Google Cloud Professional Security Engineer

Practice Questions and Answers

Draft Version 1.1 7/22/21

Copyright

Front cover image by Self.
Book design by Self

Printed by TechCommanders, LLC., in the United States of America.

First printing edition 2021.

TechCommanders, LLC

Jacksonville, FL 32256

www.TechCommanders.com

Disclosure

TechCommanders, LLC is an independent entity from Google and Google Cloud. This publication may be used in assisting candidates, students, and readers to better prepare for the Google Cloud Professional Security Engineer exam.
Neither TechCommanders, LLC nor Google and or Google Cloud warrant this publication will ensure passing the Google Cloud Professional Security Engineer exam.
The Google Cloud and Google Cloud Professional Security Engineer are trademarks or registered trademarks of Google in the United States and/or other countries. All other trademarks are trademarks of their respective owners.

GCP Professional Security Engineer Mock Exam Questions

BEFORE YOU BEGIN

The main objective of these mock exams is to validate you have understood the objectives for the exam.

Answers with explanations are on the following pages.

If you do well on these exams (Over 75%) you should feel confident to sit for and pass the Professional Cloud Engineer exam immediately!

Additional FREE practice Questions are available online at

https://TechCommanders.com

GCP PROFESSIONAL SECURITY ENGINEER

PRACTICE EXAM

50 QUESTIONS

This practice exam is followed with the same practice exam with answers and explanation.

Good Luck. These questions are more difficult than on the exam. If you do well here. you should feel confident on sitting for the exam.

1. Your IT Team wants to centrally manage GCP IAM permissions from their on-premises Active Directory Service. Your IT team also needs to manage permissions by AD group membership.

What should your IT team do to meet these requirements? (Select One)

A. Configure SAML 2.0 (SSO) and them great a group in IAM.
B. Configure Cloud Identity and IAM to manage permissions from the on-premises AD Servers.
C. Configure Cloud Directory to synchronize groups and then set permissions to those groups.
D. Gcloud components install components kubectl

2. A recent software update to your enterprises e-commerce website that is running on Google Cloud has caused the website to crash for several hours.

Your CTO decides that all critical changes must now have a back-out/roll-back plan. The website is deployed on hundreds of virtual machines (VMs), and critical changes are frequent.

Which two actions should you take to implement the back-out/roll-back plan? (Select Two)

A. Use managed instance groups with the "update-instances" command when starting a rolling update
B. Enable object versioning on the website's static data files stored in Google Cloud Storage
C. Create a new instance template with applied fixes and roll out via A/B test
D. Use unmanaged instance groups with the "update-instances" command when starting a rolling update

---

3. A customer deploys an application to App Engine and needs to check for Open Web Application Security Project (OWASP) vulnerabilities. Which service should be used to accomplish this? (Select One)

A. Cloud Armor
B. Binary Authorization
C. Cloud Security Scanner
D. Forseti Security

---

4. Your customer has asked you to follow Google-recommended practices to leverage envelope encryption and encrypt data at the application layer. What should you do? (Select One)

A. Generate a data encryption key (DEK) remotely to encrypt the data, and then generate a new key encryption key (KEK) in Cloud KMS to encrypt the DEK. Store both these keys and your plaintext that have been created on your USB drive.
B. Generate a data encryption key (DEK) locally to encrypt the data, and then generate a new key encryption key (KEK) in

Cloud KMS to encrypt the DEK. Store the encrypted data and the encrypted DEK.

C. Generate a data encryption key (DEK) locally to encrypt the data, and then generate a new key encryption key (KEK) in Cloud KMS to encrypt the DEK. Store the encrypted data and the wrapped KEK.
D. Generate a data encryption key (DEK) locally to encrypt the data, and then generate a new data encryption key (DEK) in Cloud KMS to encrypt the DEK. Store the encrypted data and the encrypted KEK locally.

---

5. You're currently setting up your VMs on Compute Engine and you were asked to install the monitoring agent for Cloud Operations. What is the agent called you will install (Select One)

A. Cloud Operations agent
B. Cloud Monitoring agent
C. Collectd Agent
D. Stastd Agent

---

6. Cloud KMS stores keys in a key hierarchy designed for ease, with access to resources in the key hierarchy governed by Identity and Access Management. Which of the following answers shows the correct level and order of a Cloud KMS key hierarchy? (Select One)

A. Key Ring, Key, Key Version
B. Key Ring, Key Version, Key
C. Key Version, Key, Key Ring
D. Key Version, Key Ring, Key

---

7. You have been invited to a meeting with your enterprise lead architect. The enterprise architect is requesting help on how he would be able to reliably deliver Cloud Operations logs from GCP to their on-premises SIEM system? He also stated he would the simplest option. (Select One)

A. Build a custom connector for the SIEM to query for all the logs from the provided Google Cloud API's.
B. Send your logs to the SIEM system using syslog.
C. Configure an organization log sink which would export to a Cloud/Pub topic. This could be sent to their SIEM via Cloud DataFlow template.
D. Configure every project to have a log sink which would export to a Cloud/Pub topic. This could be sent to their SIEM via Cloud DataFlow.

---

8. You have been asked to meet PCI DSS requirements with a customer's application on GCP. The customer wants to ensure that all outbound traffic is authorized. Which following two cloud offerings will meet this requirement without introducing additional compensating controls? (Select Two)

A. Compute Engine
B. Cloud Run
C. Cloud Functions
D. Kubernetes Engine
E. App Engine

---

9 Your considering placing your Infrastructure as code processes on Cloud Deployment Manager. What could be considered a security risk of doing this? (Select One)

A. Cloud Deployment Manager requires a Google APIs service account to run.
B. Cloud Deployment Manager APIs could be deprecated in the future which pose risks.
C. Cloud Deployment Manager can be used to permanently delete cloud resources.
D. Cloud Deployment Manager takes some training to use.

---

10 When working with agents in a support center via online chat, an organization's customers often share pictures of their documents with personally identifiable information (PII).

The organization that owns the support center is concerned that the PII is being stored in their databases as part of the regular chat logs, they retain for review by internal or external analysts for customer service trend analysis.

Which Google Cloud solution should the organization use to help resolve this concern for the customer while still maintaining data utility? (Select One)

A. Use image inspection and redaction of DLP to redact PII data from the images before storing them to be analysed.
B. Use Object Lifecycle Management to validate all records with PII data are deleted
C. Use the Cloud Key Management Service (KMS) to encrypt your PII data that will be shared and then stored.
D. Use the generalization feature Data Loss Prevention (DLP) to redact everything that is not allowed to be stored.

---

11. Your IT team sets up a Shared VPC Network where project my-vpc-production is the host project.

Your IT team has configured the firewall rules, subnets, and VPN gateway on the host project. The IT Team needs to enable the Engineering Group to attach a Compute Engine instance to only the 10.1.1.0/24 subnet.

What should your team grant to Engineering Group A to meet this requirement? (Select One)

A. Compute Network User Role at the host project level.
B. Compute Network User Role at the subnet level.
C. Compute Shared VPC Admin Role at the host project level
D. Compute Shared VPC Admin Role at the service project level.

---

12. A customer has contacted you about migrating to Google Cloud. The customer would like to migrate their data from on premises as soon as possible. They don't have the budget to rewrite code, and they want the most direct route. What migration option should suggest to the customer? (Select One)

A. Lift and Shift
B. Improve and Move
C. Rip and Replace
D. None, since the customer is not cloud native ready.

---

13. What load balancer type is supported with Cloud Armor security policies? (Select One)

A. Regional SSL
B. HTTP(S) Only
C. HTTP(S) and SSL
D. SSL Proxy, HTTP(S) and SSL

---

14. When creating a project in Google Cloud it is important to understand quotas limits of a project. By default you can create up to _____ networks per project. (Select One)

A. 10
B. 100
C. 5
D. 50

---

15. Your company is currently using Google Kubernetes Engine for its container cluster orchestration. Google Cloud and the customer have responsibilities in a Share Responsibility Model.

