Designing for security and compliance

Completed on 27-January-2021

Attempt	Marks Obtained	Your score	Time Taken	Result
01	0 / 25	0.0%	00 H 00 M 07 S	Failed

Domains wise Quiz Performance Report

No	Domain	Total Question	Correct	Incorrect	Unattempted	Marked as Review
1	Other	25	0	1	24	0
Total	All Domain	25	0	1	24	0

Review the Answers

Sorting by All

Question 1 **Unattempted**

Domain : Other

You have been hired as a Cloud consultant for a company which is already using Google Cloud for their production and staging workload in separate GCP projects within an organization. Recently they came across a situation where an application running on a compute engine in a staging project requires a read access to a private GCS bucket which is in a production project. According to IAM best practices how will you grant access?

A. **Create a service account in production with access keys, grant Storage object viewer role and configure the application in to use access keys**

B. Create a service account in a staging project and attach the service account to the compute engine where the application is running. In production project grant staging projects service account Storage object viewer role in GCS bucket permission section. ✓

C. Create a service account in a staging project and attach the service account to the compute engine where the application is running. In production project grant staging projects service account Storage object viewer role in project IAM section.

D. Add allUsers as a member in the permission section of GCS bucket in production project and grant Storage object viewer role.

Explanation:

Answer B
As per IAM best practices, you should add staging project's service account in GCS bucket permission section and grant Storage object viewer role to provide cross account access

https://cloud.google.com/dataprep/docs/concepts/gcs-buckets

Option A is a possible option but directly using access keys in the compute engine is not a good security practice.
Option C is incorrect because assigning the role in IAM section of the project will give access to all buckets in that project, not a particular bucket, this will grant access permissions
Option D is incorrect because adding allUsers will make the bucket public and anyone can access it.

Ask our Experts Rate this Question? ☺ ☹

View Queries open

Question 2 **Unattempted**

Domain : Other

You have been hired as a Security consultant for a Financial company. The company holds sensitive data like customer account numbers, credit card information in the GCS bucket. The CTO wants additional security for mitigating exfiltration of data from a discontinued employee or attacker who has stolen identities. How will you mitigate this security risk by providing access to only authorized projects?

A. Cloud Armor

B. Threat Detection

C. VPC service controls

D. DLP

Explanation:

Answer C
VPC service controls allow you to lock down GCP resources. In VPC service control you can define which projects can call on your GCP APIs allowing you to whitelist the project which you want to grant access to. This can protect sensitive data from attackers or stolen identity

The most common use cases for VPC service controls are

1. Mitigate threats such as data exfiltration
2. Isolate parts of the environment by trust level
3. Secure access to multi-tenant services

https://cloud.google.com/vpc-service-controls

Option A is incorrect because it is used to mitigate DDoS attack and provides WAF
Option B is incorrect because it is used to detect threats like Burt force attack from logs and reports to Security command center
Option D is incorrect because Cloud DLP is used to detect and de-identify any sensitive information like credit card number or any PII data

Ask our Experts Rate this Question?

View Queries open

Question 3 **Unattempted**

Domain : Other

You are working for a large enterprise as a Solutions Architect. As per their compliance requirement all the data which is stored in Cloud SQL, Compute Engine and Cloud storage must be encrypted by customer-managed encryption keys with rotation schedule for symmetric keys to automatically generate a new key, please suggest the right choice for encryption?

A. Use default encryption which is provided by Google Cloud

B. Use CMEK using Cloud KMS

C. Use CSEK

D. Use third party service from Marketplace for customer-managed-encryption

Explanation:

Answer : B
Use CMEK using Cloud KMS
Customer-managed encryption keys (CMEK) using Cloud KMS lets you create your own encryption keys in Cloud KMS where you can create, rotate, automatically rotate and destroy symmetric encryption keys

https://cloud.google.com/storage/docs/encryption/customer-managed-keys

Option A is incorrect because default encryption is fully managed by GCP from creating keys to encrypting the data and storing the keys and rotating them
Option C is incorrect because CSEK is used when there is a requirement to store the encryption keys on-premise and only supports two services i.e cloud storage compute engine
Option D is incorrect because you cannot use a third-party solution for encrypting GCP services

Ask our Experts Rate this Question?

