Professional Cloud Security Engineer.VCEplus.premium.exam.50q

Passing Score: 800
Time Limit: 120 min
File Version: 1.0

Google Cloud Certified - Professional Cloud Security Engineer

Version 1.0

Exam A

QUESTION 1
Your team needs to make sure that a Compute Engine instance does not have access to the internet or to any Google APIs or services.

Which two settings must remain disabled to meet these requirements? (Choose two.)

A. Public IP
B. IP Forwarding
C. Private Google Access
D. Static routes
E. IAM Network User Role

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://cloud.google.com/vpc/docs/configure-private-google-access

QUESTION 2 Which two implied firewall rules are defined on a VPC network?
(Choose two.)

A. A rule that allows all outbound connections
B. A rule that denies all inbound connections
C. A rule that blocks all inbound port 25 connections
D. A rule that blocks all outbound connections
E. A rule that allows all inbound port 80 connections

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Reference: https://cloud.google.com/vpc/docs/firewalls

QUESTION 3 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Your team wants to centrally manage GCP IAM permissions from their on-premises Active Directory Service. Your team wants to manage permissions by AD group membership.

What should your team do to meet these requirements?
A. Set up Cloud Directory Sync to sync groups, and set IAM permissions on the groups.

B. Set up SAML 2.0 Single Sign-On (SSO), and assign IAM permissions to the groups.
C. Use the Cloud Identity and Access Management API to create groups and IAM permissions from Active Directory.
D. Use the Admin SDK to create groups and assign IAM permissions from Active Directory.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://cloud.google.com/blog/products/identity-security/using-your-existing-identity-management-system-with-google-cloud-platform

QUESTION 5
When creating a secure container image, which two items should you incorporate into the build if possible? (Choose two.)

A. Ensure that the app does not run as PID 1.
B. Package a single app as a container.
C. Remove any unnecessary tools not needed by the app.
D. Use public container images as a base image for the app.
E. Use many container image layers to hide sensitive information.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://cloud.google.com/solutions/best-practices-for-building-containers

QUESTION 6
A customer needs to launch a 3-tier internal web application on Google Cloud Platform (GCP). The customer's internal compliance requirements dictate that end-user access may only be allowed if the traffic seems to originate from a specific known good CIDR. The customer accepts the risk that their application will only have SYN flood DDoS protection. They want to use GCP's native SYN flood protection.

Which product should be used to meet these requirements?

A. Cloud Armor
B. VPC Firewall Rules
C. Cloud Identity and Access Management
D. Cloud CDN

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://cloud.google.com/blog/products/identity-security/understanding-google-cloud-armors-new-waf-capabilities

QUESTION 7
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: DE

Section: (none)
Explanation

Explanation/Reference:
Reference: https://cloud.google.com/solutions/secure-data-workloads-use-cases

QUESTION 8 A customer implements Cloud Identity-Aware Proxy for their ERP system hosted on Compute Engine. Their security team wants to add a security layer so that the ERP systems only accept traffic from Cloud Identity-Aware Proxy.

What should the customer do to meet these requirements?

A. Make sure that the ERP system can validate the JWT assertion in the HTTP requests.
B. Make sure that the ERP system can validate the identity headers in the HTTP requests.
C. Make sure that the ERP system can validate the x-forwarded-for headers in the HTTP requests.
D. Make sure that the ERP system can validate the user's unique identifier headers in the HTTP requests.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
A company has been running their application on Compute Engine. A bug in the application allowed a malicious user to repeatedly execute a script that results in the Compute Engine instance crashing. Although the bug has been fixed, you want to get notified in case this hack re-occurs.

What should you do?