Which of the following would Google responsibilities in this shared model for managing GKE? (Select Three)

A. Control Plane
B. Pods
C. Master Nodes
D. Worker Nodes
E. Containers
F. Etcd

---

16. Your currently using Google Kubernetes Engine(GKE)you're your container deployments on Google Cloud. Which of the following would be customer responsibilities for maintaining your cluster? (Select Two)

A. Maintain your workloads, including your application code, build files, container images, data, etc.
B. Monitor the cluster and applications and respond to any alerts and incidents.
C. Hardening and patching Kubernetes node components your workloads run on.
D. Protecting the underlying infrastructure, including hardware, firmware, kernel, OS, storage, network, etc.

---

17. Cloud Data Loss Prevention (DLP) is a fully managed service designed to help discover, classify, and protect the most sensitive data. DLP provides three key features (Select Two)

A. Classification
B. De-Identification
C. De-classification

D. Reinspection

---

18. You want to deploy a new cluster in GKE and now want to restrict specific pod-to-pod communication in the cluster. How would you accomplish this using the tools in GKE and GCP? (Select One)

A. Firewall Rules
B. Network Policies
C. Namespace
D. Kube-proxy
E. Binary Authorization

---

19. A DDoS attack is an attempt to render the service or application unavailable to the end-users using multiple sources. In Google Cloud we mitigate these DDoS attacks with best practices. Which of the following are best practices according to Google? (Select Three)

A. Isolate internal traffic from the external world.
B. Enabling Proxy-based load balancing
C. Shutdown your services that are threatened
D. Turn off API-Rate Limiting
E. Scale to absorb the attack
F. Contact Google support to resolve

---

20. You have been contacted by the enterprise support team which has told you there have reports of significant latency at specific times for an application running on GCP. They would like you to review the issue and provide them insight into why the application is latent at specific times? What Google Cloud service could you use to inspect latency data that has been collected in near real time? (Select One)

A. Cloud Debug

B. Cloud Trace
C. VPC Trace Logs
D. Cloud Profiler

---

21. The Organization resource is the root node in the Google Cloud Platform hierarchy and is the hierarchical super node of projects. What are the types of customers an organization resource is available for? (Select Two)

A. Google Workspace
B. Gmail
C. Google for Education
D. Cloud Identity

---

22 . In GCP there are two types of managed instance groups.

(Select Two)

A. Zonal
B. Regional
C. Global
D. GDPR

---

23. Which of the following features are supported by GCP Cloud Storage? (Select Two)

A. Object Versioning
B. Object Lifecycle Management
C. Object Analysis Management
D. Object Antivirus Scanning

---

24. Which of the following Google Cloud service would you select for an organization to define a fine-grained attribute-based access control for projects and resources. (Select One)

A. Network Policies
B. Access Context Manager
C. JSON or XML
D. JSON or .Doc

---

25. Which of the following is not possible using basic roles in GCP? (Select One)

A. Allows a user access to view all datasets in a project, but not run queries on them.
B. Allows Development owner access and Production editor access for all datasets in a project.
C. Allows a user access to view all datasets in a project only

---

26. You're currently reviewing your BigQuery security permissions and want to confirm at what resource level you can grant access around to a user? Which of following are Google BigQuery resource levels? (Select Three)

A. Organization or project level
B. Table or view level
C. API Level
D. Dataset level
E. Query level

---

27. You're currently considering moving your on-premises CI pipeline from on premises to Google Cloud Platform. You would like to have code maintained in a private Git repository which is hosted on the Google Cloud Platform. What service would you choose? (Select One)

A. Container Registry
B. Kubernetes Engine
C. Cloud Source Repositories
D. Cloud Build
E. Cloud Run

---

28. Your development team is working on application that will be accessing GCP services from on premises. You need to provide the development team a solution that will intercepts the web requests sent to the application, authenticates the user making the request using the Google Identity Service, and only lets the requests through if they come from an authorized user.

What would be the best solution for the development team? (Select One)

A. Use SSL Proxy to handle the incoming requests to use a JSON Web Tokens (JWT) as signed headers to make sure that a request to the app is authorized.
B. Use Identity-Aware Proxy (IAP) which can be configured to use JSON Web Tokens (JWT) as signed headers to make sure that a request to the app is authorized and doesn't bypass IAP
C. Use Identity and Access Management (IAM) to use groups for authorized users.
D. Use Cloud Armor which will provide protection to applications running behind an external HTTP(S) and TCP/SSL Proxy load balancer.

---

29. You have been contacted by your CIO to improve your application availability and recovery. You have decided to use instance groups by spreading your instances across three zones. What type of instance group do you select? (Select One)

A. Multi-Regional managed groups
B. Multi-Zonal managed groups
C. Regional managed groups
D. Zonal managed groups

---

30 Your developer lead has accidentally deleted a service account last week, which now has clearly caused the application functionality to degrade. You want to recover the application as quickly as possible without compromising security. What should you do? (Select One)

A. Clone another service account and provide for the proper permissions.
B. Use the undelete command for recovery.
C. Create a new service account and recover the data from a backup.
D. Contact Google Support to assist since these accounts are managed by Google.

---

31. You have been hired as GCP Security consultant by a new company to the world of GCP. They would like to synchronize all accounts that have an email address from their LDAP directory and map them to Google Cloud. What should you do in this case?

Select the best answer. (Select One)

A. Configure Google Cloud Directory (Sync) to provide a one-way sync by searching LDAP rules and map them to Google Cloud IAM with a two-way sync.
B. Configure Google Cloud Directory (Sync) to provide a one-way sync by searching LDAP rules and map them to Google Cloud IAM with a one-way sync.

C. Configure IAM API to interface with your on-premises LDAP services and then synchronize your groups.
D. Configure IAM API to use a 3rd party solution such as OKTA to perform the one way.

---

32. You're currently working with several contractors. They are using Cloud Storage buckets for dropping files for review and your company's approval. Which of the following should you NOT perform? (Select One)

A. Create a separate bucket for each vendor.
B. Give each vendor the roles/storage.objectAdmin for their respective bucket.
C. Give each vendor the roles/owner for their respective bucket.
D. Give them a link to their bucket, which has the format:

console.cloud.google.com/storage/browser/[BUCKET_NAME]

---

33. When learning about external IP addresses in GCP which of the following is NOT correct? (Select One)

A. Assigned from a pool
B. Assigned from an internal static address
C. Assigned from an external static address
D. VM does not know its address but its mapped internally to an internal IP

---

34. Your users are only uploading resources (writing) to an access-controlled bucket. You can use the _____functionality of Cloud Storage to require only one signed URL. (Select One)

A. Resumable uploads
B. Controlled uploads
C. Authenticated uploads

D. Signed uploads by URL

---

35. VPC Network Peering allows you to peer two VPC networks so that the VMs in the two networks can communicate via internal, private IP addresses. This provides advantages since the organization is exposing its service to the public internet.

Which of the following is NOT true about VPC Network Peering? (Select One)

A. VPC Network Peering works with Compute Engine and App Engine Standard
B. Peered VPC networks remain administratively separate.
C. Each side of a peering association is set up independently.
D. A given VPC network can peer with multiple VPC networks
E. VPC Network Peering works with Compute Engine and App Engine Flexible

---

36. There has been a security threat that has been discovered and you believe there is a comprised service account key. What would be the next step(s) you would want to perform to determine which resources were created by the service account? (Select One)

A. Query Support Logs, identify user who deleted it.
B. Create a Dashboard in Cloud Operations and then import all the logs for that service account.
C. Review the VPC Trace logs and export to BigQuery for analysis.
D. Query the Admin Access Logs and review the activity
E. Query the Access Transparency Logs and contact support.

---

37. Your company is requesting a way to test user provisioning with Google services. They would like to have you manually provision users for testing or other purposes. What capability in GCP could you use to manually provision users for testing? (Select One)

A. Gmail Console
B. Google Workspace Admin Console
C. GCP Cloud Console
D. Open ID

---

38. Your business unit director has contacted you since one of the other company cloud administrators was fired from the company.

