | Cloud KMS Documentation

Confidential VM and Compute Engine | Google Cloud

Google Cloud

Section 4: Managing operations in a cloud solution environment



4.1 Diagnostic Question 01

Cymbal Bank has received Docker source files from its third-party developers in an Artifact Registry repository. These Docker fil2es will be part of a CI/CD pipeline to update Cymbal Bank's personal loan offering. The bank wants to prevent the possibility of remote users arbitrarily using the Docker files to run any code. You have been tasked with using Container Analysis' On-Demand scanning to scan the images for a one-time update.

What should you do?

A. Prepare a cloudbuild.yaml file. In this file, add four steps in order—build, scan, severity check, and push—specifying the location of Artifact Registry repository. Specify severity level as **CRITICAL**. Start the build with the command `gcloud builds submit.`

B. Prepare a cloudbuild.yaml file. In this file, add four steps in order—scan, build, severity check, and push—specifying the location of the Artifact Registry repository. Specify severity level as **HIGH**. Start the build with the command `gcloud builds submit.`

C. Prepare a cloudbuild.yaml file. In this file, add four steps in order—scan, severity check, build, and—push specifying the location of the Artifact Registry repository. Specify severity level as **HIGH**. Start the build with the command `gcloud builds submit.`

D. Prepare a cloudbuild.yaml file. In this file, add four steps in order—build, severity check, scan, and push—specifying the location of the Artifact Registry repository. Specify severity level as **CRITICAL**. Start the build with the command `gcloud builds submit.`

4.1 Diagnostic Question 02

Cymbal Bank's management is concerned about virtual machines being compromised by bad actors. More specifically, they want to receive immediate alerts if there have been changes to the boot sequence of any of their Compute Engine instances.

What should you do?

A. Set an organization-level policy that requires all Compute Engine VMs to be configured as Shielded VMs. Use Secure Boot enabled with Unified Extensible Firmware Interface (UEFI). Validate integrity events in Cloud Monitoring and place alerts on launch attestation events.

B. Set Cloud Logging measurement policies on the VMs. Use Cloud Logging to place alerts whenever actualMeasurements and policyMeasurements don't match.

C. Set an organization-level policy that requires all Compute Engine VMs to be configured as Shielded VMs. Use Measured Boot enabled with Virtual Trusted Platform Module (vTPM). Validate integrity events in Cloud Monitoring and place alerts on late boot validation events.

D. Set project-level policies that require all Compute Engine VMs to be configured as Shielded VMs. Use Measured Boot enabled with Virtual Trusted Platform Module (vTPM). Validate integrity events in Cloud Monitoring and place alerts on late boot validation events.

4.1 Diagnostic Question 03

Cymbal Bank runs a Node.js application on a Compute Engine instance. Cymbal Bank needs to share this base image with a 'development' Google Group. This base image should support secure boot for the Compute Engine instances deployed from this image. How would you automate the image creation?

How would you automate the image creation?

A. Prepare a shell script. Add the command gcloud compute instances stop with the Node.js instance name. Set up certificates for secure boot. Add gcloud compute images create, and specify the Compute Engine instance's persistent disk and zone and the certificate files. Add gcloud compute images add-iam-policy-binding and specify the 'development' group.

B. Start the Compute Engine instance. Set up certificates for secure boot. Prepare a cloudbuild.yaml configuration file. Specify the persistent disk location of the Compute Engine and the 'development' group. Use the command gcloud builds submit --tag, and specify the configuration file path and the certificates.

C. Prepare a shell script. Add the command gcloud compute instances start to the script to start the Node.js Compute Engine instance. Set up Measured Boot for secure boot. Add gcloud compute images create, and specify the persistent disk and zone of the Compute Engine instance.

D. Stop the Compute Engine instance. Set up Measured Boot for secure boot. Prepare a cloudbuild.yaml configuration file. Specify the persistent disk location of the Compute Engine instance and the 'development' group. Use the command gcloud builds submit --tag, and specify the configuration file path.

4.1 Diagnostic Question 04

Cymbal Bank uses Docker containers to interact with APIs for its personal banking application. These APIs are under PCI-DSS compliance. The Kubernetes environment running the containers will not have internet access to download required packages.

How would you automate the pipeline that is building these containers?

