Google Professional-Cloud-Security-Engineer Practice Questions

Shared by Holloway on 24-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You need to set up two network segments: one with an untrusted subnet and the other with a trusted subnet. You want to configure a virtual appliance such as a next-generation firewall (NGFW) to inspect all traffic between the two network segments. How should you design the network to inspect the traffic?

Options:

A- 1. Set up one VPC with two subnets: one trusted and the other untrusted.2. Configure a custom route for all traffic (0.0.0.0/0) pointed to the virtual appliance.
B- 1. Set up one VPC with two subnets: one trusted and the other untrusted.2. Configure a custom route for all RFC1918 subnets pointed to the virtual appliance.
C- 1. Set up two VPC networks: one trusted and the other untrusted, and peer them together.2. Configure a custom route on each network pointed to the virtual appliance.
D- 1. Set up two VPC networks: one trusted and the other untrusted.2. Configure a virtual appliance using multiple network interfaces, with each interface connected to one of the VPC networks.

Answer:

D

Explanation:

Multiple network interfaces. The simplest way to connect multiple VPC networks through a virtual appliance is by using multiple network interfaces, with each interface connecting to one of the VPC networks. Internet and on-premises connectivity is provided over one or two separate network interfaces. With many NGFW products, internet connectivity is connected through an interface marked as untrusted in the NGFW software.

https://cloud.google.com/architecture/best-practices-vpc-design#l7

This architecture has multiple VPC networks that are bridged by an L7 next-generation firewall (NGFW) appliance, which functions as a multi-NIC bridge between VPC networks. An untrusted, outside VPC network is introduced to terminate hybrid interconnects and internet-based connections that terminate on the outside leg of the L7 NGFW for inspection. There are many variations on this design, but the key principle is to filter traffic through the firewall before the traffic reaches trusted VPC networks.

Question 2

Question Type: MultipleChoice

Your company's detection and response team requires break-glass access to the Google Cloud organization in the event of a security investigation At the end of each day, all security group membership is removed You need to automate user provisioning to a Cloud Identity security group You have created a service account to provision group memberships Your solution must follow Google-recommended practices and comply with the principle of least privilege What should you do?

Options:

A- In Google Workspace, grant the service account client ID access to the scope, https://wwwgoogleapiscom/auth/admindirectorygroup, by using domain-wide delegation, and use a service account key
B- In Google Workspace, grant the service account client ID access to the scope, https://wwwgoogleapiscom/auth/admindirectorygroup, by using domain-wide delegation Use Application Default Credentials with the resource-attached service account
C- In Google Workspace, grant the Groups Editor role to the service account Enable the Cloud Identity API Use a service account key
D- In Google Workspace, grant the Groups Editor role to the service account, enable the Cloud Identity API, and use Application Default Credentials with the resource-attached service account

Answer:

B

Explanation:

The problem requires automating user provisioning to a Cloud Identity security group using a service account, adhering to Google-recommended practices and the principle of least privilege

Cloud Identity Groups and Google Workspace: Cloud Identity groups are managed as part of Google Workspace To programmatically manage Google Workspace resources (like groups), you typically use the Admin SDK APIs

Domain-Wide Delegation: Service accounts cannot directly authenticate to Google Workspace APIs using IAM roles Instead, they require 'domain-wide delegation' to impersonate a user with the necessary administrative privileges within Google Workspace This allows a service account to access user data or perform administrative tasks across the domain The correct scope for managing groups is https://wwwgoogleapiscom/auth/admindirectorygroupExtract Reference: 'To allow a service account to access user data on behalf of users in a Google Workspace domain, you must delegate domain-wide authority to your service account' (Google Cloud documentation:
https://developersgooglecom/identity/protocols/oauth2/service-account#delegating)

Extract Reference (Admin SDK Scopes): The https://wwwgoogleapiscom/auth/admindirectorygroup scope is explicitly listed for 'View and manage all groups on the domain' (Google Workspace Admin SDK documentation: https://developersgooglecom/admin-sdk/directory/v1/scopes)

Application Default Credentials (ADC) with Resource-Attached Service Account: Google-recommended practices strongly advise against using service account keys directly for authentication when running on Google Cloud infrastructure Instead, it's recommended to use Application Default Credentials (ADC) with a service account attached to the resource (eg, a Compute Engine VM, Cloud Run service, or Cloud Functions) This method manages credentials automatically and securely, reducing the risk associated with managing and rotating keysExtract Reference: 'For most Google Cloud services, Application Default Credentials (ADC) is the recommended way to authenticate' and 'When running code in a Google Cloud environment, such as Compute Engine, Cloud Run, or Cloud Functions, use the built-in service account to authenticate automatically with ADC This is the most secure approach, as you don't need to manually create or manage service account keys' (Google Cloud documentation: https://cloudgooglecom/docs/authentication/production)

Options C and D are incorrect because granting an IAM role like 'Groups Editor' in Google Cloud does not enable a service account to manage Google Workspace (Cloud Identity) group memberships; domain-wide delegation is required for that Option A uses a service account key, which is less secure than ADC with a resource-attached service account according to Google's recommendations

Therefore, option B is the most aligned with Google's recommended practices for securely automating group provisioning using a service account and domain-wide delegation

Question 3

Question Type: MultipleChoice

location and to deploy different types of models in a consistent way You must ensure that your users can only access the approved models What should you do?