The director has requested that the administrators accounts are deprovisioned automatically from now on. What would do to accomplish this? (Select One)

A. Use Cloud Directory Sync and your LDAP server to provision and deprovision users from Cloud Identity.
B. Use Cloud Directory Sync and your LDAP server to delete from IAM user permissions from Cloud Identity
C. Use the Cloud SDK to remove the user from Cloud Identity and your LDAP servers.
D. Use the Cloud SDK to remove the user from Cloud IAM and your LDAP servers

---

39. What is the international compliance standard that provides guidelines for information security controls applicable to the provision and use of cloud services? (Select One)

A. ISO 27001
B. ISO 27002
C. ISO 27017
D. ISO 27000
E.

40. The maximum number of subnets in a project is how many? (Select One)

A. 10
B. 100
C. 125
D. 1250

---

41. What is the maximum size of a log entry with logging (Select One)

A. 128 KB
B. 256 KB
C. 512 KB
D. 127 KB

---

42. What does Cloud Logging in Google Cloud include as part of the service? (Select Three)

A. User Interface (Logs Viewer)
B. API for programmatic access
C. Storage for logs
D. Analytics Tools
E. Kubernetes Logging extensions.

---

43. What is the default retention period for Admin Activity Logs? (Select One)

A. 30 days
B. 400 days
C. 500 days
D. 31 days

44. Using gsutil you can download text files from a bucket by using what gsutil command? (Select One)

A. gsutil cp gs://my-bucket/*.files
B. gsutil dn gs://my-bucket/*.txt
C. gsutil copy gs://my-bucket/*.txt
D. gsutil cp gs://my-bucket/*.txt

---

45. You would like to obtain the current IAM Policy for a project called my-project test. What would be the correct syntax? (Select One)

A. gcloud set-iam-policy project my-project-test
B. gcloud projects get-iam-policy my-project-test
C. gcloud projects get-iam-policy --my-project-test
D. gcloud get-iam-policy my-project-test

---

46. Your customer requires that metrics from all applications be retained for 5 years for future analysis in possible legal proceedings. Which approach should you use? (Select One)

A. Configure Cloud Operations Monitoring for all Projects, and export to Cloud Storage.
B. Configure Cloud Operations Monitoring for all Projects with the default retention policies.
C. Configure Cloud Operations Monitoring for all Projects, and export to BigQuery.
D. Configure Cloud Operations Monitoring for all Projects, and export to Cloud Datastore

---

47. The _____resource represents the Access Control Lists (ACLs) for buckets within Google Cloud Storage. ACLs let you specify who has access to your data and to what extent. (Select One)

A. SetIAMPolicy
B. TestIAMPermissions
C. DefaultAccessControls
D. BucketAccessControls

---

48. How do you isolate VM systems within one project to guarantee that they can't communicate over the internal IP address? (Select One)

A. Place them in different zones
B. Place them in different networks
C. Place them in separate organizations
D. Place them in a separate project

---

49. Compute Engine blocks or restricts traffic through all the following ports/protocols between the Internet and virtual machines, and between two virtual machines when traffic is addressed to their external IP addresses through these ports (this also includes load-balanced addresses). These ports are permanently blocked; they cannot be opened using firewall rules. What ports are blocked in Compute Engine? (Select Three)

A. All outgoing traffic to port 25 (SMTP) is blocked.
B. All traffic coming from on premises
C. GRE traffic is blocked, even between VMs
D. Most outgoing traffic to port 465 or 587 (SMTP over SSL) is blocked, except for known Google IP addresses
E. All outgoing traffic to port 22 (SSH) is blocked.

50. Your business director has specifically requested to you to ensure that the deployment limit users with administrative privileges at the organization level.
Which two roles do you need to restrict? (Select One)

A. GKE Cluster Admin
B. Compute Admin
C. Organization Administrator
D. Super Admin
E. None of the above

GCP SECURITY ENGINEER PRACTICE EXAM ONE

50 QUESTIONS

WITH ANSWERS AND EXPLANATIONS

1. Your IT Team wants to centrally manage GCP IAM permissions from their on-premises Active Directory Service. Your IT team also needs to manage permissions by AD group membership.

What should your IT team do to meet these requirements? (Select One)

E. Configure SAML 2.0 (SSO) and them great a group in IAM.
F. Configure Cloud Identity and IAM to manage permissions from the on-premises AD Servers.
G. Configure Cloud Directory to synchronize groups and then set permissions to those groups.
H. Gcloud components install components kubectl

Correct Answer(s): C. To be able to keep using the existing identity management system, identities need to be synchronized between AD and GCP IAM. To do so google provides a tool called Cloud Directory Sync. This tool will read all identities in AD and replicate those within GCP.

Once the identities have been replicated then it's possible to apply IAM permissions on the groups. After that you will configure SAML so google can act as a service provider and either you ADFS or other third-party tools such as Okta will act as the identity provider. This way you effectively delegate the authentication from Google to something that is under your control.

Please review this page before the exam.

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

---

2. A recent software update to your enterprises e-commerce website that is running on Google Cloud has caused the website to crash for several hours.

Your CTO decides that all critical changes must now have a back-out/roll-back plan. The website is deployed on hundreds of virtual machines (VMs), and critical changes are frequent.

Which two actions should you take to implement the back-out/roll-back plan? (Select Two)

E. Use managed instance groups with the "update-instances" command when starting a rolling update
F. Enable object versioning on the website's static data files stored in Google Cloud Storage
G. Create a new instance template with applied fixes and roll out via A/B test
H. Use unmanaged instance groups with the "update-instances" command when starting a rolling update

Correct Answer(s): A, B. Use managed instance groups with the "update-instances" command when starting a rolling update

And Enable object versioning on the website's static data files stored in Google Cloud Storage
Explanation: Use managed instance groups to provide updates and object versioning will ensure that you can get back to the previous stable version.

Please review this page before the exam
https://cloud.google.com/compute/docs/instance-groups

---

3. A customer deploys an application to App Engine and needs to check for Open Web Application Security Project (OWASP) vulnerabilities. Which service should be used to accomplish this? (Select One)

E. Cloud Armor
F. Binary Authorization
G. Cloud Security Scanner
H. Forseti Security

Correct Answer(s): C. Cloud Security Scanner
Explanation: Web Security Scanner identifies security vulnerabilities in your App Engine, Google Kubernetes Engine (GKE), and Compute Engine web applications. It crawls your application, following all links within the scope of your starting URLs, and attempts to exercise as many user inputs and event handlers as possible.
Currently, Web Security Scanner only supports public URLs and IPs that aren't behind a firewall. Web Security Scanner currently supports the App Engine standard environment and App Engine flexible environments, Compute Engine instances, and GKE resources.

Please review this page before the exam

https://cloud.google.com/security-command-center/docs/concepts-web-security-scanner-overview

4. Your customer has asked you to follow Google-recommended practices to leverage envelope encryption and encrypt data at the application layer. What should you do? (Select One)

E. Generate a data encryption key (DEK) remotely to encrypt the data, and then generate a new key encryption key (KEK) in Cloud KMS to encrypt the DEK. Store both these keys and your plaintext that have been created on your USB drive.

F. Generate a data encryption key (DEK) locally to encrypt the data, and then generate a new key encryption key (KEK) in Cloud KMS to encrypt the DEK. Store the encrypted data and the encrypted DEK.

G. Generate a data encryption key (DEK) locally to encrypt the data, and then generate a new key encryption key (KEK) in Cloud KMS to encrypt the DEK. Store the encrypted data and the wrapped KEK.

H. Generate a data encryption key (DEK) locally to encrypt the data, and then generate a new data encryption key (DEK) in Cloud KMS to encrypt the DEK. Store the encrypted data and the encrypted KEK locally.

Correct Answer(s): B. Generate a data encryption key (DEK) locally to encrypt the data, and then generate a new key encryption key (KEK) in Cloud KMS to encrypt the DEK. Store the encrypted data and the encrypted DEK.

Explanation: A DEK should be generated locally and always encrypted at rest. To encrypt the DEK you must use KEK, which is generated and stored centrally in KMS. Therefore, both the data and the encrypted DEK (using the KEK) should be stored at rest. To encrypt the data using envelope encryption:

1. Generate a DEK locally. You could do this with an open-source library such as OpenSSL, specifying a cipher type and a password from which to generate the key. You can also specify a salt and digest to use, if desired.
2. Use this DEK locally to encrypt your data.