A. Create a Dockerfile with container definition and cloudbuild.yaml file. Use Cloud Build to build the image from Dockerfile. Upload the built image to a Google Container registry and Dockerfile to a Git repository. In the cloudbuild.yaml template, include attributes to tag the Git repository path with a Google Kubernetes Engine cluster. Create a trigger in Cloud Build to automate the deployment using the Git repository.

B. Create a Dockerfile with a container definition and a Cloud Build configuration file. Use the Cloud Build configuration file to build and deploy the image from Dockerfile to a Google Container registry. In the configuration file, include the Google Container Registry path and the Google Kubernetes Engine cluster. Upload the configuration file to a Git repository. Create a trigger in Cloud Build to automate the deployment using the Git repository.

C. Build a foundation image. Store all artifacts and a Packer definition template in a Git repository. Use Container Registry to build the artifacts and Packer definition. Use Cloud Build to extract the built container and deploy it to a Google Kubernetes Engine (GKE) cluster. Add the required users and groups to the GKE project.

D. Build an immutable image. Store all artifacts and a Packer definition template in a Git repository. Use Container Registry to build the artifacts and Packer definition. Use Cloud Build to extract the built container and deploy it to a Google Kubernetes Engine Cluster (GKE). Add the required users and groups to the GKE project.

4.1 Building and deploying secure infrastructure and applications

Courses

[Security in Google Cloud](#)
- M5 Securing Compute Engine: Techniques and Best Practices
- M7 Application Security: Techniques and Best Practices
- M8 Securing Kubernetes: Techniques and Best Practices
- M11 Monitoring, Logging, Auditing, and Scanning

[Security Best Practices in Google Cloud](#)
- M1 Securing Compute Engine: Techniques and Best Practices
- M3 Application Security: Techniques and Best Practices
- M4 Securing Kubernetes: Techniques and Best Practices

[Mitigating Security Vulnerabilities in Google Cloud](#)
- M3 Monitoring, Logging, Auditing, and Scaning

Skill Badges

Google Cloud

[Secure Workloads in Google Kubernetes Engine Quest](#)

Documentation

[Using On-Demand Scanning in your Cloud Build pipeline | Container Analysis documentation | Google Cloud](#)

[Container scanning | Container Analysis documentation | Google Cloud](#)

[Creating custom shielded images | Shielded VM | Google Cloud](#)

[Creating, deleting, and deprecating custom images | Compute Engine Documentation | Google Cloud](#)

[Managing access to custom images | Compute Engine Documentation | Google Cloud](#)

[Image management best practices | Compute Engine Documentation | Google Cloud](#)

[Deploying to GKE | Cloud Build Documentation](#)

[Quickstart: Build and push a Docker image with Cloud Build](#)

[Automated image builds with Jenkins, Packer, and Kubernetes | Cloud Architecture Center | Google Cloud](#)

4.2 Diagnostic Question 05

Cymbal Bank has Docker applications deployed in Google Kubernetes Engine. The bank has no offline containers. This GKE cluster is exposed to the public internet and has recently recovered from an attack. Cymbal Bank suspects that someone in the organization changed the firewall rules and has tasked you to analyze and find all details related to the firewall for the cluster. You want the most cost-effective solution for this task.

What should you do?

A. View the GKE logs in Cloud Logging. Use the log scoping tool to filter the Firewall Rules log. Create a Pub/Sub topic. Export the logs to a Pub/Sub topic using the command gcloud logging sinks create. Use Dataflow to read from Pub/Sub and query the stream.

B. View the GKE logs in the local GKE cluster. Use the kubectl Sysdig Capture tool to filter the Firewall Rules log. Create a Pub/Sub topic. Export these logs to a Pub/Sub topic using the GKE cluster. Use Dataflow to read from Pub/Sub and query the stream.

C. View the GKE logs in the local GKE cluster. Use Docker-explorer to explore the Docker file system. Filter and export the Firewall logs to Cloud Logging. Create a dataset in BigQuery to accept the logs. Use the command gcloud logging sinks create to export the logs to a BigQuery dataset. Query this dataset.

D. View the GKE logs in Cloud Logging. Use the log scoping tool to filter the Firewall Rules log. Create a dataset in BigQuery to accept the logs. Export the logs to BigQuery using the command gcloud logging sinks create. Query this dataset.