View Queries open

Question 4 **Unattempted**

Domain : Other

You have been hired as Consultant for a company which is planning migration of their enterprise application to GCP. As the company holds sensitive data and has the requirement to generate own encryption keys and manage it on-premises as per their regulatory compliance. The CTO has asked you to list the Google Cloud Products Which Supports Customer-supplied Keys(CSEK) before they perform migration. Please select the services which support CSEK.

A. All Google Cloud Products support CSEK

B. Compute Engine, Cloud Storage and Cloud SQL

C. Compute Engine and Cloud Storage

D. BigQuery, Cloud SQL and Datastore

Explanation:

Answer : C

CSEK is a feature in Google Cloud Storage and Google Compute Engine services

https://cloud.google.com/security/encryption-at-rest/customer-supplied-encryption-keys

Options A, B & D are incorrect because only Cloud Storage and Compute Engine supports CSEK.

Ask our Experts Rate this Question?

View Queries open

Question 5 **Unattempted**

Domain : Other

You have been hired as a DevSecOps Engineer by a large finance company. As per their regulatory compliance the CTO has informed you that by default all VM instances which are created in the entire organization are not allowed to use external IP addresses. How can you fulfill this requirement?

A. **Create a custom IAM policy at Organization level**

B. **Create an Organization Policy at Organization level**

C. **Create an Organization policy at individual project level**

D. **You cannot apply such kind of restriction in Google cloud**

Explanation:

Answer : B

An organization policy is a configuration of restrictions. You can create Organization policy at Organization level which will inherit to all resource under it and with Constraints for Compute Engine service which include Define allowed external IPs for VM instances set to Deny All

https://cloud.google.com/resource-manager/docs/organization-policy/overview

https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints

Option A is incorrect because IAM policy is attached to resources which are used to define access control

Option C is incorrect because we want to apply the restriction for all the projects under the organization, not a specific project
Option D is incorrect because we can have such kind of restriction using Organization Policy

Ask our Experts Rate this Question?

View Queries open

Question 6 **Unattempted**

Domain : Other

For this question, refer to the Dress4Win case study: "https://cloud.google.com/certification/guides/cloud-architect/casestudy-dress4win-rev2
In the initial phase of migration how will you isolate development and test environments?

A. **Create a separate project for testing and separate project for development** ✓

B. **Create a Single VPC for all environments, separate by subnets**

C. **Create a VPC network for development and separate VPC network for testing**

D. **You cannot isolate access between different environments in Google cloud**

Explanation:

Answer : A
As per the IAM best practices, you should create a separate project for each environment to isolate each environment.

https://cloud.google.com/blog/products/gcp/iam-best-practice-guides-available-now

Option B is incorrect because as per IAM best practice you should create a separate project for each team
Option C is incorrect because you cannot isolate each env by creating 2 VPC in the same project. If anyone has permission to start/stop VM he can stop both environments VM's if they are in the project
Option D is incorrect because you can isolate env's by creating a separate project for each

Ask our Experts Rate this Question?

View Queries open

Question 7 **Unattempted**

Domain : Other

You have been hired by a large U.S based healthcare firm as a Consultant which is planning to migrate entire application and on-premise data to Google Cloud. As the data includes medical records of different hospitals located in the U.S. What regulations would you look to for more guidance on complying with relevant regulations?

