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

How should a customer reliably deliver Stackdriver logs from GCP to their on-premises SIEM system?

A. Send all logs to the SIEM system via an existing protocol such as syslog.

B. Configure every project to export all their logs to a common BigQuery DataSet, which will be queried by the SIEM system.

C. Configure Organizational Log Sinks to export logs to a Cloud Pub/Sub Topic, which will be sent to the SIEM via Dataflow.

D. Build a connector for the SIEM to query for all logs in real time from the GCP RESTful JSON APIs.

Correct Answer: C

Scenarios for exporting Cloud Logging data: Splunk This scenario shows how to export selected logs from Cloud Logging to Pub/Sub for ingestion into Splunk. Splunk is a security information and event management (SIEM) solution that supports several ways of ingesting data, such as receiving streaming data out of Google Cloud through Splunk HTTP Event Collector (HEC) or by fetching data from Google Cloud APIs through Splunk Add-on for Google Cloud. Using the Pub/Sub to Splunk Dataflow template, you can natively forward logs and events from a Pub/Sub topic into Splunk HEC. If Splunk HEC is not available in your Splunk deployment, you can use the Add-on to collect the logs and events from the Pub/Sub topic. https://cloud.google.com/solutions/exporting-stackdriver-logging-for-splunk

QUESTION 2

Your team needs to make sure that their backend database can only be accessed by the frontend application and no other instances on the network.

How should your team design this network?

A. Create an ingress firewall rule to allow access only from the application to the database using firewall tags.

B. Create a different subnet for the frontend application and database to ensure network isolation.

C. Create two VPC networks, and connect the two networks using Cloud VPN gateways to ensure network isolation.

D. Create two VPC networks, and connect the two networks using VPC peering to ensure network isolation.

Correct Answer: A

"However, 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"

QUESTION 3

A customer wants to move their sensitive workloads to a Compute Engine-based cluster using Managed Instance Groups (MIGs). The jobs are bursty and must be completed quickly. They have a requirement to be able to manage and

rotate the encryption keys.

Which boot disk encryption solution should you use on the cluster to meet this customer\\'s requirements?

A. Customer-supplied encryption keys (CSEK)

B. Customer-managed encryption keys (CMEK) using Cloud Key Management Service (KMS)

C. Encryption by default

D. Pre-encrypting files before transferring to Google Cloud Platform (GCP) for analysis

Correct Answer: B

Reference https://cloud.google.com/kubernetes-engine/docs/how-to/dynamic-provisioning-cmek

QUESTION 4

You are troubleshooting access denied errors between Compute Engine instances connected to a Shared VPC and BigQuery datasets. The datasets reside in a project protected by a VPC Service Controls perimeter. What should you do?

A. Add the host project containing the Shared VPC to the service perimeter.

B. Add the service project where the Compute Engine instances reside to the service perimeter.

C. Create a service perimeter between the service project where the Compute Engine instances reside and the host project that contains the Shared VPC.

D. Create a perimeter bridge between the service project where the Compute Engine instances reside and the perimeter that contains the protected BigQuery datasets.

Correct Answer: A

https://cloud.google.com/vpc-service-controls/docs/service-perimeters#secure-google-managed-resources If you\\'re using Shared VPC, you must include the host project in a service perimeter along with any projects that belong to the Shared VPC.

QUESTION 5

You want to prevent users from accidentally deleting a Shared VPC host project. Which organization-level policy constraint should you enable?

A. compute.restrictSharedVpcHostProjects

B. compute.restrictXpnProjectLienRemoval

C. compute.restrictSharedVpcSubnetworks

D. compute.sharedReservationsOwnerProjects

Correct Answer: B

Reference: https://cloud.google.com/vpc/docs/provisioning-shared-vpc https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints#constraints- for-specific-services -constraints/compute.restrictXpnProjectLienRemoval -Restrict shared VPC project lien removal This boolean constraint restricts the set of users that can remove a Shared VPC host project lien without organization-level permission where this constraint is set to True. By default, any user with the permission to update liens can remove a Shared VPC host project lien. Enforcing this constraint requires that permission be granted at the organization level.