PROFESSIONAL-CLOUD-SECURITY-ENGINEER Q&As

Professional Cloud Security Engineer

Pass Google PROFESSIONAL-CLOUD-SECURITY-ENGINEER Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/professional-cloud-security-engineer.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Google Official Exam Center

QUESTION 1

A customer wants to deploy a large number of 3-tier web applications on Compute Engine.

How should the customer ensure authenticated network separation between the different tiers of the application?

A. Run each tier in its own Project, and segregate using Project labels.

B. Run each tier with a different Service Account (SA), and use SA-based firewall rules.

C. Run each tier in its own subnet, and use subnet-based firewall rules.

D. Run each tier with its own VM tags, and use tag-based firewall rules.

Correct Answer: B

"Isolate VMs using service accounts when possible" "even though it is possible to uses tags for target filtering in this manner, we recommend that you use service accounts where possible. Target tags are not access-controlled and can be changed by someone with the instanceAdmin role while VMs are in service. Service accounts are access-controlled, meaning that a specific user must be explicitly authorized to use a service account. There can only be one service account per instance, whereas there can be multiple tags. Also, service accounts assigned to a VM can only be changed when the VM is stopped." https://cloud.google.com/solutions/best-practices-vpc-design#isolate-vms-service-accounts

QUESTION 2

You define central security controls in your Google Cloud environment for one of the folders in your organization you set an organizational policy to deny the assignment of external IP addresses to VMs. Two days later you receive an alert about a new VM with an external IP address under that folder.

What could have caused this alert?

A. The VM was created with a static external IP address that was reserved in the project before the organizational policy rule was set.

B. The organizational policy constraint wasn\\'t properly enforced and is running in "dry run mode.

C. At project level, the organizational policy control has been overwritten with an \\'allow\\' value.

D. The policy constraint on the folder level does not have any effect because of an allow" value for that constraint on the organizational level.

Correct Answer: C

QUESTION 3

Your Google Cloud organization allows for administrative capabilities to be distributed to each team through provision of a Google Cloud project with Owner role (roles/ owner). The organization contains thousands of Google Cloud Projects

Security Command Center Premium has surfaced multiple cpen_myscl_port findings. You are enforcing the guardrails and need to prevent these types of common misconfigurations.

What should you do?

A. Create a firewall rule for each virtual private cloud (VPC) to deny traffic from 0 0 0 0/0 with priority 0.

B. Create a hierarchical firewall policy configured at the organization to deny all connections from 0 0 0 0/0.

C. Create a Google Cloud Armor security policy to deny traffic from 0 0 0 0/0.

D. Create a hierarchical firewall policy configured at the organization to allow connections only from internal IP ranges

Correct Answer: B

QUESTION 4

You are setting up a new Cloud Storage bucket in your environment that is encrypted with a customer managed encryption key (CMEK). The CMEK is stored in Cloud Key Management Service (KMS), in project "prj-a", and the Cloud Storage bucket will use project "prj-b". The key is backed by a Cloud Hardware Security Module (HSM) and resides in the region europe-west3. Your storage bucket will be located in the region europe-west1. When you create the bucket, you cannot access the key, and you need to troubleshoot why.

What has caused the access issue?

A. A firewall rule prevents the key from being accessible.

B. Cloud HSM does not support Cloud Storage.

C. The CMEK is in a different project than the Cloud Storage bucket.

D. The CMEK is in a different region than the Cloud Storage bucket.

Correct Answer: D

The correct answer is D. The CMEK is in a different region than the Cloud Storage bucket.

When you use a customer-managed encryption key (CMEK) to secure a Cloud Storage bucket, the key and the bucket must be located in the same region. In this case, the key is in europe-west3 and the bucket is in europe-west1, which is why you\\'re unable to access the key.

QUESTION 5

An engineering team is launching a web application that will be public on the internet. The web application is hosted in multiple GCP regions and will be directed to the respective backend based on the URL request.

Your team wants to avoid exposing the application directly on the internet and wants to deny traffic from a specific list of malicious IP addresses

Which solution should your team implement to meet these requirements?

A. Cloud Armor

B. Network Load Balancing

C. SSL Proxy Load Balancing

D. NAT Gateway

Correct Answer: A

https://cloud.google.com/armor/docs/security-policy-overview#edge-security Reference: https://cloud.google.com/armor/docs/security-policy-concepts

QUESTION 6

Your organization uses the top-tier folder to separate application environments (prod and dev). The developers need to see all application development audit logs but they are not permitted to review production logs. Your security team can review all logs in production and development environments. You must grant Identity and Access Management (1AM) roles at the right resource level tor the developers and security team while you ensure least privilege.