A. HIPAA ✓

B. PCI-DS

C. GDPR

D. SOX

Explanation:

Answer : A
HIPAA (Health Insurance Portability and Accountability Act) is regulatory compliance in the U.S which is used to protect the healthCare data collected by websites and application for business purpose in the U.S

https://cloud.google.com/security/compliance/hipaa-compliance

Option B is incorrect because it is a Payment Card Industry Data Security Standard to protect credit card information collected for business
Option C is incorrect because GDPR(General Data Protection Regulation) is regulatory compliance in Europe which is used to protect any personally identifiable information collected for business purpose within the Europe region
Option D is incorrect because Option SOX compliance is used for financial auditing purpose

Ask our Experts Rate this Question? ☺ ☹

View Queries open

Question 8 **Unattempted**

Domain : Other

You are working as a Solutions Architect for an enterprise. Your company recently developed a Web-App which will be deployed on App Engine. Following the IAM best practices, which roles should be granted when the Team Lead needs to audit App Engine code in Production using read-only access, and Developers need to release code into Production?

A. roles/appengine.appAdmin, roles/appengine.appViewer

B. roles/appengine.appAdmin, roles/appengine.codeViewer

C. roles/appengine.serviceAdmin, roles/appengine.deployer

D. roles/appengine.codeViewer, roles/appengine.deployer

Explanation:

Answer : D
The team lead is responsible for auditing App engine code in production so he will need only roles/appengine.codeViewer to perform his duties. This role grants read-only access to deployed source code and application configurations. Developers can be granted roles/appengine.deployer which grants them read-only access to all application configuration, settings and allow them to create a new version of the application

https://cloud.google.com/appengine/docs/admin-api/access-control#roles

Option A is incorrect because it grants Read/Write/Modify permission to team lead and developers will not have permission to create a new version of an application
Option B is incorrect because it will grant Read/Write/Modify permission to team lead
Option C is incorrect because it will not allow the team lead to read the deployed source code

Ask our Experts Rate this Question?

View Queries open

Question 9 **Unattempted**

Domain : Other

You have been working as a Solutions Architect for a company who has recently developed an online mobile game which will be mostly used for children ages 10 to 14 and will be deployed on Google Cloud in the us-west1 region. The online game will collect the personal information of the player such as name, address, age and hobbies. With which regulation would you advise them to comply with?

A. HIPAA

B. PCI-DS

C. GDPR

D. COPPA ✓

Explanation:

Answer : D
COPPA is regulatory compliance in the U.S which is related to protecting the privacy of children below 13 age in the U.S

https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0

Option A is incorrect because HIPAA is related to protecting the privacy of healthcare data in the U.S
Option B is incorrect because it is a Payment Card Industry Data Security Standard to protect credit card information collected for business
Option C is incorrect because GDPR(General Data Protection Regulation) is regulatory compliance in Europe which is used to protect any personally identifiable information collected for business purpose within the Europe region

Ask our Experts Rate this Question? ☺ ☹

View Queries open

Question 10 **Unattempted**

Domain : Other

You have been hired as a DevSecOps Engineer by an enterprise who are planning to migrate their application on Google Cloud Platform but as per the compliance requirement they want to use their existing Active Directory domain to manage user identities. What you should suggest in this scenario?

A. Use Google Cloud Directory Sync to sync Active Directory username with Cloud Identity ✓

B. Use Identity-Aware Proxy configured with your Active Directory Domain

C. There is no option for using Active Directory Domain. Use G-Suite for user management

D. Create an Active Directory domain controller on Compute Engine that is a replica of on-premise AD and use Google Cloud Directory Sync

Explanation:

Answer : A
By using Google Cloud Directory Sync you can sync Active directory username with Cloud Identity. In order to sync users and groups, you need to install GCDS agent in you AD servers

https://support.google.com/a/answer/106368?hl=en

Option B is incorrect because Identity aware proxy lets you manage access to the applications which are running on App Engine, Kubernetes engine and VM's
Option C is incorrect because you can sync Active directory users using GCDS
Option D is incorrect because there is no need to move AD servers to compute engine, you can directly install GCDS agent on AD servers

Ask our Experts Rate this Question? ☺ ☹

View Queries open

Question 11 **Unattempted**

Domain : Other

You have been hired as Consultant by an enterprise. The company is running their production workload on Google Cloud. One of your clients requested a penetration testing report for your application and your CTO has decided to hire a Security specialist to perform penetration testing on your application, what is the procedure to conduct penetration testing on Google Cloud?