3. Generate a new key in Cloud KMS, or use an existing key, which will act as the KEK. Use this key to encrypt (wrap) the DEK.

4. Store the encrypted data and the wrapped DEK.

Please review this page before the exam.

https://cloud.google.com/kms/docs/envelope-encryption

---

5. You're currently setting up your VMs on Compute Engine and you were asked to install the monitoring agent for Cloud Operations. What is the agent called you will install on the VM? (Select One)

E. Cloud Operations agent
F. Cloud Monitoring agent
G. Collectd Agent
H. Stastd Agent

Correct Answer(s): B. Cloud Monitoring Agent
Explanation: The Cloud Monitoring agent is a collectd-based daemon that gathers system and application metrics from virtual machine instances and sends them to Cloud Operations Monitoring.

Please review this page before the exam.

https://cloud.google.com/monitoring/agent/monitoring

---

6. Cloud KMS stores keys in a key hierarchy designed for ease, with access to resources in the key hierarchy governed by Identity and Access Management. Which of the following answers shows the correct level and order of a Cloud KMS key hierarchy? (Select One)

E. Key Ring, Key, Key Version
F. Key Ring, Key Version, Key
G. Key Version, Key, Key Ring
H. Key Version, Key Ring, Key

Correct Answer(s): A. Key Ring, Key, Key Version
Explanation: A key ring organizes keys in a specific Google Cloud location and allows you to manage access control on groups of keys. Cloud KMS stores keys in a key hierarchy designed for ease, with access to resources in the key hierarchy governed by Identity and Access Management. The following shows the main levels of a Cloud KMS key hierarchy:

Please review this page before the exam.
https://cloud.google.com/kms/docs/envelope-encryption
And also, please review this page before the exam
https://cloud.google.com/kms/docs/resource-hierarchy

---

7. You have been invited to a meeting with your enterprise lead architect. The enterprise architect is requesting help on how he would be able to reliably deliver Cloud Operations logs from GCP to their on-premises SIEM system? He also stated he would the simplest option. (Select One)

E. Build a custom connector for the SIEM to query for all the logs from the provided Google Cloud API's.
F. Send your logs to the SIEM system using syslog.
G. Configure an organization log sink which would export to a Cloud/Pub topic. This could be sent to their SIEM via Cloud DataFlow template.
H. Configure every project to have a log sink which would export to a Cloud/Pub topic. This could be sent to their SIEM via Cloud DataFlow.

Correct Answer(s): C. Configure an organization log sink which would export to a Cloud/Pub topic. This could be sent to their SIEM via Cloud DataFlow.
Explanation: C is the most efficient option. Google allows to create an organization log sink and export the logs to cloud sub/pub. From there it's possible to use Dataflow to send data to a SIEM.
Note: If you are using Splunk as your SIEM, there is already a default Dataflow template created by google.

Please review this page before the exam.

https://cloud.google.com/dataflow/docs/guides/templates/provided-streaming#pubsub-to-splunk

---

8. You have been asked to meet PCI DSS requirements with a customer's application on GCP. The customer wants to ensure that all outbound traffic is authorized. Which following two cloud offerings will meet this requirement without introducing additional compensating controls? (Select Two)

F. Compute Engine
G. Cloud Run
H. Cloud Functions

I. Kubernetes Engine
J. App Engine

Correct Answer(s): A, D. Compute Engine, Kubernetes Engine
Explanation: The PCI Data Security Standard, created by the PCI Security Standards Council, is an information security standard for businesses that handle payment card (both credit and debit) information. The PCI Security Standards Council includes every major payment card company. Businesses that take Visa, MasterCard, Discover, American Express, or JCB are expected to comply with PCI DSS, and they can be fined or penalized if they don't. According to PCI DSS and as per requirements 1.2.1 and 1.3.4, you must ensure that all outbound traffic is authorized.

There are only two google services that allow to filter egress traffic and those are Google Compute Engine and Kubernetes Engine. Regarding App Engine, Cloud Functions, ingress rules are available, but egress ones are not, so it's not a valid option.

Please Review this page before the exam.

https://cloud.google.com/solutions/pci-dss-compliance-in-gcp

---

9 Your considering placing your Infrastructure as code processes on Cloud Deployment Manager. What could be considered a security risk of doing this? (Select One)

E. Cloud Deployment Manager requires a Google APIs service account to run.
F. Cloud Deployment Manager APIs could be deprecated in the future which pose risks.
G. Cloud Deployment Manager can be used to permanently delete cloud resources.
H. Cloud Deployment Manager takes some training to use.

Correct Answer(s): B. Cloud Deployment Manager APIs could be deprecated in the future which pose risks.
Explanation: APIs could be deprecated in the future.

APIs of course take maintenance to be updated and checked. Older unsupported APIs could pose risks. Other choices would likely not be a risk.

Please review this page before the exam.

https://cloud.google.com/deployment-manager/docs#docs

---

10 When working with agents in a support center via online chat, an organization's customers often share pictures of their documents with personally identifiable information (PII).

The organization that owns the support center is concerned that the PII is being stored in their databases as part of the regular chat logs, they retain for review by internal or external analysts for customer service trend analysis.

Which Google Cloud solution should the organization use to help resolve this concern for the customer while still maintaining data utility? (Select One)

E. Use image inspection and redaction of DLP to redact PII data from the images before storing them to be analysed.
F. Use Object Lifecycle Management to validate all records with PII data are deleted
G. Use the Cloud Key Management Service (KMS) to encrypt your PII data that will be shared and then stored.
H. Use the generalization feature Data Loss Prevention (DLP) to redact everything that is not allowed to be stored.

Correct Answer(s): A. Use image inspection and redaction of DLP to redact PII data from the images before storing them to be analysed

Explanation: The only valid option is to use the DLP API to redact PII from images before storing it for later analysis.

Please review this page before the exam.

https://cloud.google.com/dlp/docs

---

11. Your IT team sets up a Shared VPC Network where project my-vpc-production is the host project.

Your IT team has configured the firewall rules, subnets, and VPN gateway on the host project. The IT Team needs to enable the Engineering Group to attach a Compute Engine instance to only the 10.1.1.0/24 subnet.

What should your team grant to Engineering Group A to meet this requirement? (Select One)

E. Compute Network User Role at the host project level.
F. Compute Network User Role at the subnet level.
G. Compute Shared VPC Admin Role at the host project level
H. Compute Shared VPC Admin Role at the service project level.

Correct Answer(s): B. Compute Network User Role at the subnet level.

Explanation. A is incorrect as it would grant permissions to attach instances to all subnets in the host project. C is incorrect as it will grant to many permissions to the team and violate the principle of least privilege. Option D is incorrect as the permissions need to be granted at the host project level. Therefore, the correct answer is B.

Please reference this page before the exam.

https://cloud.google.com/vpc/docs/shared-vpc#svc_proj_admins

This YouTube video also provides a great walkthrough https://www.youtube.com/watch?v=LxDHd0MsFXI

---

12. A customer has contacted you about migrating to Google Cloud. The customer would like to migrate their data from on premises as soon as possible. They don't have the budget to rewrite code, and they want the most direct route. What migration option should suggest to the customer? (Select One)

E. Lift and Shift
F. Improve and Move
G. Rip and Replace
H. None, since the customer is not cloud native ready.

Correct Answer(s): A. Lift and Shift

Explanation. With Lift and Shift migrations, the customer could move workloads from a source environment to a target environment with few or no modifications or refactoring.

Please review this page before the exam.

https://cloud.google.com/architecture/migration-to-gcp-getting-started

---

13. What load balancer type is supported with Cloud Armor security policies? (Select One)

E. Regional SSL
F. HTTP(S) Only
G. HTTP(S) and SSL
H. SSL Proxy, HTTP(S) and SSL

Correct Answer(s): B: HTTP(S) Only

Explanation. Google Cloud Armor security policies protect your application by providing Layer 7 filtering and by scrubbing incoming requests for common web attacks or other Layer 7 attributes to potentially block traffic before it reaches your load balanced backend services or backend buckets. Each security policy is made up of a set of rules that filter traffic based on conditions such as an incoming request's IP address, IP range, region code, or request headers.

