IT 认证电子书

半年免费升级服务

质 量 更 高 服 务 更 好

半年免费升级服务

1 / 3

Exam : **Professional Cloud Security Engineer**

Title : Google Cloud Certified - Professional Cloud Security Engineer

Version : DEMO

1.A customer needs an alternative to storing their plain text secrets in their source-code management (SCM) system.

How should the customer achieve this using Google Cloud Platform?

A. Use Cloud Source Repositories, and store secrets in Cloud SQL.

B. Encrypt the secrets with a Customer-Managed Encryption Key (CMEK), and store them in Cloud Storage.

C. Run the Cloud Data Loss Prevention API to scan the secrets, and store them in Cloud SQL.

D. Deploy the SCM to a Compute Engine VM with local SSDs, and enable preemptible VMs.

Answer: B

2.You are the security admin of your company. Your development team creates multiple GCP projects under the "implementation" folder for several dev, staging, and production workloads. You want to prevent data exfiltration by malicious insiders or compromised code by setting up a security perimeter. However, you do not want to restrict communication between the projects.

What should you do?

A. Use a Shared VPC to enable communication between all projects, and use firewall rules to prevent data exfiltration.

B. Create access levels in Access Context Manager to prevent data exfiltration, and use a shared VPC for communication between projects.

C. Use an infrastructure-as-code software tool to set up a single service perimeter and to deploy a Cloud Function that monitors the "implementation" folder via Stackdriver and Cloud Pub/Sub. When the function notices that a new project is added to the folder, it executes Terraform to add the new project to the associated perimeter.

D. Use an infrastructure-as-code software tool to set up three different service perimeters for dev, staging, and prod and to deploy a Cloud Function that monitors the "implementation" folder via Stackdriver and Cloud Pub/Sub. When the function notices that a new project is added to the folder, it executes Terraform to add the new project to the respective perimeter.

Answer: C

Explanation:

https://cloud.google.com/vpc-service-controls/docs/overview#benefits

https://github.com/terraform-google-modules/terraform-google-vpc-service-controls/tree/master/examples/automatic_folder

3.Your company is using Cloud Dataproc for its Spark and Hadoop jobs. You want to be able to create, rotate, and destroy symmetric encryption keys used for the persistent disks used by Cloud Dataproc. Keys can be stored in the cloud.

What should you do?

A. Use the Cloud Key Management Service to manage the data encryption key (DEK).

B. Use the Cloud Key Management Service to manage the key encryption key (KEK).

C. Use customer-supplied encryption keys to manage the data encryption key (DEK).

D. Use customer-supplied encryption keys to manage the key encryption key (KEK).

Answer: B

Explanation:

This PD and bucket data is encrypted using a Google-generated data encryption key (DEK) and key

encryption key (KEK). The CMEK feature allows you to create, use, and revoke the key encryption key (KEK). Google still controls the data encryption key (DEK). For more information on Google data encryption keys, see Encryption at Rest.

https://cloud.google.com/dataproc/docs/concepts/configuring-clusters/customer-managed-encryption

https://codelabs.developers.google.com/codelabs/encrypt-and-decrypt-data-with-cloud-kms#0

4.You perform a security assessment on a customer architecture and discover that multiple VMs have public IP addresses. After providing a recommendation to remove the public IP addresses, you are told those VMs need to communicate to external sites as part of the customer's typical operations.

What should you recommend to reduce the need for public IP addresses in your customer's VMs?

A. Google Cloud Armor

B. Cloud NAT

C. Cloud Router

D. Cloud VPN

Answer: B

Explanation:

https://cloud.google.com/nat/docs/overview

5.A customer is running an analytics workload on Google Cloud Platform (GCP) where Compute Engine instances are accessing data stored on Cloud Storage. Your team wants to make sure that this workload will not be able to access, or be accessed from, the internet.

Which two strategies should your team use to meet these requirements? (Choose two.)

A. Configure Private Google Access on the Compute Engine subnet

B. Avoid assigning public IP addresses to the Compute Engine cluster.

C. Make sure that the Compute Engine cluster is running on a separate subnet.

D. Turn off IP forwarding on the Compute Engine instances in the cluster.

E. Configure a Cloud NAT gateway.

Answer: A,B