A. You need to raise a support ticket with Google cloud for permission to perform Penetration testing

B. Google Cloud does not allow to perform any kind of penetration testing

C. You do not have to notify Google when conducting a penetration test on your application ✓

D. Raise a support ticket with Google to perform penetration testing on your behalf

Explanation:

Answer : C
You can perform penetration testing on your application without informing Google Cloud but you must satisfy all the terms and conditions of Google Cloud

https://support.google.com/cloud/answer/6262505?hl=en.

Option A is incorrect because there is no need to raise a support ticket to conduct penetration testing on your application
Option B is incorrect because you can perform penetration testing on GCP
Option D is incorrect because google does not perform penetration testing on your behalf. You can perform yourself without notifying google cloud

Ask our Experts Rate this Question?

View Queries open

Question 12 **Unattempted**

Domain : Other

You have been hired as a DevOps Engineer by a large finance company. As per their regulatory compliance the CTO has informed you that any resources which will be created in Google Cloud must be created in the U.S region only and all other regions are restricted by default. How can you restrict the resources creation limited to the U.S region only?

A. Create a custom IAM policy at Organization level

B. Create an Organization Policy at Organization level

C. Create an Organization policy at individual project level

D. You cannot apply such kind of restriction in Google cloud

Explanation:

Answer : B
An organization policy is a configuration of restrictions. You can create Organization policy at Organization level which will inherit to all resource under it and with Constraint for Google Cloud Platform - Resource Location Restriction set to the U.S only

https://cloud.google.com/resource-manager/docs/organization-policy/overview

https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints

Option A is incorrect because IAM policy is attached to resources which are used to define access control
Option C is incorrect because we want to apply the restriction for all the projects under the organization, not a specific project
Option D is incorrect because we can have such kind of restriction using Organization Policy

Ask our Experts Rate this Question?

View Queries open

Question 13 **Unattempted**

Domain : Other

You are working for a large enterprise as a GCP Cloud Architect. As per the new compliance requirement, you should regularly save your all admin activity and VM system logs within your project centrally for third party auditing which will happen once every month. How will you achieve this requirement keeping the cost low?

A. All admin and VM system logs are automatically collected by Stackdriver, just create sink for selected logs to GCS nearline bucket

B. Stackdriver automatically collects admin activity logs for most services. Only the Stackdriver Logging agent must be installed on each instance to collect system logs and create sink for selected logs to GCS nearline bucket ✓

C. Stackdriver automatically collects admin activity logs for most services. Only the Stackdriver Logging agent must be installed on each instance to collect system logs and create sink for selected logs to GCS cold storage bucket

D. All admin and VM system logs are automatically collected by Stackdriver, just create sink for selected logs to GCS cold storage bucket

Explanation:

Answer : B
Admin activity logs are automatically collected for most of the services in GCP. For the VM system logs, you need to install a Logging agent in each VM whose logs you want to export to stackdriver logging.
As per the compliance requirement, you must retain logs for auditing for that you should create a sink to GCS nearline bucket. These logs will be accessed once a month that's why the

nearline bucket is the best storage option.

https://cloud.google.com/logging/docs/agent

https://cloud.google.com/logging/docs/audit

Option A is incorrect because VM system logs are not automatically collected. You need to install a stackdriver agent to get VM system logs.
Option C is incorrect because the audit will happen once a month and for that Coldline storage is not a good option
Option D is incorrect because VM system logs are not automatically collected you need to install stackdriver agent to get VM system logs and also coldline is not a right storage option

Ask our Experts Rate this Question?