Google Cloud Armor security policies are available only for backend services behind an external HTTP(S) load balancer. The load balancer can be in Premium Tier or Standard Tier.

Google Cloud Armor security policies and IP DENY lists and ALLOW lists are available only for HTTP(S) load balancing.

Please refer to this page before the exam.

https://cloud.google.com/armor/docs/security-policy-overview

---

14. When creating a project in Google Cloud it is important to understand quotas limits of a project. By default you can create up to _____ networks per project. (Select One)

E. 10
F. 100
G. 5
H. 50

Correct Answer(s): C. 5

Explanation. By default ,the limit is 5 per project. You can contact support to have this adjusted as needed. The exam has a few trivia around projects and quotas.

https://cloud.google.com/vpc/docs/using-vpc

---

15. Your company is currently using Google Kubernetes Engine for its container cluster orchestration. Google Cloud and the customer have responsibilities in a Share Responsibility Model.

Which of the following would Google responsibilities in this shared model for managing GKE? (Select Three)

G. Control Plane
H. Pods
I. Master Nodes
J. Worker Nodes
K. Containers
L. Etcd

Correct Answer(s): A,C, F. Control Plane, Master Nodes and Virtual Machine Hosts

Explanation: In GKE, the Kubernetes control plane components are managed and maintained by Google. The control plane components host the software that runs the Kubernetes control plane, including the API server, scheduler, controller manager and the etcd database where your Kubernetes configuration is persisted.

Please review this page before the exam.

https://cloud.google.com/kubernetes-engine/docs/concepts/security-overview

Please review this page before the exam.

https://cloud.google.com/kubernetes-engine/docs/concepts/shared-responsibility

---

16. Your currently using Google Kubernetes Engine(GKE)you're your container deployments on Google Cloud. Which of the following would be customer responsibilities for maintaining your cluster? (Select Two)

E. Maintain your workloads, including your application code, build files, container images, data, etc.
F. Monitor the cluster and applications and respond to any alerts and incidents.
G. Hardening and patching Kubernetes node components your workloads run on.
H. Protecting the underlying infrastructure, including hardware, firmware, kernel, OS, storage, network, etc.

Correct Answer(s): A,B. Maintain your workloads, including your application code, build files, container images, data. Monitor the cluster and applications and respond to any alerts and incidents.

Explanation: Google's responsibilities and the Customers responsibilities are clearly defined here in the document below. Effectively, if it has to do with the control plane, hardware, software, threats to nodes, etc it is Google's responsibility. The customers responsibilities focus on the day-to-day management of their clusters.

Please review this page before the exam.

https://cloud.google.com/kubernetes-engine/docs/concepts/shared-responsibility

---

17. Cloud Data Loss Prevention (DLP) is a fully managed service designed to help discover, classify, and protect the most sensitive data. DLP provides three key features (Select Two)

E. Classification
F. De-Identification
G. De-classification
H. Reinspection

Correct Answer(s): A, B, E. Classification. De-classification and Inspection

Explanation: Classification is the process to inspect the data and know what data we have, how sensitive it is, and the likelihood. Inspection and classification happen here.

De-identification is the process of removing, masking, replacing information from data.

Please review this page before the exam

https://cloud.google.com/dlp/docs

---

18. You want to deploy a new cluster in GKE and now want to restrict specific pod-to-pod communication in the cluster. How would you accomplish this using the tools in GKE and GCP? (Select One)

F. Firewall Rules

G. Network Policies
H. Namespace
I. Kube-proxy
J. Binary Authorization

Correct Answer(s): B. Network Policies

Explanation: You can use GKE's network policy enforcement to control the communication between your cluster's Pods and Services. You define a network policy by using the Kubernetes Network Policy API to create Pod-level firewall rules. These firewall rules determine which Pods and Services can access one another inside your cluster. The default behaviour is that all pod-to-pod communication is always open. To segment your network, you need to enforce pod-level networking policies.

https://cloud.google.com/kubernetes-engine/docs/how-to/network-policy

---

19. A DDoS attack is an attempt to render the service or application unavailable to the end-users using multiple sources. In Google Cloud we mitigate these DDoS attacks with best practices. Which of the following are best practices according to Google? (Select Three)

G. Isolate internal traffic from the external world.
H. Enabling Proxy-based load balancing
I. Shutdown your services that are threatened
J. Turn off API-Rate Limiting
K. Scale to absorb the attack
L. Contact Google support to resolve

Correct Answer(s): A, B and E: Isolate internal traffic from the external world. Enabling Proxy-based load balancing and Scale to absorb attack.

Explanation: Google has clearly specified best practices in the document below. This Best Practices for DDoS Protection and Mitigation document is a must read. You can expect a few questions from this document so be ready.

https://cloud.google.com/files/GCPDDoSprotection-04122016.pdf

---

20. You have been contacted by the enterprise support team which has told you there have reports of significant latency at specific times for an application running on GCP. They would like you to review the issue and provide them insight into why the application is latent at specific times? What Google Cloud service could you use to inspect latency data that has been collected in near real time? (Select One)

E. Cloud Debug
F. Cloud Trace
G. VPC Trace Logs
H. Cloud Profiler

Correct Answer(s): A: Cloud Trace

Explanation: Cloud Trace formerly Stackdriver Trace is a distributed tracing system that collects latency data from your applications and displays it in the Google Cloud Console. You can track how requests propagate through your application and receive detailed near real-time performance insights. Cloud Trace automatically analyses all your application's traces to generate in-depth latency reports to surface performance degradations, and can capture traces from all your VMs, containers, or App Engine projects.

Please review this page before the exam

https://cloud.google.com/trace

---

21. The Organization resource is the root node in the Google Cloud Platform hierarchy and is the hierarchical super node of projects. What are the types of customers an organization resource is available for? (Select Two)

E. Google Workspace
F. Gmail
G. Google for Education
H. Cloud Identity

Correct Answer(s): A and D: Gsuite and Cloud Identity

Explanation: An Organization resource is available for G Suite and Cloud Identity customers. Organizations are confusing at first, but for this exam we must understand the GCP cloud hierarchy details and what role an Org Administrator is about as well. https://cloud.google.com/resource-manager/docs/creating-managing-organization

---

22 . In GCP there are two types of managed instance groups.

(Select Two)

E. Zonal
F. Regional
G. Global
H. GDPR

Correct Answer(s): A, B Zonal and Regional

Explanation: You can create two types of managed instance groups: A zonal managed instance group, which contains instances from the same zone. A regional managed instance group, which contains instances from multiple zones across the same region. Lastly, don't confused over an unmanaged instance group.

https://cloud.google.com/compute/docs/instance-groups/

---

23. Which of the following features are supported by GCP Cloud Storage? (Select Two)

E. Object Versioning
F. Object Lifecycle Management
G. Object Analysis Management
H. Object Antivirus Scanning

Correct Answer(s): A. Object Versioning and Object Lifecycle Management

Explanation: Object Lifecycle and Object Versioning
https://cloud.google.com/storage/docs/lifecycle

---

24. Which of the following Google Cloud service would you select for an organization to define a fine-grained attribute-based access control for projects and resources. (Select One)

E. Network Policies
F. Access Context Manager
G. JSON or XML
H. JSON or .Doc

Correct Answer(s): A: Access Context Manager

Explanation: Access Context Manager allows organization administrators to define fine-grained, attribute-based access control for projects and resources. Access Context Manager allows you to reduce the size of the privileged network and move to a model where endpoints do not carry ambient authority based on the network. Instead, you can grant access based on the context of the request, such as device type, user identity, and more, while still checking for corporate network access when necessary.

It provides the following benefits. 1 Helps mitigate and prevent data exfiltration. 2. It helps reduce the size of the privileged network and move to a model where endpoints do not carry ambient authority based on the network. 3. It helps define desired rules and policy but isn't responsible for policy enforcement. Theses Attribute policies are configured and enforced across various points, such as VPC Service Controls.