4.2 Diagnostic Question 06

Cymbal Bank experienced a recent security issue. A rogue employee with admin permissions for Compute Engine assigned existing Compute Engine users some arbitrary permissions. You are tasked with finding all these arbitrary permissions.

What should you do to find these permissions most efficiently?

A. Use Event Threat Detection and configure Continuous Exports to filter and write only Firewall logs to the Security Command Center. In the Security Command Center, select **Event Threat Detection** as the source, filter by **evasion: Iam**, and sort to find the attack time window. Click on **Persistence: IAM Anomalous Grant** to display Finding Details. View the **Source** property of the Finding Details section.

B. Use Event Threat Detection and configure Continuous Exports to filter and write only Firewall logs to the Security Command Center. In the Security Command Center, select **Event Threat Detection** as the source, filter by **category: anomalies**, and sort to find the attack time window. Click on **Evasion: IAM Anomalous Grant** to display Finding Details. View the **Source** property of the Finding Details section.

C. Use Event Threat Detection and trigger the IAM Anomalous grants detector. Publish results to the Security Command Center. In the Security Command Center, select **Event Threat Detection** as the source, filter by **category: iam**, and sort to find the attack time window. Click on **Persistence: IAM Anomalous Grant** to display Finding Details. View the **Source** property of the Finding Details section.

D. Use Event Threat Detection and trigger the IAM Anomalous Grant detector. Publish results to Cloud Logging. In the Security Command Center, select **Cloud Logging** as the source, filter by **category: anomalies**, and sort to find the attack time window. Click on **Persistence: IAM Anomalous Grant** to display Finding Details. View the **Source** property of the Finding Details section.

4.2 Diagnostic Question 07

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 08

Cymbal Bank has suffered a remote botnet attack on Compute Engine instances in an isolated project. The affected project now requires investigation by an external agency. An external agency requests that you provide all admin and system events to analyze in their local forensics tool. You want to use the most cost-effective solution to enable the external analysis.

What should you do?

A. Use Event Threat Detection. Trigger the IAM Anomalous Grant detector to detect all admins and users with admin or system permissions. Export these logs to the Security Command Center. Give the external agency access to the Security Command Center.

B. Use Cloud Audit Logs. Filter Admin Activity audit logs for only the affected project. Use a Pub/Sub topic to stream the logs from Cloud Audit Logs to the external agency's forensics tool.

C. Use the Security Command Center. Select Cloud Logging as the source, and filter by category: Admin Activity and category: System Activity. View the Source property of the Finding Details section. Use Pub/Sub topics to export the findings to the external agency's forensics tool.

D. Use Cloud Monitoring and Cloud Logging. Filter Cloud Monitoring to view only system and admin logs. Expand the system and admin logs in Cloud Logging. Use Pub/Sub to export the findings from Cloud Logging to the external agency's forensics tool or storage.

4.2 Diagnostic Question 09

The loan application from Cymbal Bank's lending department collects credit reports that contain credit payment information from customers. According to bank policy, the PDF reports are stored for six months in Cloud Storage, and access logs for the reports are stored for three years. You need to configure a cost-effective storage solution for the access logs.

What should you do?

A. Set up a logging export dataset in BigQuery to collect data from Cloud Logging and Cloud Monitoring. Create table expiry rules to delete logs after three years.

B. Set up a logging export dataset in BigQuery to collect data from Cloud Logging and the Security Command Center. Create table expiry rules to delete logs after three years.

C. Set up a logging export bucket in Cloud Storage to collect data from the Security Command Center. Configure object lifecycle management rules to delete logs after three years.

D. Set up a logging export bucket in Cloud Storage to collect data from Cloud Audit Logs. Configure object lifecycle management rules to delete logs after three years.

4.2 Diagnostic Question 10

Cymbal Bank uses Compute Engine instances for its APIs, and recently discovered bitcoin mining activities on some instances. The bank wants to detect all future mining attempts and notify the security team. The security team can view the Security Command Center and Cloud Audit Logs.

How should you configure the detection and notification?