View Queries open

Question 14 **Unattempted**

Domain : Other

You are working for a large enterprise where the management of network and security resources such as firewalls are typically managed by a dedicated Security team for the entire organization. The development teams only want flexibility to launch instances and carry out other actions related to instances in the dev project only. How will you grant respective IAM permission to the development team and security team keeping the least privilege principle in mind?

A. **Compute Network Admin role for Security team at Organization level and Compute Instance Admin role for development team for dev project only** ✓

B. **Compute Network Admin role for Security team at Organization level and Compute Instance Admin role for development team at organization level**

C. **Compute Network Admin role for Security team at Organization level and Compute Network Admin role for development team for dev project only**

D. **Compute Instance Admin role for Security team at Organization level and Compute Network Admin role for development team at Organization level**

Explanation:

Answer : A
Assign Compute Network Admin role to the Security team at the Organization level. This will grant them Permissions to administer networking resources. The network admin role does not

allow the security team to control the compute engine resources. By assigning this role at Organization level the Security team will have access to every project within an organization

Assign Compute Instance Admin role to the Development team at a specific project-level i.e. dev project. This will grant the dev-team full access to compute engine resources only and read-only access to networking resources. By assigning this role at a specific project level will grant them access to resources in that particular project only.

https://cloud.google.com/compute/docs/access/iam

https://cloud.google.com/iam/docs/resource-hierarchy-access-control

Option B is incorrect because it will grant dev-team access to all projects under the organization.
Option C is incorrect because the Network admin role will not allow dev-team to control compute resources
Option D is incorrect because Compute Instance admin role will not allow the Security team to administrate networking resources and Network Admin role will not allow the dev team to administrate compute resources

Ask our Experts Rate this Question?

View Queries open

Question 15 **Unattempted**

Domain : Other

You are working for a large Finance company as a Solutions architect. They have multiple applications running in production. All the applications log data is stored in GCS bucket for future analysis to improve the application performance. What is the recommended approach to De-identify personally identifiable information or payment card information stored in logs?

A. Use Cloud DLP

B. Use threat detection

C. Use Web Security Scanner

D. Use Cloud Armor

Explanation:

Answer : A
Cloud DLP is a fully managed service used to de-identify sensitive data like credit card

numbers, Phone numbers, and any other PII information stored in text files within cloud storage and Bigquery. After detecting sensitive data the DPL API provides various options like mask the data or delete the data

https://cloud.google.com/dlp/docs/deidentify-sensitive-data

Option B is incorrect because it is used to detect threats like Brute force attack from logs and reports to Security command center
Option C is incorrect because it is used to find any vulnerable library used in your application code
Option D is incorrect because it is used to mitigate DDoS attack and provide WAF

Ask our Experts Rate this Question?

View Queries open

Question 16 **Unattempted**

Domain : Other

You have been hired by a large enterprise as a Solutions Architect which has several departments like HR, development, and finance. There is a requirement that they want to control IAM policies for each department separately but centrally. Which hierarchy should you use?

A. **A single organization with separate folders for each department**

B. **A separate organization for each department**

C. **A single organization with a separate project for each department**

D. **A separate organization with multiple folders**

Explanation:

A) Option is correct

As per Google recommended best practices you should have multiple folders within an organization for each department. Each department can have multiple teams and projects. By using folders, you can group resources for each department that shares common IAM policies.

For example, you have multiple projects for the HR department and want to assign a Compute Instance Admin role to a user for each project in the HR department. You can assign a Compute Instance Admin role to the user at the HR folder level which will grant him access to

each project within the HR folder.

https://cloud.google.com/resource-manager/docs/creating-managing-folders

Option B is incorrect because you cannot manage IAM Policies centrally if you create separate Organization for each department

Option C is incorrect because each department can have multiple teams and multiple projects under it. So it will become difficult to manage IAM policy centrally for each project within the department

Option D is incorrect because you cannot manage IAM Policies centrally if you create separate Organizations for each department.