Please review the following page before the exam

https://cloud.google.com/access-context-manager/docs/overview

---

25. Which of the following is not possible using basic roles in GCP? (Select One)

D. Allows a user access to view all datasets in a project, but not run queries on them.
E. Allows Development owner access and Production editor access for all datasets in a project.
F. Allows a user access to view all datasets in a project only
G. None of the above

Correct Answer(s): A: Allows a user access to view all datasets in a project, but not run queries on them.

Explanation: Basic roles can be used to give owner, editor, or viewer access to a user or group, but they can't be used to separate data access permissions from job-running permissions. Basic Roles were created before IAM was released and therefore does not support granularity.

Please refer to this page before the exam.
https://cloud.google.com/bigquery/docs/access-control#primitive_iam_roles

---

26. You're currently reviewing your BigQuery security permissions and want to confirm at what resource level you can grant access around to a user? Which of following are Google BigQuery resource levels? (Select Three)

F. Organization or project level
G. Table or view level
H. API Level
I. Dataset level
J. Query level

Correct Answer(s): A, B, D at the Organization level or project level, Table or view level and Dataset level

Explanation: To grant access to a BigQuery resource, assign one or more roles to a user, group, or service account. You can grant access at the following BigQuery resource levels:

- organization or Google Cloud project level
- dataset level
- table or view level

Please review this page before the exam.

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

---

27. You're currently considering moving your on-premises CI pipeline from on premises to Google Cloud Platform. You would like to have code maintained in a private Git repository which is hosted on the Google Cloud Platform. What service would you choose? (Select One)

F. Container Registry
G. Kubernetes Engine
H. Cloud Source Repositories
I. Cloud Build
J. Cloud Run

Correct Answer(s): C. Cloud Source Repositories

Explanation: Cloud Source Repositories is a secure hosted private Git on Google Cloud.

https://cloud.google.com/source-repositories/

---

28. Your development team is working on application that will be accessing GCP services from on premises. You need to provide the development team a solution that will intercepts the web requests sent to the application, authenticates the user making the request using the Google Identity Service, and only lets the requests through if they come from an authorized user.

What would be the best solution for the development team? (Select One)

E. Use SSL Proxy to handle the incoming requests to use a JSON Web Tokens (JWT) as signed headers to make sure that a request to the app is authorized.
F. Use Identity-Aware Proxy (IAP) which can be configured to use JSON Web Tokens (JWT) as signed headers to make sure that a request to the app is authorized and doesn't bypass IAP
G. Use Identity and Access Management (IAM) to use groups for authorized users.
H. Use Cloud Armor which will provide protection to applications running behind an external HTTP(S) and TCP/SSL Proxy load balancer.

Correct Answer(s): C. Identity-Aware Proxy IAP allows managing access to HTTP-based apps both on Google Cloud and outside of Google Cloud.

Identity-Aware Proxy IAP intercepts the web requests sent to the application, authenticates the user making the request using the Google Identity Service, and only lets the requests through if they come from an authorized user. In addition, it can modify the request headers to include information about the authenticated user.

Identity-Aware Proxy IAP helps establish a central authorization layer for applications accessed by HTTPS to use an application-level access control model instead of relying on network-level firewalls.

IAP uses Google identities and IAM and can leverage external identity providers as well like OAuth with Facebook, GitHub, Microsoft, SAML, etc.

Identity-Aware Proxy (IAP) can be configured to use JSON Web Tokens (JWT) as signed headers to make sure that a request to the app is authorized and doesn't bypass IAP

Please reference this page before exam.

https://cloud.google.com/iap/docs/concepts-overview

Please reference this page before exam

https://cloud.google.com/iap/docs/signed-headers-howto

---

29. You have been contacted by your CIO to improve your application availability and recovery. You have decided to use instance groups by spreading your instances across three zones. What type of instance group do you select? (Select One)

E. Multi-Regional managed groups
F. Multi-Zonal managed groups
G. Regional managed groups
H. Zonal managed groups

Correct Answer(s): A. Multi-Regional managed groups

Explanation: An instance group is a collection of virtual machines (VM) instances that you can manage as a single entity. There are two types Managed and Unmanaged Instance Groups. Instance Groups can be a way to provide High Availability, Scalability, etc.

Please reference this page before the exam.

https://cloud.google.com/compute/docs/instance-groups#managed_instance_groups

---

30 Your developer lead has accidentally deleted a service account last week, which now has clearly caused the application functionality to degrade. You want to recover the application as quickly as possible without compromising security. What should you do? (Select One)

E. Clone another service account and provide for the proper permissions.
F. Use the undelete command for recovery.
G. Create a new service account and recover the data from a backup.
H. Contact Google Support to assist since these accounts are managed by Google.

Correct Answer(s): B. Use the undelete command for recovery.

Explanation: Being that the service account deletion was under 30 days ago the simplest way to fix this problem is to undelete a service account using the gcloud beta iam service-accounts undelete <account-id>.

After 30 days, IAM permanently removes the service account. Google Cloud cannot recover the service account after it is permanently removed, even if you file a support request. The other options would either violate best practices or do not make sense.

https://cloud.google.com/iam/docs/creating-managing-service-accounts#undeleting_a_service_account

---

31. You have been hired as GCP Security consultant by a new company to the world of GCP. They would like to synchronize all accounts that have an email address from their LDAP directory and map them to Google Cloud. What should you do in this case?

Select the best answer. (Select One)

E. Configure Google Cloud Directory (Sync) to provide a one-way sync by searching LDAP rules and map them to Google Cloud IAM with a two-way sync.
F. Configure Google Cloud Directory (Sync) to provide a one-way sync by searching LDAP rules and map them to Google Cloud IAM with a one-way sync.
G. Configure IAM API to interface with your on-premises LDAP services and then synchronize your groups.
H. Configure IAM API to use a 3rd party solution such as OKTA to perform the one way.

Correct Answer(s): B. Configure Google Cloud Directory (Sync) to provide a one-way sync by searching LDAP rules and map them to Google Cloud IAM with a one-way sync.

Explanation: You can use LDAP search rules to synchronize data from your LDAP directory server to your Google Account with Google Cloud Directory Sync (GCDS). Data that matches the search rule is synchronized to your Google Account. Data that doesn't match the search rule is removed.

Please review this link before the exam.

https://support.google.com/a/answer/6126589?hl=en

Please review this link before the exam.

https://cloud.google.com/architecture/identity/federating-gcp-with-active-directory-introduction

---

32. You're currently working with several contractors. They are using Cloud Storage buckets for dropping files for review and your company's approval. Which of the following should you NOT perform? (Select One)

E. Create a separate bucket for each vendor.
F. Give each vendor the roles/storage.objectAdmin for their respective bucket.
G. Give each vendor the roles/owner for their respective bucket.
H. Give them a link to their bucket, which has the format:

console.cloud.google.com/storage/browser/[BUCKET_NAME]

Correct Answer(s): C. Give each vendor the roles/owner for their respective bucket.

Explanation: Now you would almost never give temporary users, partners, or non-employee owner rights. This is a best practice

https://cloud.google.com/storage/docs/collaboration

---

33. When learning about external IP addresses in GCP which of the following is NOT correct? (Select One)

E. Assigned from a pool
F. Assigned from an internal static address
G. Assigned from an external static address
H. VM does not know its address but its mapped internally to an internal IP

Correct Answer(s): D. VM does not know its address but its mapped internally to an internal IP

Explanation: A static external IP address is the IP address that is reserved for your project until you decide to release it. If you have an IP address that your customers or users rely on to access your service, you can reserve that IP address so that only your project can use it. You can also promote an ephemeral external IP address to a static external IP address.

You can reserve two types of external IP addresses:

A regional IP address that can be used by VM instances with one or more network interfaces or by regional load balancers.

A global IP address which can be used for global load balancers.