Options:

A- Configure IAM permissions on individual Model Garden to restrict access to specific models
B- Regularly audit user activity logs in Vertex AI to identify and revoke access to unapproved models
C- Train custom models within your Vertex AI project and restrict user access to these models
D- Implement an organization policy that restricts the vertexaiallowedModels constraint

Answer:

D

Explanation:

The problem states that the organization is using Model Garden and needs to ensure users can only access approved models This implies a need for a central, enforceable control mechanism

Organization Policies and Constraints: Google Cloud Organization Policy Service allows administrators to centrally control resources across an organization Constraints are specific types of restrictions that can be applied For AI Platform (which includes Vertex AI and Model Garden), there are specific constraints designed to control model usage

vertexaiallowedModels Constraint: This specific organization policy constraint is designed precisely to restrict which models can be used within a given organization, folder, or project It provides a centralized way to define a list of approved models that users are allowed to accessExtract Reference: 'The vertexaiallowedModels constraint allows you to specify a list of model URIs that are allowed to be used within the resource hierarchy' and 'This constraint helps organizations enforce compliance and control which models are consumed by their users' (Google Cloud documentation, typically found under Organization Policy Service constraints for Vertex AI or AI Platform)

Let's evaluate the other options:

A Configure IAM permissions on individual Model Garden to restrict access to specific models: IAM (Identity and Access Management) typically grants permissions at a broader resource level (eg, project, dataset, model resource) While you can control who can manage models, directly restricting access to specific models within Model Garden for consumption via IAM roles on individual models is not the primary mechanism for enforcing a list of approved models across an organization in a preventative way Organization policies are designed for this kind of broad, preventative control

B Regularly audit user activity logs in Vertex AI to identify and revoke access to unapproved models: Auditing logs is a reactive measure While important for monitoring and detecting violations, it does not prevent users from accessing unapproved models in the first place The requirement is to ensure they can only access approved models, implying a proactive control

C Train custom models within your Vertex AI project and restrict user access to these models: This is about managing access to custom-trained models, not about controlling access to the collection of models in Model Garden, which often includes pre-trained or publicly available models that need to be whitelisted It doesn't address the requirement of ensuring users only access approved models from the broader Model Garden collection

Question 4

Question Type: MultipleChoice

Your security team wants to implement a defense-in-depth approach to protect sensitive data

stored in a Cloud Storage bucket. Your team has the following requirements:

The Cloud Storage bucket in Project A can only be readable from Project B.

The Cloud Storage bucket in Project A cannot be accessed from outside the network.

Data in the Cloud Storage bucket cannot be copied to an external Cloud Storage bucket.

What should the security team do?

Options:

A- Enable domain restricted sharing in an organization policy, and enable uniform bucket-level access on the Cloud Storage bucket.
B- Enable VPC Service Controls, create a perimeter around Projects A and B. and include the Cloud Storage API in the Service Perimeter configuration.
C- Enable Private Access in both Project A and B's networks with strict firewall rules that allow communication between the networks.
D- Enable VPC Peering between Project A and B's networks with strict firewall rules that allow communication between the networks.

Answer:

B

Explanation:

VPC Peering is between organizations not between Projects in an organization. That is Shared VPC. In this case, both projects are in same organization so having VPC Service Controls around both projects with necessary rules should be fine.

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

Question 5

Question Type: MultipleChoice

You are a security engineer at a finance company. Your organization plans to store data on Google Cloud, but your leadership team is worried about the security of their highly sensitive data Specifically, your

company is concerned about internal Google employees' ability to access your company's data on Google Cloud. What solution should you propose?

Options:

A- Use customer-managed encryption keys.
B- Use Google's Identity and Access Management (IAM) service to manage access controls on Google Cloud.
C- Enable Admin activity logs to monitor access to resources.
D- Enable Access Transparency logs with Access Approval requests for Google employees.

Answer:

D

Explanation:

https://cloud.google.com/access-transparency Access approval Explicitly approve access to your data or configurations on Google Cloud. Access Approval requests, when combined with Access Transparency logs, can be used to audit an end-to-end chain from support ticket to access request to approval, to eventual access.

Question 6

Question Type: MultipleChoice

You plan to deploy your cloud infrastructure using a CI/CD cluster hosted on Compute Engine. You want to minimize the risk of its credentials being stolen by a third party. What should you do?