A. Use Event Threat Detection's threat detectors. Export findings from 'Suspicious account activity' and 'Anomalous IAM behavior' detectors and publish them to a Pub/Sub topic. Create a Cloud Function to send notifications of suspect activities. Use Pub/Sub notifications to invoke the Cloud Function.

B. Enable the VM Manager tools suite in the Security Command Center. Perform a scan of Compute Engine instances. Publish results to Cloud Audit Logging. Create an alert in Cloud Monitoring to send notifications of suspect activities.

C. Enable Anomaly Detection in the Security Command Center. Create and configure a Pub/Sub topic and an email service. Create a Cloud Function to send email notifications for suspect activities. Export findings to a Pub/Sub topic, and use them to invoke the Cloud Function.

D. Enable the Web Security Scanner in the Security Command Center. Perform a scan of Compute Engine instances. Publish results to Cloud Audit Logging. Create an alert in Cloud Monitoring to send notifications for suspect activities.

4.2 Configuring logging, monitoring, and detection

Courses

[Security in Google Cloud](#)
- M11 Monitoring, Logging, Auditing, and Scanning

[Mitigating Security Vulnerabilities in Google Cloud](#)
- M3 Monitoring, Logging, Auditing, and Scanning

Documentation

[Security controls and forensic analysis for GKE apps | Cloud Architecture Center](#)

[Scenarios for exporting logging data: Security and access analytics | Cloud Architecture Center | Google Cloud](#)

[Security controls and forensic analysis for GKE apps | Cloud Architecture Center](#)

[Cloud Audit Logs overview](#)

[Cloud Audit Logs with Cloud Storage | Google Cloud](#)

[Configure Data Access audit logs](#)

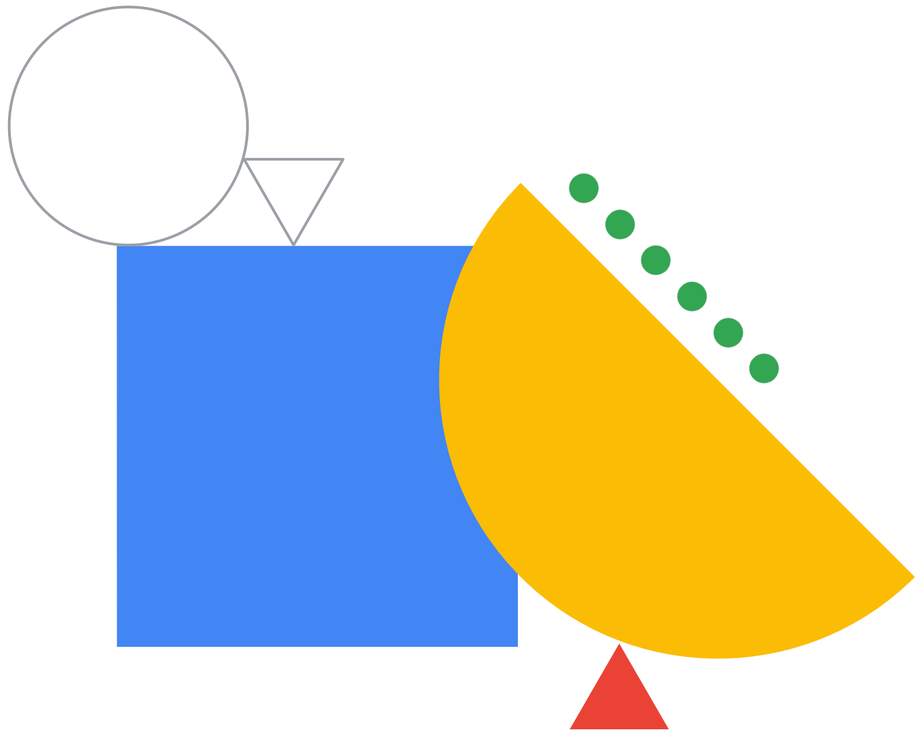
[Scenarios for exporting Cloud Logging: Compliance requirements | Cloud Architecture Center | Google Cloud](#)

[Security sources for vulnerabilities and threats | Security Command Center | Google Cloud](#)

[Configuring Security Command Center](#)

[Enabling real-time email and chat notifications](#)

Google Cloud



Section 5:
Ensuring compliance

5.1 Diagnostic Question 01

Cymbal Bank's lending department stores sensitive information, such as your customers' credit history, address and phone number, in parquet files. You need to upload this personally identifiable information (PII) to Cloud Storage so that it's secure and compliant with ISO 27018.