Ask our Experts Rate this Question?

View Queries open

Question 17 **Unattempted**

Domain : Other

You have been hired as a DevSecOps engineer by a finance company. They want to upload files from an on-premise server to Google Cloud Storage. But as per there security policy, the files must be encrypted using customer-supplied encryption keys on Google Cloud storage. How will you fulfill this requirement?

A. **Use --encryption_key flag with gsutil command to supply encryption key while uploading files**

B. **Supply the encryption key in Cloud KMS and use that key for encryption**

C. **Add the encryption_key option in the boto configuration file and use gsutil command to upload files** ✓

D. **Configure the encryption key in gcloud configuration and use gsutil to upload files**

Explanation:

C) Option is correct

To use customer-supplied encryption keys with Google Cloud Storage while uploading files, you must add the encryption_key option in [GSUtil] section of the boto configuration file.

Boto configuration file is the file where you can configure all configurations related to gsutil command line
https://cloud.google.com/storage/docs/gsutil/addlhelp/UsingEncryptionKeys

Option A is incorrect because you need to add encryption_key option in GSUtil section of boto configuration file there is no such flag while using gsutil commands

Option B is incorrect because as per security policy they don't want to store Keys in Google Cloud. So CMEK is not an option.

Option D is incorrect because encryption_key must be added in boto file, not the gcloud configuration

Ask our Experts Rate this Question?

View Queries open

Question 18 **Unattempted**

Domain : Other

You are working for a large enterprise as a DevSecOps engineer. They are running several applications on compute engine VM. The database credentials required by an application are stored in the Cloud Secret Manager service. As per the best practices, what is the recommended approach for the application to authenticate with Google Secret manager service in order to obtain the credentials?

A. **Ensure that the service account used by the VM's have appropriate Cloud Secret Manager IAM roles and VM's have proper access scopes** ✓

B. **Ensure that the VM's have full access scope to all Cloud APIs and do not have access to Cloud Secret Manager service in IAM roles**

C. **Generate OAuth token with appropriate IAM permissions and use it in your application**

D. **Create a service account and access key with appropriate IAM roles attached to access secrets and use that access key in your application**

Explanation:

A) Option is correct

In order to access Cloud services for an application running on compute engine VM, you should use a service account attached to the VM. If you are using the default service account

you need to set access scope for API's and also need to attach appropriate IAM roles to the service account

https://googleapis.dev/python/google-api-core/latest/auth.html

https://cloud.google.com/compute/docs/access/service-accounts

Option B is incorrect because you also need to attach IAM roles to the service account with required Cloud API's access scope

Option C is incorrect because as per Google's recommended best practices you should use service account attached with the service

Option D is incorrect because as per Google's recommended best practices you should use service account attached with the service

Ask our Experts Rate this Question?

View Queries open

Question 19 **Unattempted**

Domain : Other

You are working for a large finance company as a Solutions Architect. There is a requirement that the Security team wants read-only access to all the projects under the organization for internal auditing purposes. How will you grant access to the security team as per Google's IAM best practices?

A. **Organization viewer, Project editor**

B. **Organization viewer, Security Center Admin**

C. **Organization viewer, Project owner**

D. **Organization viewer, Project viewer**

Explanation:

D) Option is correct

Organization viewer role will provide the ability to view the entire organization and Project viewer role will grant read-only access to all the projects and resources under it within the organization

Option A is incorrect because the Project editor is a too broad role and it will grant read-write access to the resources within the project

Option B is incorrect because the Security Center Admin will not grant read-only access to the project

Option C is incorrect because the Project editor is a too broad role and it will grant admin access to all the resources within the project

Ask our Experts Rate this Question?

View Queries open

Question 20 **Unattempted**

Domain : Other

Your organization is developing an event-driven application in which cloud functions will access Cloud SQL for managing data. As per the security best practices, you want to store the Cloud SQL credentials securely. Where will you store the Cloud SQL credentials?