What should you do?

A. 1 Grant logging, viewer rote to the security team at the organization resource level. 2 Grant logging, viewer rote to the developer team at the folder resource level that contains all the dev projects.

B. 1 Grant logging. viewer rote to the security team at the organization resource level. 2 Grant logging. admin role to the developer team at the organization resource level.

C. 1 Grant logging.admin role to the security team at the organization resource level. 2 Grant logging. viewer rote to the developer team at the folder resource level that contains all the dev projects.

D. 1 Grant logging.admin role to the security team at the organization resource level. 2 Grant logging.admin role to the developer team at the organization resource level.

Correct Answer: A

QUESTION 7

Your organization recently activated the Security Command Center {SCO standard tier. There are a few Cloud Storage buckets that were accidentally made accessible to the public. You need to investigate the impact of the incident and remediate it.

What should you do?

A. 1 Remove the Identity and Access Management (IAM) granting access to allusers from the buckets 2 Apply the organization policy storage. unifromBucketLevelAccess to prevent regressions 3 Query the data access logs to report on unauthorized access

B. 1 Change bucket permissions to limit access 2 Query the data access audit logs for any unauthorized access to the buckets 3 After the misconfiguration is corrected mute the finding in the Security Command Center

C. 1 Change permissions to limit access for authorized users 2 Enforce a VPC Service Controls perimeter around all the production projects to immediately stop any unauthorized access 3 Review the administrator activity audit logs to report on any unauthorized access

D. 1 Change the bucket permissions to limit access 2 Query the buckets usage logs to report on unauthorized access to the data 3 Enforce the organization policy storage.publicAccessPrevention to avoid regressions

Correct Answer: D

QUESTION 8

A company allows every employee to use Google Cloud Platform. Each department has a Google Group, with all department members as group members. If a department member creates a new project, all members of that department should automatically have read-only access to all new project resources. Members of any other department should not have access to the project. You need to configure this behavior.

What should you do to meet these requirements?

A. Create a Folder per department under the Organization. For each department\\'s Folder, assign the Project Viewer role to the Google Group related to that department.

B. Create a Folder per department under the Organization. For each department\\'s Folder, assign the Project Browser role to the Google Group related to that department.

C. Create a Project per department under the Organization. For each department\\'s Project, assign the Project Viewer role to the Google Group related to that department.

D. Create a Project per department under the Organization. For each department\\'s Project, assign the Project Browser role to the Google Group related to that department.

Correct Answer: A

https://cloud.google.com/iam/docs/understanding-roles#project-roles

QUESTION 9

Your company must follow industry specific regulations. Therefore, you need to enforce customer- managed encryption keys (CMEK) for all new Cloud Storage resources in the organization called org1. What command should you execute?

A. organization poli-cy:constraints/gcp.restrictStorageNonCmekServices binding at: org1 policy type: allow policy value: all supported services

B. organization policy: con-straints/gcp.restrictNonCmekServices binding at: org1 policy type: deny policy value: storage.googleapis.com

C. organization policy: con-straints/gcp.restrictStorageNonCmekServices binding at: org1 policy type: deny policy value: storage.googleapis.com

D. organization policy: con-straints/gcp.restrictNonCmekServices binding at: org1 policy type: allow policy value: storage.googleapis.com

Correct Answer: B

QUESTION 10

You want data on Compute Engine disks to be encrypted at rest with keys managed by Cloud Key Management Service (KMS). Cloud Identity and Access Management (IAM) permissions to these keys must be managed in a grouped way because the permissions should be the same for all keys.

What should you do?

A. Create a single KeyRing for all persistent disks and all Keys in this KeyRing. Manage the IAM permissions at the Key level.

B. Create a single KeyRing for all persistent disks and all Keys in this KeyRing. Manage the IAM permissions at the KeyRing level.

C. Create a KeyRing per persistent disk, with each KeyRing containing a single Key. Manage the IAM permissions at the Key level.

D. Create a KeyRing per persistent disk, with each KeyRing containing a single Key. Manage the IAM permissions at the KeyRing level.

