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

Shared by Moore on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You manage a mission-critical workload for your organization, which is in a highly regulated industry The workload uses Compute Engine VMs to analyze and process the sensitive data after it is uploaded to Cloud Storage from the endpomt computers. Your compliance team has detected that this workload does not meet the data protection requirements for sensitive dat

a. You need to meet these requirements;

* Manage the data encryption key (DEK) outside the Google Cloud boundary.

* Maintain full control of encryption keys through a third-party provider.

* Encrypt the sensitive data before uploading it to Cloud Storage

* Decrypt the sensitive data during processing in the Compute Engine VMs

* Encrypt the sensitive data in memory while in use in the Compute Engine VMs

What should you do?

Choose 2 answers

Options:

A- Create a VPC Service Controls service perimeter across your existing Compute Engine VMs and Cloud Storage buckets

B- Migrate the Compute Engine VMs to Confidential VMs to access the sensitive data.

C- Configure Cloud External Key Manager to encrypt the sensitive data before it is uploaded to Cloud Storage and decrypt the sensitive data after it is downloaded into your VMs

D- Create Confidential VMs to access the sensitive data.

E- Configure Customer Managed Encryption Keys to encrypt the sensitive data before it is uploaded to Cloud Storage, and decrypt the sensitive data after it is downloaded into your VMs.

Answer:

C, D

Explanation:

https://cloud.google.com/confidential-computing/confidential-vm/docs/creating-cvm-instance#considerations

Confidential VM does not support live migration. You can only enable Confidential Computing on a VM when you first create the instance. https://cloud.google.com/confidential-computing/confidential-vm/docs/creating-cvm-instance

Question 2

Question Type: MultipleChoice

Your organization wants to be compliant with the General Data Protection Regulation (GDPR) on Google Cloud You must implement data residency and operational sovereignty in the EU.

What should you do?

Choose 2 answers

Options:

A- Limit the physical location of a new resource with the Organization Policy Service resource locations constraint.'

B- Use Cloud IDS to get east-west and north-south traffic visibility in the EU to monitor intra-VPC and mter-VPC communication.

C- Limit Google personnel access based on predefined attributes such as their citizenship or geographic location by using Key Access Justifications

D- Use identity federation to limit access to Google Cloud resources from non-EU entities.

E- Use VPC Flow Logs to monitor intra-VPC and inter-VPC traffic in the EU.

Answer:

A, C

Explanation:

https://cloud.google.com/architecture/framework/security/data-residency-sovereignty#manage_your_operational_sovereignty

Question 3

Question Type: MultipleChoice

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?

Options:

A- Assign a BigQuery Data Viewer role along with an 1AM condition that limits the access to specified working hours.

B- Configure Cloud Scheduler so that it triggers a Cloud Functions instance that modifies the organizational policy constraints for BigQuery 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- Run a gsuttl script that assigns a BigQuery Data Viewer role, and remove it only during the specified working hours.

Answer:

A

Question 4

Question Type: MultipleChoice

You are developing a new application that uses exclusively Compute Engine VMs Once a day. this application will execute five different batch jobs Each of the batch jobs requires a dedicated set of permissions on Google Cloud resources outside of your application. You need to design a secure access concept for the batch jobs that adheres to the least-privilege principle

What should you do?

Options:

A- 1. Create a general service account **g-sa' to execute the batch jobs.
* 2 Grant the permissions required to execute the batch jobs to g-sa.
* 3. Execute the batch jobs with the permissions granted to g-sa

B- 1. Create a general service account 'g-sa' to orchestrate the batch jobs.
* 2. Create one service account per batch job Mb-sa-[1-5],' and grant only the permissions required to run the individual batch jobs to the service accounts.
* 3. Grant the Service Account Token Creator role to g-sa Use g-sa to obtain short-lived access tokens for b-sa-[1-5] and to execute the

batch jobs with the permissions of b-sa-[1-5].

