Free Questions for Professional-Cloud-Security-Engineer by go4braindumps

Shared by Brewer on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You need to set up a Cloud interconnect connection between your company's on-premises data center and VPC host network. You want to make sure that on-premises applications can only access Google APIs over the Cloud Interconnect and not through the public internet. You are required to only use APIs that are supported by VPC Service Controls to mitigate against exfiltration risk to non-supported APIs. How should you configure the network?

Options:

A- Enable Private Google Access on the regional subnets and global dynamic routing mode.

B- Set up a Private Service Connect endpoint IP address with the API bundle of 'all-apis', which is advertised as a route over the Cloud interconnect connection.

C- Use private.googleapis.com to access Google APIs using a set of IP addresses only routable from within Google Cloud, which are advertised as routes over the connection.

D- Use restricted googleapis.com to access Google APIs using a set of IP addresses only routable from within Google Cloud, which are advertised as routes over the Cloud Interconnect connection.

Answer:

B

Question 2

Question Type: MultipleChoice

Your company's Chief Information Security Officer (CISO) creates a requirement that business data must be stored in specific locations due to regulatory requirements that affect the company's global expansion plans. After working on the details to implement this requirement, you determine the following:

The services in scope are included in the Google Cloud Data Residency Terms.

The business data remains within specific locations under the same organization.

The folder structure can contain multiple data residency locations.

You plan to use the Resource Location Restriction organization policy constraint. At which level in the resource hierarchy should you set the constraint?

Options:

A- Folder

B- Resource

C- Project

D- Organization

Answer:

B

Question 3

Question Type: MultipleChoice

You are tasked with exporting and auditing security logs for login activity events for Google Cloud console and API calls that modify configurations to Google Cloud resources. Your export must meet the following requirements:

Export related logs for all projects in the Google Cloud organization.

Export logs in near real-time to an external SIEM.

What should you do? (Choose two.)

Options:

A- Create a Log Sink at the organization level with a Pub/Sub destination.

B- Create a Log Sink at the organization level with the includeChildren parameter, and set the destination to a Pub/Sub topic.

C- Enable Data Access audit logs at the organization level to apply to all projects.

D- Enable Google Workspace audit logs to be shared with Google Cloud in the Admin Console.

E- Ensure that the SIEM processes the AuthenticationInfo field in the audit log entry to gather identity information.

Answer:

A, E

Question 4

Question Type: **MultipleChoice**

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?

Options:

A- Google Cloud Armor

B- Cloud NAT

C- Cloud Router

D- Cloud VPN

Answer:

D

Question 5

Question Type: MultipleChoice

You plan to use a Google Cloud Armor policy to prevent common attacks such as cross-site scripting (XSS) and SQL injection (SQLi) from reaching your web application's backend. What are two requirements for using Google Cloud Armor security policies? (Choose two.)

Options:

A- The load balancer must be an external SSL proxy load balancer.

B- Google Cloud Armor Policy rules can only match on Layer 7 (L7) attributes.

C- The load balancer must use the Premium Network Service Tier.

D- The backend service's load balancing scheme must be EXTERNAL.

E- The load balancer must be an external HTTP(S) load balancer.

Answer:

B, E

Question 6

Question Type: MultipleChoice

You are a security administrator at your company. Per Google-recommended best practices, you implemented the domain restricted sharing organization policy to allow only required domains to access your projects. An engineering team is now reporting that users at an external partner outside your organization domain cannot be granted access to the resources in a project. How should you make an exception for your partner's domain while following the stated best practices?

Options:

A- Turn off the domain restriction sharing organization policy. Set the policy value to 'Allow All.'

B- Turn off the domain restricted sharing organization policy. Provide the external partners with the required permissions using Google's Identity and Access Management (IAM) service.

C- Turn off the domain restricted sharing organization policy. Add each partner's Google Workspace customer ID to a Google group, add the Google group as an exception under the organization policy, and then turn the policy back on.

D- Turn off the domain restricted sharing organization policy. Set the policy value to 'Custom.' Add each external partner's Cloud Identity or Google Workspace customer ID as an exception under the

organization policy, and then turn the policy back on.

Answer:

B

Question 7

Question Type: MultipleChoice

Users are reporting an outage on your public-facing application that is hosted on Compute Engine. You suspect that a recent change to your firewall rules is responsible. You need to test whether your firewall rules are working properly. What should you do?

Options:

A- Enable Firewall Rules Logging on the latest rules that were changed. Use Logs Explorer to analyze whether the rules are working correctly.

B- Connect to a bastion host in your VPC. Use a network traffic analyzer to determine at which point your requests are being blocked.

C- In a pre-production environment, disable all firewall rules individually to determine which one is blocking user traffic.

D- Enable VPC Flow Logs in your VPC. Use Logs Explorer to analyze whether the rules are working correctly.

Answer:

A

Question 8

Question Type: MultipleChoice

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

Options:

A- compute.restrictSharedVpcHostProjects

B- compute.restrictXpnProjectLienRemoval

C- compute.restrictSharedVpcSubnetworks

D- compute.sharedReservationsOwnerProjects

Answer:

B

Question 9

Question Type: MultipleChoice

Which type of load balancer should you use to maintain client IP by default while using the standard network tier?

Options:

A- SSL Proxy

B- TCP Proxy

C- Internal TCP/UDP

D- TCP/UDP Network

Answer:

C

Question 10

Question Type: MultipleChoice

You are setting up a CI/CD pipeline to deploy containerized applications to your production clusters on Google Kubernetes Engine (GKE). You need to prevent containers with known vulnerabilities from being deployed. You have the following requirements for your solution:

Must be cloud-native

Must be cost-efficient

Minimize operational overhead

How should you accomplish this? (Choose two.)

Options:

A- Create a Cloud Build pipeline that will monitor changes to your container templates in a Cloud Source Repositories repository. Add a step to analyze Container Analysis results before allowing the build to continue.

B- Use a Cloud Function triggered by log events in Google Cloud's operations suite to automatically scan your container images in Container Registry.

C- Use a cron job on a Compute Engine instance to scan your existing repositories for known vulnerabilities and raise an alert if a non-compliant container image is found.

D- Deploy Jenkins on GKE and configure a CI/CD pipeline to deploy your containers to Container Registry. Add a step to validate your container images before deploying your container to the cluster.

E- In your CI/CD pipeline, add an attestation on your container image when no vulnerabilities have been found. Use a Binary Authorization policy to block deployments of containers with no attestation in your cluster.

Answer:

C, E