A. In the Cloud function code

B. In the Cloud function environment variable

C. In Cloud Secret Manager

D. In Cloud KMS

Explanation:

C) Option is correct

You should store Cloud SQL credentials in Cloud Secret Manager where you can rotate, create versions and can manage access to credentials

https://cloud.google.com/secret-manager/docs/creating-and-accessing-secrets

Option A is incorrect because storing the credentials in the code itself will make it accessible to anyone having access to cloud functions and it will also become difficult to rotate credentials

Option B is incorrect because storing the credentials in the environment variable will make it accessible to anyone having access to cloud functions

Option D is incorrect because Cloud KMS is used to managing encryption and decryption

Ask our Experts

Rate this Question?

View Queries open

Question 21 **Unattempted**

Domain : Other

You are working for a company that is using Google Cloud for its production workload. As per their new security policy, all the Admin activity logs must be retained for at least 5 years and will be accessed once a year for auditing purposes. How will you ensure that all IAM Admin Activity logs are stored for at least 5 years keeping cost low?

A. Create a sink to Cloud Storage bucket with "Archival" as a storage class

B. Create a sink to BigQuery

C. Create a sink to Pub/Sub

D. Store it in Cloud logging itself

Explanation:

A) Option is correct

All the admin activity logs are enabled by default and stored in cloud logging.
The default retention period for Admin activity logs is 400 Days. If you want to store logs for a longer period, you must create a sink. In our case since logs will be accessed once a year for auditing purposes then Cloud storage sink is the most suitable option.

Option B is incorrect because BigQuery is not a cost-effective solution

Option C is incorrect because Pub Sub is not used for long term storage

Option D is incorrect because Cloud Logging default retention period is 400 days

Ask our Experts Rate this Question?

View Queries open

Question 22 **Unattempted**

Domain : Other

For this question, refer to the Dress4Win case study: https://cloud.google.com/certification/guides/cloud-architect/casestudy-dress4win-rev2
Dress4Win is planning to expand its business in the European region. Which regulation would you advise them to comply with?

A. HIPAA

B. PCI-DSS

C. COPPA

D. GDPR

Explanation:

D) Option correct

GDPR (General Data Protection Regulation) is regulatory compliance in Europe which is used to protect any personally identifiable information collected for business purpose within the European region

Option A is incorrect because HIPAA is related to protecting the privacy of healthcare data in the U.S

Option B is incorrect because it is a Payment Card Industry Data Security Standard to protect credit card information collected for business

Option C is incorrect because COPPA is regulatory compliance in the U.S which is related to protecting the privacy of children below 13 age in the U.S

Ask our Experts Rate this Question?

View Queries open

Question 23 **Unattempted**

Domain : Other

You are working as a Solutions Architect for a large Media Company. They are using BigQuery for their data warehouse purpose with multiple datasets in it.

There is a requirement that a data scientist wants full access to a particular dataset only on which he can run queries against the data.
How will you assign appropriate IAM permissions keeping the least privilege principle in mind?

A. **Grant bigquery.dataEditor at the required dataset level and bigquery.user at the project level** ✓

B. **Grant bigquery.dataEditor and bigquery.user at the project level**

C. **Grant bigquery.dataEditor at the project level and bigquery.user at the required dataset level**

D. **Grant bigquery.admin at required dataset level and bigquery.user at the project level**

Explanation:

A) Option is correct

bigquery.dataEditor on the required dataset will grant write access to the particular Dataset only and bigquery.user at the project level will grant him access to run query jobs in project

https://cloud.google.com/bigquery/docs/access-control

All other options are incorrect because they are too broad access roles as per our requirement

Ask our Experts Rate this Question? ☺ ☹

View Queries open

Question 24 **Unattempted**

Domain : Other

Your company recently performed an audit on your production GCP project. The audit

revealed that recently an SSH port was opened to the world on a compute engine VM. The management has requested entire details of the API call made. How will you provide detailed information?