How should you protect this sensitive information using Cymbal Bank's encryption keys and using the least amount of computational resources?

A. Generate an AES-256 key as a 32-byte bytestring. Decode it as a base-64 string. Upload the blob to the bucket using this key.

B. Generate an RSA key as a 32-byte bytestring. Decode it as a base-64 string. Upload the blob to the bucket using this key.

C. Generate a customer-managed encryption key (CMEK) using RSA or AES256 encryption. Decode it as a base-64 string. Upload the blob to the bucket using this key.

D. Generate a customer-managed encryption key (CMEK) using Cloud KMS. Decode it as a base-64 string. Upload the blob to the bucket using this key.

5.1 Diagnostic Question 02

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 03

Cymbal Bank wants to launch a new website for their customers to enter their personal details and calculate their credit scores. The data will be stored in BigQuery tables and Cloud Storage buckets following GDPR compliance and data expiry rules. Cymbal Bank will also engage external analysts to build customized reports on BigQuery and Cloud Storage buckets. The external analysts must be able to run commands such as gsutil and bq from their command-line interfaces (CLIs), but they should not be able to copy the tables to any public storage.

How should you provide this access without violating the GDPR compliance?

A. Create the BigQuery dataset and Cloud Storage bucket in Europe. Change the project that contains BigQuery data to a new VPC with configured access to BigQuery and Cloud Storage. Add the external analysts to another Project. Use Shared VPC to share the configured Project with the external analyst's Project. Use Identity Access Management (IAM) to provide the Editor role to the external analysts.

B. Create a multi-region BigQuery dataset and dual-region Cloud Storage for high availability. Implement Identity and Access Management (IAM) controls on a service account with bigquery.rowAccessPolicies.getFilteredData permissions. Configure a Compute Engine instance to use this service account. Provide external analysts with access to this Compute Engine instance.

C. Create a multi-region BigQuery dataset and dual-region Cloud Storage for high availability. Implement Identity and Access Management (IAM) controls on a Compute Engine instance and provide all bigquery.datasets.* permissions. Create a Google group and provide access to the Compute Engine instance. Add all the external analysts to this group.

D. Create the BigQuery dataset and Cloud Storage bucket in Europe. Implement VPC Service Controls. Define the service perimeter to include a Cloud Storage bucket, BigQuery tables, and a Compute Engine instance. Configure the Compute Engine instance to connect to BigQuery and Cloud Storage. Provide external analysts with SSH access to the Compute Engine instance.

5.1 Diagnostic Question 04

Cymbal Bank's Insurance Analyst needs to collect and store anonymous protected health information of patients from various hospitals. The information is currently stored in Cloud Storage, where each hospital has a folder that contains its own bucket. You have been tasked with collecting and storing the healthcare data from these buckets into Cymbal Bank's Cloud Storage bucket while maintaining HIPAA compliance.

What should you do?

A. Create a new folder. Create a new Cloud Storage bucket in this folder. Give the Insurance Analyst the 'Editor' role on the new folder. Collect all hospital data in this bucket. Use the Google Cloud Healthcare Data Protection Toolkit to monitor this bucket.

B. Create a new Project. Create a new Cloud Storage bucket in this Project with customer-supplied encryption keys (CSEK). Give the Insurance Analyst the 'Reader' role on the Project that contains the Cloud Storage bucket. Use the Cloud DLP API to find and mask personally identifiable information (PII) data to comply with HIPAA.

C. Create a new Project. Use the Google Cloud Healthcare Data Protection Toolkit to set up a collection bucket, monitoring alerts, audit log sinks, and Forseti monitoring resources. Use Dataflow to read the data from source buckets and write to the new collection buckets. Give the Insurance Analyst the 'Editor' role on the collection bucket.

D. Use the Cloud Healthcare API to read the data from the hospital buckets and use de-identification to redact the sensitive information. Use Dataflow to ingest the Cloud Healthcare API feed and write data in a new Project that contains the Cloud Storage bucket. Give the Insurance Analyst the 'Editor' role on this Project.