Please review this page before the exam.

https://cloud.google.com/compute/docs/ip-addresses/reserve-static-external-ip-address

---

34. Your users are only uploading resources (writing) to an access-controlled bucket. You can use the _____functionality of Cloud Storage to require only one signed URL. (Select One)

E. Resumable uploads
F. Controlled uploads
G. Authenticated uploads
H. Signed uploads by URL

Correct Answer(s): D. Signed uploads by URL

Explanation: If your users are only uploading resources (writing) to an access-controlled bucket, you can use the resumable uploads functionality of Cloud Storage to require only one signed URL.

This signed URL is part of the initial POST request, during which no data is uploaded.

https://cloud.google.com/storage/docs/access-control/signed-urls

35. VPC Network Peering allows you to peer two VPC networks so that the VMs in the two networks can communicate via internal, private IP addresses. This provides advantages since the organization is exposing its service to the public internet.

Which of the following is NOT true about VPC Network Peering? (Select One)

F. VPC Network Peering works with Compute Engine and App Engine Standard
G. Peered VPC networks remain administratively separate.
H. Each side of a peering association is set up independently.
I. A given VPC network can peer with multiple VPC networks
J. VPC Network Peering works with Compute Engine and App Engine Flexible

Correct Answer(s): A .VPC Network Peering works with Compute Engine and App Engine Standard

Explanation: Does not support App Engine Standard.

There's a lot "Key properties" here with a VPC Network Peering

Please review this page before the exam.

https://cloud.google.com/vpc/docs/vpc-peering

---

36. There has been a security threat that has been discovered and you believe there is a comprised service account key. What would be the next step(s) you would want to perform to determine which resources were created by the service account? (Select One)

F. Query Support Logs, identify user who deleted it.
G. Create a Dashboard in Cloud Operations and then import all the logs for that service account.
H. Review the VPC Trace logs and export to BigQuery for analysis.

I. Query the Admin Access Logs and review the activity
J. Query the Access Transparency Logs and contact support.

Correct Answer(s): D. Query the Admin Access Logs

Explanation: The Admin Access Logs allow auditing the creation of new resources as well as the following:

- Updating/patching resources
- Setting/changing metadata
- Setting/changing tags
- Setting/changing labels
- Setting/changing permissions
- Setting/changing any properties of a resource

Let's not confuse Access Transparency logs, which provides you with logs that capture the actions Google personnel take when accessing your content.

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

---

37. Your company is requesting a way to test user provisioning with Google services. They would like to have you manually provision users for testing or other purposes. What capability in GCP could you use to manually provision users for testing? (Select One)

E. Gmail Console
F. Google Workspace Admin Console
G. GCP Cloud Console
H. Open ID

Correct Answer(s): B Google Workspace Admin Control

Explanation: Workspace (formerly G Suite Admin Console) allows you to manually provision users for testing or other purposes, Cloud Platform administrators can provision users and their associations with groups and organizations manually by using the Google Workspace Admin Console.

https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations

---

38. Your business unit director has contacted you since one of the other company cloud administrators was fired from the company.

The director has requested that the administrators accounts are deprovisioned automatically from now on. What would do to accomplish this? (Select One)

E. Use Cloud Directory Sync and your LDAP server to provision and deprovision users from Cloud Identity.
F. Use Cloud Directory Sync and your LDAP server to delete from IAM user permissions from Cloud Identity
G. Use the Cloud SDK to remove the user from Cloud Identity and your LDAP servers.
H. Use the Cloud SDK to remove the user from Cloud IAM and your LDAP servers

Correct Answer(s): A. Use Cloud Directory Sync and your LDAP server to provision and deprovision users from Cloud Identity

Explanation: Cloud Directory Sync can be used to perform changes in the directory service. These changes are automatically replicated to Cloud identity. When someone leaves the company his/her account is automatically removed blocking all access to GCP resources.

Please review this page before the exam.

https://cloud.google.com/identity/solutions/automate-user-provisioning#cloud_identity_automated_provisioning

---

39. What is the international compliance standard that provides guidelines for information security controls applicable to the provision and use of cloud services? (Select One)

F. ISO 27001

G. ISO 27002
H. ISO 27017
I. ISO 27000

Correct Answer(s): C. ISO 27017

Explanation: ISO/IEC 27017:2015 gives guidelines for information security controls applicable to the provision and use of cloud services by providing additional implementation guidance for relevant controls specified in ISO/IEC 27002 and additional controls with implementation guidance that specifically relate to cloud services

ISO 27001 outlines and provides the requirements for an information security management system (ISMS), specifies a set of best practices, and details the security controls that can help manage information risks but it's not specific to cloud. ISO 27002 is related to security controls to implement ISO 27001 and ISO 27018 relates to one of the most critical components of cloud privacy: the protection of Personally Identifiable Information (PII).

Please review the page below before the exam.

https://cloud.google.com/security/compliance/iso-27017

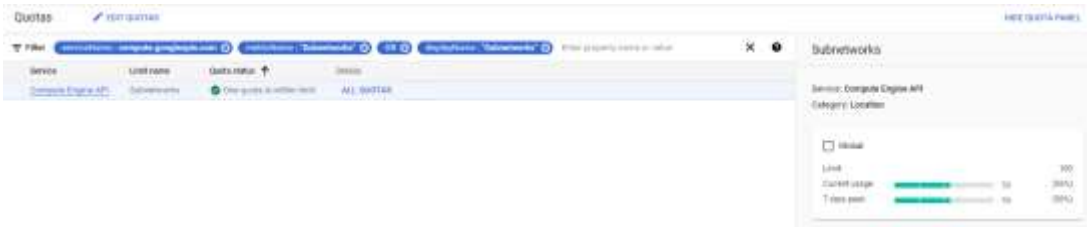
---

40. The maximum number of subnets in a project is how many? (Select One)

E. 10
F. 100
G. 125
H. 1250

Correct Answer(s): B. 100

Explanation: The default limit is 100. You can view this in your GCP project



Please review the following page before the exam.

https://cloud.google.com/vpc/docs/quota

---

41. What is the maximum size of a log entry with logging (Select One)

E. 128 KB
F. 256 KB
G. 512 KB
H. 127 KB

Correct Answer(s): B. 256

Explanation: Don't confuse the length of the logging retention or metrics for example. Note 256KB is approximate limit is based on internal data sizes, not the actual REST API request size.
https://cloud.google.com/logging/quotas

---

42. What does Cloud Logging in Google Cloud include as part of the service? (Select Three)

F. User Interface (Logs Viewer)
G. API for programmatic access
H. Storage for logs
I. Analytics Tools
J. Kubernetes Logging extensions.

Correct Answer(s): A, B, C. User Interface (Logs Viewer) B, API for programmatic access and C. Storage for logs.

Explanation: Cloud Logging is integrated with Stackdriver but there are no analytics or special extensions for Kubernetes. There are Kubernetes metrics used. Stackdriver is the default logging solution for clusters deployed on Google Kubernetes Engine. Stackdriver Logging is deployed to a new cluster by default unless you explicitly opt-out.

Please review the following page before the exam.

https://cloud.google.com/logging/docs/basic-concepts

---

43. What is the default retention period for Admin Activity Logs? (Select One)

E. 30 days
F. 400 days
G. 500 days
H. 31 days

Correct Answer(s): B: 400

Explanation: There is some trivia on the exam around logging. We need to know both 400 and 30 days. Cloud Logging retention periods apply to log buckets, regardless of which types of logs are included in the bucket or whether they were copied from another location

In the Operations section is a table that list there for Admin Activity, Data Access, etc. https://cloud.google.com/logging/quotas

---

44. Using gsutil you can download text files from a bucket by using what gsutil command? (Select One)

E. gsutil cp gs://my-bucket/*.files
F. gsutil dn gs://my-bucket/*.txt
G. gsutil copy gs://my-bucket/*.txt
H. gsutil cp gs://my-bucket/*.txt

Correct Answer(s): D gsutil cp gs://my-bucket/*.txt

Explanation: We will need to know a wide range of gcloud commands and gsutil is part of the objectives. Gsutil is used for managing Cloud Storage.

https://cloud.google.com/storage/docs/gsutil/commands/cp

---

45. You would like to obtain the current IAM Policy for a project called my-project test. What would be the correct syntax? (Select One)

E. gcloud set-iam-policy project my-project-test
F. gcloud projects get-iam-policy my-project-test
G. gcloud projects get-iam-policy --my-project-test
H. gcloud get-iam-policy my-project-test

Correct Answer(s): B: gcloud projects get-iam-policy my-project-test.