A. **Navigate to the Logs viewer section from the console, select VM Instance as a resource and search for the required entry** ✓

B. **Navigate to the Stackdriver trace section from the console, select GCE Network as a resource and search for the required entry**

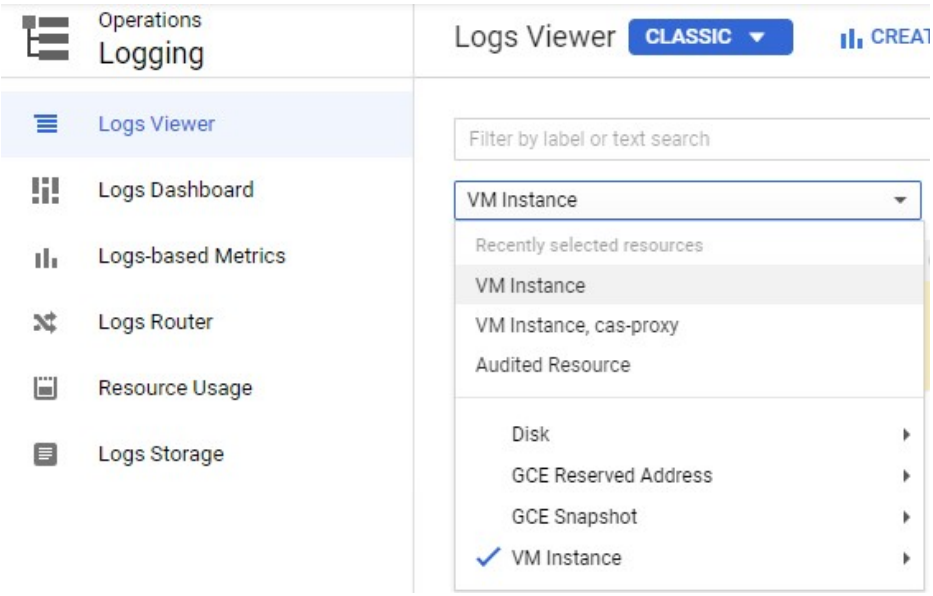
C. **Connect to the compute engine VM and check system logs for API call information**

D. **Navigate to the Stackdriver monitoring section from the console, select GCE Network as a resource and search for the required entry**

Explanation:

A) Option is correct

All the IAM admin related activity logs are stored in the logs viewer section of Cloud Logging. You can see the entire details for an API call made in the logs viewer section of that resource. You can see what network tags were added to the particular VM in this section.



Option B is incorrect because Stackdriver trace is used to collect latency details from applications

Option C is incorrect because system logs will contain all logs related to the operating system only, not the Google cloud resources

Option D is incorrect because Stackdriver monitoring is used to monitor CPU, memory,

disk, or any other custom metrics.

Ask our Experts Rate this Question?

View Queries open

Question 25 **Incorrect**

Domain : Other

One of your application recently was a victim of a large scale DDOS attack and web application attacks which is running in the Managed instance group behind the HTTPS load balancer. The CTO has tasked you to look for the services which can mitigate the DDOS attack and also provide a web application firewall. Which GCP service will you use?

A. Threat Protection

✓ B. GCP Firewalls

C. Web Security Scanner

D. Cloud Armor

Explanation:

D) Option is correct

Cloud Armor is a fully managed service that protects your application against DDOS attack and also provides a Web access firewall which can further provide protection against attacks like XSS (cross-site-scripting), SQL injection, etc. You can also have geo-based access control to your application using Cloud armor.
https://cloud.google.com/armor

Option A is incorrect because it is used to detect threats like Burt force attack from logs and reports to Security command center

Option B is incorrect because it is used to control incoming and outgoing traffic to and from your compute engine VM's

Option C is incorrect because it is used to find any vulnerable library used in your application code

Ask our Experts

Rate this Question?

View Queries open

Finish Review