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.geekcert.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 company is running workloads in a dedicated server room. They must only be accessed from within the private company network. You need to connect to these workloads from Compute Engine instances within a Google Cloud Platform project.

Which two approaches can you take to meet the requirements? (Choose two.)

A. Configure the project with Cloud VPN.

B. Configure the project with Shared VPC.

C. Configure the project with Cloud Interconnect.

D. Configure the project with VPC peering.

E. Configure all Compute Engine instances with Private Access.

Correct Answer: AC

A) IPsec VPN tunels: https://cloud.google.com/network-connectivity/docs/vpn/concepts/overviewInterconnect https://cloud.google.com/network-connectivity/docs/interconnect/concepts/dedicated-overview https://cloud.google.com/solutions/secure-data-workloadsuse-cases

QUESTION 2

Your organization processes sensitive health information. You want to ensure that data is encrypted while in use by the virtual machines (VMs). You must create a policy that is enforced across the entire organization. What should you do?

A. Implement an organization policy that ensures that all VM resources created across your organization use customer-managed encryption keys (CMEK) protection.

B. Implement an organization policy that ensures all VM resources created across your organization are Confidential VM instances.

C. Implement an organization policy that ensures that all VM resources created across your organization use Cloud External Key Manager (EKM) protection.

D. No action is necessary because Google encrypts data while it is in use by default.

Correct Answer: B

QUESTION 3

Your company\\'s users access data in a BigQuery table. You want to ensure they can only access the data during working hours.

What should you do?

A. Assign a BigQuery Data Viewer role along with an IAM condition that limits the access to specified working hours.

B. Run a gsutil script that assigns a BigQuery Data Viewer role, and remove it only during the specified working hours.

C. Assign a BigQuery Data Viewer role to a service account that adds and removes the users daily during the specified working hours.

D. Configure Cloud Scheduler so that it triggers a Cloud Functions instance that modifies the organizational policy constraint for BigQuery during the specified working hours.

Correct Answer: A

The correct answer is A. Assign a BigQuery Data Viewer role along with an IAM condition that limits the access to specified working hours.

IAM conditions in Google Cloud can be used to fine-tune access control according to attributes like time, date, and IP address. In this case, you can create an IAM condition that allows access only during working hours. This condition can be attached to the BigQuery Data Viewer role, ensuring that users can only access the data in the BigQuery table during the specified times.

QUESTION 4

For compliance reporting purposes, the internal audit department needs you to provide the list of virtual machines (VMs) that have critical operating system (OS) security updates available, but not installed. You must provide this list every six months, and you want to perform this task quickly.

What should you do?

A. Run a Security Command Center security scan on all VMs to extract a list of VMs with critical OS vulnerabilities every six months.

B. Run a gcloud CLI command from the Command Line Interface (CLI) to extract the VM\\'s OS version information every six months.

C. Ensure that the Cloud Logging agent is installed on all VMs, and extract the OS last update log date every six months.

D. Ensure the OS Config agent is installed on all VMs and extract the patch status dashboard every six months.

Correct Answer: D

https://cloud.google.com/compute/docs/vm-manager

QUESTION 5

An administrative application is running on a virtual machine (VM) in a managed group at port 5601 inside a Virtual Private Cloud (VPC) instance without access to the internet currently. You want to expose the web interface at port 5601 to users and enforce authentication and authorization Google credentials.

What should you do?

A. Configure the bastion host with OS Login enabled and allow connection to port 5601 at VPC firewall. Log in to the bastion host from the Google Cloud console by using SSH-in-browser and then to the web application.

B. Modify the VPC routing with the default route point to the default internet gateway. Modify the VPC Firewall rule to

allow access from the internet 0.0.0.0/0 to port 5601 on the application instance.

C. Configure Secure Shell Access (SSH) bastion host in a public network, and allow only the bastion host to connect to the application on port 5601. Use a bastion host as a jump host to connect to the application.

D. Configure an HTTP Load Balancing instance that points to the managed group with Identity-Aware Proxy (IAP) protection with Google credentials. Modify the VPC firewall to allow access from IAP network range.

Correct Answer: D

The correct answer is D. Configure an HTTP Load Balancing instance that points to the managed group with Identity-Aware Proxy (IAP) protection with Google credentials. Modify the VPC firewall to allow access from IAP network range.

This approach allows you to expose the web interface securely by using Identity-Aware Proxy (IAP), which provides authentication and authorization with Google credentials. The HTTP Load Balancer can distribute traffic to the VMs in the managed group, and the VPC firewall rule ensures that access is allowed from the IAP network range.