5.1 Diagnostic Question 05

Cymbal Bank plans to launch a new public website where customers can pay their equated monthly installments (EMI) using credit cards. You need to build a secure payment processing solution using Google Cloud which should follow the PCI-DSS isolation requirements. How would you architect a secure payment processing environment with Google Cloud services to follow PCI-DSS?

Select the two correct choices

A. Create a new Google Cloud account with restricted access (separate from production environment) for the payment processing solution. Create a new Compute Engine instance and configure firewall rules, a VPN tunnel, and an internal load balancer.

B. Create a new Google Cloud account with restricted access (separate from production environment) for the payment processing solution. Configure firewall rules, a VPN tunnel, and an SSL proxy load balancer for a new App Engine flexible environment.

C. Create a new Google Cloud account with restricted access (separate from production environment) for the payment processing solution. Configure firewall rules, a VPN tunnel, and an HTTP(S) load balancer for a new Compute Engine instance.

D. Deploy an Ubuntu Compute Engine instance. Install the libraries needed for payment solutions and encryption/decryption. Deploy using Cloud Deployment Manager.

E. Deploy a Linux base image from preconfigured operating system images. Install only the libraries you need. Deploy using Cloud Deployment Manager.

5.1 Ensuring compliance

Documentation

Upload an object by using CSEK | Cloud Storage

Customer-managed encryption keys (CMEK) | Cloud KMS Documentation

Customer-supplied encryption keys | Cloud Storage

Data encryption options | Cloud Storage

ISO/IEC 27018 Certified Compliant | Google Cloud

Automating the Classification of Data Uploaded to Cloud Storage | Cloud Architecture Center | Google Cloud

Cloud DLP client libraries | Data Loss Prevention Documentation

Data Loss Prevention Demo

Overview of VPC Service Controls | Google Cloud

Getting to know the Google Cloud Healthcare API: Part 1

Sharing and collaboration | Cloud Storage

Google Cloud Platform HIPAA overview guide

Setting up a HIPAA-aligned project | Cloud Architecture Center

PCI Data Security Standard compliance | Cloud Architecture Center

Plan time to prepare

When will you take the exam?

How many weeks do you have to prepare?

How many hours will you spend preparing for the exam each week?

How many total hours will you prepare?

Sample study plan

Week 1	Week 2	Week 3	Week 4	Week 5	Week 6
Google Cloud Fundamentals: Core Infrastructure	Networking in Google Cloud: Defining and implementing networks	Networking in Google Cloud: Hybrid connectivity and network management	Build and secure networks in Google Cloud Skill Badge	Managing Security in Google Cloud	Security Best Practices in Google Cloud

Week 7	Week 8	Week 9	Week 10	Week 11	Week 12
Mitigating Security Vulnerabilities on Google Cloud	Ensure Access & Identity in Google Cloud Skill Badge	Secure Workloads in Google Kubernetes Engine Skill Badge	Review documentation	Sample questions	Take the certification exam

Weekly study plan

Now, consider what you've learned about your knowledge and skills through the diagnostic questions in this course. You should have a better understanding of what areas you need to focus on and what resources are available.

Use the template that follows to plan your study goals for each week. Consider:

- What exam guide section(s) or topic area(s) will you focus on?
- What courses (or specific modules) will help you learn more?
- What Skill Badges or labs will you work on for hands-on practice?
- What documentation links will you review?
- What additional resources will you use - such as sample questions?

You may do some or all of these study activities each week.

Duplicate the weekly template for the number of weeks in your individual preparation journey.

Weekly study template (example)

Area(s) of focus:	Managing service accounts
Courses/modules to complete:	Managing Security in Google Cloud M3 Identity and Access Management Security Best Practices in Google Cloud M1 Securing Compute Engine, M4 Securing Kubernetes
Skill Badges/labs to complete:	Ensure Access and Identity in Google Cloud Quest
Documentation to review:	Service accounts | IAM Documentation | Google Cloud Creating short-lived service account credentials | IAM Documentation | Google Cloud Restricting service account usage | Resource Manager Documentation | Google Cloud
Additional study:	Sample questions 1-3

Weekly study template

Area(s) of focus:	
Courses/modules to complete:	
Skill Badges/labs to complete:	
Documentation to review:	
Additional study:	