Correct Answer: B

https://cloud.netapp.com/blog/gcp-cvo-blg-how-to-use-google-cloud-encryption-with-a-persistent-disk

QUESTION 11

Which two security characteristics are related to the use of VPC peering to connect two VPC networks? (Choose two.)

A. Central management of routes, firewalls, and VPNs for peered networks

B. Non-transitive peered networks; where only directly peered networks can communicate

C. Ability to peer networks that belong to different Google Cloud Platform organizations

D. Firewall rules that can be created with a tag from one peered network to another peered network

E. Ability to share specific subnets across peered networks

Correct Answer: BC

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

QUESTION 12

Your organization must comply with the regulation to keep instance logging data within Europe. Your workloads will be hosted in the Netherlands in region europe-west4 in a new project. You must configure Cloud Logging to keep your data in the country.

What should you do?

A. Configure the organization policy constraint gcp.resourceLocations to europe-west4.

B. Set the logging storage region to eurcpe-west4 by using the gcloud CLI logging settings update.

C. Create a new tog bucket in europe-west4. and redirect the _Def auit bucKet to the new bucket.

D. Configure log sink to export all logs into a Cloud Storage bucket in europe-west4.

Correct Answer: C

QUESTION 13

You are working with a client that is concerned about control of their encryption keys for sensitive data. The client does not want to store encryption keys at rest in the same cloud service provider (CSP) as the data that the keys are encrypting.

Which Google Cloud encryption solutions should you recommend to this client? (Choose two.)

A. Customer-supplied encryption keys.

B. Google default encryption

C. Secret Manager

D. Cloud External Key Manager

E. Customer-managed encryption keys

Correct Answer: AD

QUESTION 14

You need to set up two network segments: one with an untrusted subnet and the other with a trusted subnet. You want to configure a virtual appliance such as a next-generation firewall (NGFW) to inspect all traffic between the two network segments.

How should you design the network to inspect the traffic?

A. 1. Set up one VPC with two subnets: one trusted and the other untrusted.

2. Configure a custom route for all traffic (0.0.0.0/0) pointed to the virtual appliance.

B. 1. Set up one VPC with two subnets: one trusted and the other untrusted.

2. Configure a custom route for all RFC1918 subnets pointed to the virtual appliance.

C. 1. Set up two VPC networks: one trusted and the other untrusted, and peer them together.

2. Configure a custom route on each network pointed to the virtual appliance.

D. 1. Set up two VPC networks: one trusted and the other untrusted.

2. Configure a virtual appliance using multiple network interfaces, with each interface connected to one of the VPC networks.

Correct Answer: D

Multiple network interfaces. The simplest way to connect multiple VPC networks through a virtual appliance is by using multiple network interfaces, with each interface connecting to one of the VPC networks. Internet and on-premises connectivity is provided over one or two separate network interfaces. With many NGFW products, internet connectivity is connected through an interface marked as untrusted in the NGFW software.

https://cloud.google.com/architecture/best-practices-vpc-design#l7

This architecture has multiple VPC networks that are bridged by an L7 next-generation firewall (NGFW) appliance,

which functions as a multi-NIC bridge between VPC networks. An untrusted, outside VPC network is introduced to terminate hybrid interconnects and internet-based connections that terminate on the outside leg of the L7 NGFW for inspection. There are many variations on this design, but the key principle is to filter traffic through the firewall before the traffic reaches trusted VPC networks.

QUESTION 15

Your company plans to move most of its IT infrastructure to Google Cloud. They want to leverage their existing on-premises Active Directory as an identity provider for Google Cloud. Which two steps should you take to integrate the company\\'s on-premises Active Directory with Google Cloud and configure access management? (Choose two.)

A. Use Identity Platform to provision users and groups to Google Cloud.

B. Use Cloud Identity SAML integration to provision users and groups to Google Cloud.

C. Install Google Cloud Directory Sync and connect it to Active Directory and Cloud Identity.

D. Create Identity and Access Management (1AM) roles with permissions corresponding to each Active Directory group.

E. Create Identity and Access Management (1AM) groups with permissions corresponding to each Active Directory group.

Correct Answer: CE

https://cloud.google.com/architecture/identity/federating-gcp-with-active-directory-synchronizing-user- accounts?hl=en
https://cloud.google.com/architecture/identity/federating-gcp-with-active-directory-synchronizing-user-accounts?hl=en#deciding_where_to_deploy_gcds