Explanation: We will need to know a few gcloud commands that are part of the objectives. gcloud projects get-iam-policy my-project-test
https://cloud.google.com/sdk/gcloud/reference/config/set

---

46. Your customer requires that metrics from all applications be retained for 5 years for future analysis in possible legal proceedings. Which approach should you use? (Select One)

E. Configure Cloud Operations Monitoring for all Projects, and export to Cloud Storage.
F. Configure Cloud Operations Monitoring for all Projects with the default retention policies.

G. Configure Cloud Operations Monitoring for all Projects, and export to BigQuery.
H. Configure Cloud Operations Monitoring for all Projects, and export to Cloud Datastore

Correct Answer(s): A : Configure Cloud Operations Monitoring for all Projects, and export to Cloud Storage.
Explanation: Cloud Storage is the only economical option and would meet compliance requirements if setup properly. The hint to use Cloud Storage was 5 years since it would likely be archive data.
Please reference the following page before the exam.

https://cloud.google.com/architecture/exporting-stackdriver-logging-for-compliance-requirements

---

47. The _____resource represents the Access Control Lists (ACLs) for buckets within Google Cloud Storage. ACLs let you specify who has access to your data and to what extent. (Select One)

E. SetIAMPolicy
F. TestIAMPermissions
G. DefaultAccessControls
H. BucketAccessControls

Correct Answer(s): D: BucketAccessControls
Explanation: Buckets contain objects which can be accessed by their own methods. In addition to the ACL property, buckets contain bucketAccessControls, for use in fine-grained manipulation of an existing bucket's access controls.

Please review this page before the exam.
https://cloud.google.com/storage/docs/json_api/v1/bucketAccessControls

---

48. How do you isolate VM systems within one project to guarantee that they can't communicate over the internal IP address? (Select One)

E. Place them in different zones
F. Place them in different networks
G. Place them in separate organizations
H. Place them in a separate project

Correct Answer(s): B: Place them in different networks
Explanation: Because these VMs are placed in a single Network, even though they are in different regions, they can still communicate through GCP's internal global network.

Each VM instance in GCP will have an internal IP address and typically an external IP address. The internal IP address is used to communicate between instances in the same VPC network, while the external IP address is used to communicate with instances in other networks or the Internet. These IP addresses are ephemeral by default but can be statically assigned.

Internal IPs are allocated to instances from the subnet's IP range via DHCP. This means the IPs are ephemeral and will be released if the instance is deleted.

Conventionally, some enterprise networks are separated into many small address ranges for a variety of reasons. For example, this might have been done to identify or isolate an application or keep a small broadcast domain.

Please review this page before the exam.
https://cloud.google.com/architecture/best-practices-vpc-design

---

49. Compute Engine blocks or restricts traffic through all the following ports/protocols between the Internet and virtual machines, and between two virtual machines when traffic is addressed to their external IP addresses through these ports (this

also includes load-balanced addresses). These ports are permanently blocked; they cannot be opened using firewall rules. What ports are blocked in Compute Engine? (Select Three)

F. All outgoing traffic to port 25 (SMTP) is blocked.
G. All traffic coming from on premises
H. GRE traffic is blocked, even between VMs
I. Most outgoing traffic to port 465 or 587 (SMTP over SSL) is blocked, except for known Google IP addresses
J. All outgoing traffic to port 22 (SSH) is blocked.

Correct Answer(s): A, C and D:

Explanation: All outgoing traffic to port 25 (SMTP) is blocked. Most outgoing traffic to port 465 or 587 (SMTP over SSL) is blocked, except for known Google IP addresses. GRE traffic is blocked, even between VMs. Traffic that uses a protocol other than TCP, UDP, ICMP, and IPIP is blocked, unless explicitly allowed through protocol forwarding.

Please review the following page before the exam.

https://cloud.google.com/compute/docs/networks-and-firewalls

---

50. Your business director has specifically requested to you to ensure that the deployment limit users with administrative privileges at the organization level.
Which two roles do you need to restrict? (Select One)

F. GKE Cluster Admin
G. Compute Admin
H. Organization Administrator
I. Super Admin
J. None of the above

Correct Answer(s): C, D: Organizational Admin and Super Admin

Explanation: The Google Workspace or Cloud Identity super administrators and the GCP Organization admin are key roles during the setup process and for lifecycle control for the Organization resource. The two roles are generally assigned to different users or groups, although this depends on the organization structure and needs.

Please review the following page before the exam.

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

---

End of Free Practice Exam One

Additional Resources

Additional Practice Questions are available on www.TechCommanders.com

Full Google Cloud Professional Security Engineer Course @ www.TechCommanders.com

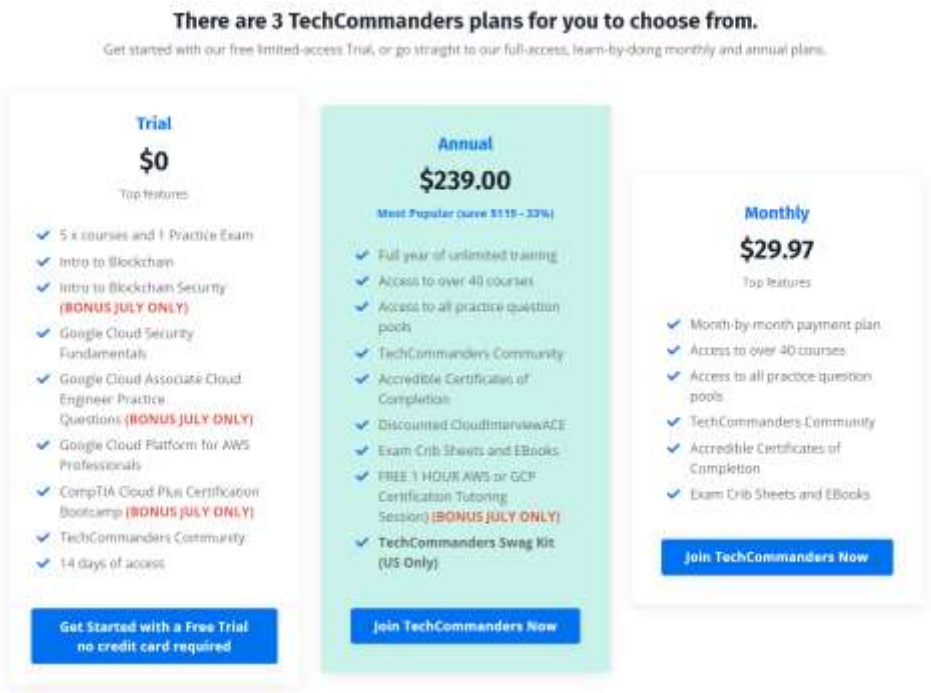
Free YouTube GCP Cloud Engineer Playlist

https://www.youtube.com/playlist?list=PLOYQCApvKhV2c4iUQdPKwzWH5x5gjsvmg

Google Cloud focused blog for all exams! http://thegcpgurus.com/

Save up to 30% on TechCommanders Membership with **SAVENOW30** at check out.

Join TechCommanders! We have both Free and Paid Tiers.



We are TechCommanders...
experts in Next Generation Technology Training.
TechCommanders is an online training platform for both aspiring and veteran IT professionals interested in next generation IT Skills. TechCommanders is led by Joseph Holbrook, a highly sought-after technology industry veteran.

TechCommanders offers blended learning which allows the students to learn on demand but with live training.

Courses offered are used to prepare students to take certification exams in Cloud, DevOps, IT Security and Blockchain.

TechCommanders was established in Jacksonville, Florida in 2020 by Joseph Holbrook, both a US Navy Veteran and a technology

industry veteran. TechCommanders, Advancing your NextGen Technology Skills.