C- 1. Create a workload identity pool and configure workload identity pool providers for each batch job
* 2 Assign the workload identity user role to each of the identities configured in the providers.
* 3. Create one service account per batch job Mb-sa-[1-5]'. and grant only the permissions required to run the individual batch jobs to the service accounts
* 4 Generate credential configuration files for each of the providers Use these files to execute the batch jobs with the permissions of b-sa-[1-5].
D.
* 1. Create a general service account 'g-sa' to orchestrate the batch jobs.
* 2 Create one service account per batch job 'b-sa-[1-5)\ Grant only the permissions required to run the individual batch jobs to the service accounts and generate service account keys for each of these service accounts
* 3. Store the service account keys in Secret Manager. Grant g-sa access to Secret Manager and run the batch jobs with the permissions of b-sa-[1-5].

Answer:

B

Question 5

Question Type: MultipleChoice

Employees at your company use their personal computers to access your organization s Google Cloud console. You need to ensure that users can only access the Google Cloud console from their corporate-issued devices and verify that they have a valid enterprise certificate

What should you do?

Options:

A- Implement an Identity and Access Management (1AM) conditional policy to verify the device certificate

B- Implement a VPC firewall policy Activate packet inspection and create an allow rule to validate and verify the device certificate.

C- Implement an organization policy to verify the certificate from the access context.

D- Implement an Access Policy in BeyondCorp Enterprise to verify the device certificate Create an access binding with the access policy just created.

Answer:

D

Explanation:

https://cloud.google.com/beyondcorp?hl=pt-br

Question 6

Question Type: MultipleChoice

You manage a fleet of virtual machines (VMs) in your organization. You have encountered issues with lack of patching in many VMs. You need to automate regular patching in your VMs and view the patch management data across multiple projects.

What should you do?

Choose 2 answers

Options:

A- Deploy patches with VM Manager by using OS patch management

B- View patch management data in VM Manager by using OS patch management.

C- Deploy patches with Security Command Center by using Rapid Vulnerability Detection.

D- View patch management data in a Security Command Center dashboard.

E- View patch management data in Artifact Registry.

Answer:

A, B

Explanation:

https://cloud.google.com/compute/docs/os-patch-management

Question 7

Question Type: MultipleChoice

Your Google Cloud environment has one organization node, one folder named Apps." and several projects within that folder The organizational node enforces the constraints/iam.allowedPolicyMemberDomains organization policy, which allows members from the terramearth.com organization The "Apps" folder enforces the constraints/iam.allowedPolicyMemberDomains organization policy, which allows members from the flowlogistic.com organization. It also has the inheritFromParent: false property.

You attempt to grant access to a project in the Apps folder to the user testuser@terramearth.com.

What is the result of your action and why?

Options:

A- The action fails because a constraints/iam.allowedPolicyMemberDomains organization policy must

be defined on the current project to deactivate the constraint temporarily.

B- The action fails because a constraints/iam.allowedPolicyMemberDomains organization policy is in place and only members from the flowlogistic.com organization are allowed.

C- The action succeeds because members from both organizations, terramearth. com or flowlogistic.com, are allowed on projects in the 'Apps' folder

D- The action succeeds and the new member is successfully added to the project's Identity and Access Management (1AM) policy because all policies are inherited by underlying folders and projects.

Answer:

B

Explanation:

The action fails because a constraints/iam.allowedPolicyMemberDomains organization policy is in place and only members from the flowlogistic.com organization are allowed. The inheritFromParent: false property on the "Apps" folder means that it does not inherit the organization policy from the organization node. Therefore, only the policy set at the folder level applies, which allows only members from the flowlogistic.com organization. As a result, the attempt to grant access to the user testuser@terramearth.com fails because this user is not a member of the flowlogistic.com organization.

Question 8

Question Type: MultipleChoice

You control network traffic for a folder in your Google Cloud environment. Your folder includes multiple projects and Virtual Private Cloud (VPC) networks You want to enforce on the folder level that egress connections are limited only to IP range 10.58.5.0/24 and only from the VPC network dev-vpc." You want to minimize implementation and maintenance effort

What should you do?

Options:

A- * 1. Attach external IP addresses to the VMs in scope.
* 2. Configure a VPC Firewall rule in 'dev-vpc' that allows egress connectivity to IP range 10.58.5.0/24 for all source addresses in this network.