Options:

A- Create a dedicated Cloud Identity user account for the cluster. Use a strong self-hosted vault solution to store the user's temporary credentials.
B- Create a dedicated Cloud Identity user account for the cluster. Enable the constraints/iam.disableServiceAccountCreation organization policy at the project level.
C- Create a custom service account for the cluster Enable the constraints/iam.disableServiceAccountKeyCreation organization policy at the project level.
D- Create a custom service account for the cluster Enable the constraints/iam.allowServiceAccountCredentialLifetimeExtension organization policy at the project level.

Answer:

C

Explanation:

Disable service account key creation You can use the iam.disableServiceAccountKeyCreation boolean constraint to disable the creation of new external service account keys. This allows you to control the use of unmanaged long-term credentials for service accounts. When this constraint is set, user-managed credentials cannot be created for service accounts in projects affected by the constraint.
https://cloud.google.com/resource-manager/docs/organization-policy/restricting-service-accounts#example_policy_boolean_constraint

Question 7

Question Type: MultipleChoice

Your organization uses the top-tier folder to separate application environments (prod and dev). The developers need to see all application development audit logs but they are not permitted to review production logs. Your security team can review all logs in production and development environments. You must grant Identity and Access Management (1AM) roles at the right resource level tor the developers and security team while you ensure least privilege.

What should you do?

Options:

A- * 1 Grant logging, viewer rote to the security team at the organization resource level.
* 2 Grant logging, viewer rote to the developer team at the folder resource level that contains all the dev projects.
B- * 1 Grant logging. viewer rote to the security team at the organization resource level.
* 2 Grant logging. admin role to the developer team at the organization resource level.
C- * 1 Grant logging.admin role to the security team at the organization resource level.
* 2 Grant logging. viewer rote to the developer team at the folder resource level that contains all the dev projects.
D- * 1 Grant logging.admin role to the security team at the organization resource level.
* 2 Grant logging.admin role to the developer team at the organization resource level.

Answer:

C

Explanation:

To ensure that the developers can view audit logs for the development environment and the security team can review all logs, you should grant IAM roles at the appropriate resource levels:

Grant logging.admin Role to the Security Team:

Assign the logging.admin role to the security team at the organization resource level.

This grants the security team full access to all logging data across the organization, including both production and development environments.

Grant logging.viewer Role to the Developer Team:

Assign the logging.viewer role to the developer team at the folder resource level that contains all the development projects.

This restricts the developers' access to only view logs in the development environment, ensuring they do not have access to production logs.

By using these roles and assigning them at the appropriate levels, you ensure that each team has the access they need while adhering to the principle of least privilege.

IAM Roles for Cloud Logging

Resource Hierarchy in Google Cloud

Question 8

Question Type: MultipleChoice

You have a highly sensitive BigQuery workload that contains personally identifiable information (Pll) that you want to ensure is not accessible from the internet. To prevent data exfiltration only requests from authorized IP addresses are allowed to query your BigQuery tables.

What should you do?

Options:

A- Use service perimeter and create an access level based on the authorized source IP address as the condition.
B- Use Google Cloud Armor security policies defining an allowlist of authorized IP addresses at the global HTTPS load balancer.
C- Use the Restrict allowed Google Cloud APIs and services organization policy constraint along with Cloud Data Loss Prevention (DLP).

D- Use the Restrict Resource service usage organization policy constraint along with Cloud Data Loss Prevention (DLP).

Answer:

A

Explanation:

Enable VPC Service Controls:

VPC Service Controls help mitigate the risk of data exfiltration by allowing you to define a security perimeter around GCP resources.

Set up a service perimeter around your BigQuery project to restrict data access to within the defined perimeter.

Create Access Levels:

In the Google Cloud Console, navigate to the Access Context Manager.

Define access levels based on IP address conditions, specifying the authorized source IP addresses that are allowed to access your BigQuery resources.

These access levels are used to enforce policies that restrict who can access your sensitive data based on their IP addresses.

Apply Service Perimeter with Access Levels:

Apply the created access levels to the service perimeter to ensure that only requests originating from the specified IP addresses are able to access BigQuery tables.

This setup ensures that the sensitive PII data is not accessible from unauthorized IP addresses, reducing the risk of data exfiltration.

VPC Service Controls

Access Context Manager

Defining Access Levels

Question 9

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:

B, C

Explanation:

To meet the requirements for exporting and auditing security logs in near real-time for login activity events and API calls:

Organization-Level Log Sink with Pub/Sub: Create a log sink at the organization level to ensure logs from all projects are captured. Use the includeChildren parameter to include logs from all child resources (projects). Set the destination to a Pub/Sub topic to facilitate near real-time log export to an external SIEM.

Enable Data Access Audit Logs: Enable Data Access audit logs at the organization level to capture and export detailed information about API calls that modify configurations of Google Cloud resources across all projects.

These steps ensure comprehensive logging and real-time export capabilities, which are crucial for security auditing and monitoring.

Reference

Audit Logs Overview

Exporting with Sinks