B- * 1. Attach external IP addresses to the VMs in scope.
* 2. Define and apply a hierarchical firewall policy on folder level to deny all egress connections and to allow egress to IP range 10 58.5.0/24 from network dev-vpc.

C- * 1. Leave the network configuration of the VMs in scope unchanged.
* 2. Create a new project including a new VPC network 'new-vpc.'
* 3 Deploy a network appliance in 'new-vpc' to filter access requests and only allow egress connections from -dev-vpc' to 10.58.5.0/24.

D- * 1 Leave the network configuration of the VMs in scope unchanged
* 2 Enable Cloud NAT for dev-vpc' and restrict the target range in Cloud NAT to 10.58.5 0/24.

Answer:

B

Explanation:

This approach allows you to control network traffic at the folder level. By attaching external IP addresses to the VMs in scope, you can ensure that the VMs have a unique, routable IP address for outbound connections. Then, by defining and applying a hierarchical firewall policy at the folder level, you can enforce that egress connections are limited to the specified IP range and only from the specified VPC network.

Question 9

Question Type: MultipleChoice

Your organization develops software involved in many open source projects and is concerned about software supply chain threats You need to deliver provenance for the build to demonstrate the software is untampered.

What should you do?

Options:

A- * 1- Generate Supply Chain Levels for Software Artifacts (SLSA) level 3 assurance by using Cloud Build.
* 2. View the build provenance in the Security insights side panel within the Google Cloud console.

B- * 1. Review the software process.
* 2. Generate private and public key pairs and use Pretty Good Privacy (PGP) protocols to sign the output software artifacts together with a file containing the address of your enterprise and point of contact.
* 3. Publish the PGP signed attestation to your public web page.

C- * 1, Publish the software code on GitHub as open source.
* 2. Establish a bug bounty program, and encourage the open source community to review, report, and fix the vulnerabilities.

D- * 1. Hire an external auditor to review and provide provenance
* 2. Define the scope and conditions.
* 3. Get support from the Security department or representative.
* 4. Publish the attestation to your public web page.

Answer:

A

Explanation:

https://cloud.google.com/build/docs/securing-builds/view-build-provenance

Question 10

Question Type: MultipleChoice

You are migrating an application into the cloud The application will need to read data from a Cloud Storage bucket. Due to local regulatory requirements, you need to hold the key material used for encryption fully under your control and you require a valid rationale for accessing the key material.

What should you do?

Options:

A- Encrypt the data in the Cloud Storage bucket by using Customer Managed Encryption Keys. Configure an 1AM deny policy for unauthorized groups

B- Encrypt the data in the Cloud Storage bucket by using Customer Managed Encryption Keys backed by a Cloud Hardware Security Module (HSM). Enable data access logs.

C- Generate a key in your on-premises environment and store it in a Hardware Security Module (HSM) that is managed on-premises Use this key as an external key in the Cloud Key Management Service (KMS). Activate Key Access Justifications (KAJ) and set the external key system to reject unauthorized accesses.

D- Generate a key in your on-premises environment to encrypt the data before you upload the data to the Cloud Storage bucket Upload the key to the Cloud Key Management Service (KMS). Activate Key Access Justifications (KAJ) and have the external key system reject unauthorized accesses.

Answer:

C

Explanation:

By generating a key in your on-premises environment and storing it in an HSM that you manage, you're ensuring that the key material is fully under your control. Using the key as an external key in Cloud KMS allows you to use the key with Google Cloud services without having the key stored on Google Cloud. Activating Key Access Justifications (KAJ) provides a reason every time the key is accessed, and you can configure the external key system to reject unauthorized access attempts.

Question 11

Question Type: MultipleChoice

You are deploying regulated workloads on Google Cloud. The regulation has data residency and data access requirements. It also requires that support is provided from the same geographical location as where the data resides.

What should you do?

Options:

A- Enable Access Transparency Logging.

B- Deploy resources only to regions permitted by data residency requirements

C- Use Data Access logging and Access Transparency logging to confirm that no users are accessing data from another region.

D- Deploy Assured Workloads.

Answer:

D

Explanation:

Assured Workloads for Google Cloud allows you to deploy regulated workloads with data residency, access, and support requirements. It helps you configure your environment in a manner that aligns with specific compliance frameworks and standards.