A. Create an Alerting Policy in Stackdriver using a Process Health condition, checking that the number of executions of the script remains below the desired threshold. Enable notifications.
B. Create an Alerting Policy in Stackdriver using the CPU usage metric. Set the threshold to 80% to be notified when the CPU usage goes above this 80%.
C. Log every execution of the script to Stackdriver Logging. Create a User-defined metric in Stackdriver Logging on the logs, and create a Stackdriver Dashboard displaying the metric.
D. Log every execution of the script to Stackdriver Logging. Configure BigQuery as a log sink, and create a BigQuery scheduled query to count the number of executions in a specific timeframe.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://cloud.google.com/logging/docs/logs-based-metrics/

QUESTION 10
Your team needs to obtain a unified log view of all development cloud projects in your SIEM. The development projects are under the NONPROD organization folder with the test and pre-production projects. The development projects share the ABC-BILLING billing account with the rest of the organization.

Which logging export strategy should you use to meet the requirements?

A. 1. Export logs to a Cloud Pub/Sub topic with `folders/NONPROD` parent and includeChildren property set to `True` in a dedicated SIEM project.
   2. Subscribe SIEM to the topic.
B. 1. Create a Cloud Storage sink with `billingAccounts/ABC-BILLING` parent and includeChildren property set to `False` in a dedicated SIEM project.
   2. Process Cloud Storage objects in SIEM.
C. 1. Export logs in each dev project to a Cloud Pub/Sub topic in a dedicated SIEM project.
   2. Subscribe SIEM to the topic.
D. 1. Create a Cloud Storage sink with a publicly shared Cloud Storage bucket in each project.
   2. Process Cloud Storage objects in SIEM.

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 11
A customer needs to prevent attackers from hijacking their domain/IP and redirecting users to a malicious site through a man-in-the-middle attack.

Which solution should this customer use?

A. VPC Flow Logs
B. Cloud Armor
C. DNS Security Extensions
D. Cloud Identity-Aware Proxy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://cloud.google.com/blog/products/gcp/dnssec-now-available-in-cloud-dns

QUESTION 12
A customer deploys an application to App Engine and needs to check for Open Web Application Security Project (OWASP) vulnerabilities.

Which service should be used to accomplish this?

A. Cloud Armor
B. Google Cloud Audit Logs
C. Cloud Security Scanner
D. Forseti Security

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://cloud.google.com/security-scanner/

QUESTION 13
A customer's data science group wants to use Google Cloud Platform (GCP) for their analytics workloads. Company policy dictates that all data must be company-owned and all user authentications must go through their own Security Assertion Markup Language (SAML) 2.0 Identity Provider (IdP). The Infrastructure Operations Systems Engineer was trying to set up Cloud Identity for the customer and realized that their domain was already being used by G Suite.

How should you best advise the Systems Engineer to proceed with the least disruption?

A. Contact Google Support and initiate the Domain Contestation Process to use the domain name in your new Cloud Identity domain.
B. Register a new domain name, and use that for the new Cloud Identity domain.
C. Ask Google to provision the data science manager's account as a Super Administrator in the existing domain.
D. Ask customer's management to discover any other uses of Google managed services, and work with the existing Super Administrator.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14

A business unit at a multinational corporation signs up for GCP and starts moving workloads into GCP. The business unit creates a Cloud Identity domain with an organizational resource that has hundreds of projects. Your team becomes aware of this and wants to take over managing permissions and auditing the domain resources.

Which type of access should your team grant to meet this requirement?

A. Organization Administrator
B. Security Reviewer
C. Organization Role Administrator
D. Organization Policy Administrator

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15 An application running on a Compute Engine instance needs to read data from a Cloud Storage bucket. Your team does not allow Cloud Storage buckets to be globally readable and wants to ensure the principle of least privilege.

Which option meets the requirement of your team?

A. Create a Cloud Storage ACL that allows read-only access from the Compute Engine instance's IP address and allows the application to read from the bucket without credentials.
B. Use a service account with read-only access to the Cloud Storage bucket, and store the credentials to the service account in the config of the application on the Compute Engine instance.
C. Use a service account with read-only access to the Cloud Storage bucket to retrieve the credentials from the instance metadata.
D. Encrypt the data in the Cloud Storage bucket using Cloud KMS, and allow the application to decrypt the data with the KMS key.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
An organization's typical network and security review consists of analyzing application transit routes, request handling, and firewall rules. They want to enable their developer teams to deploy new applications without the overhead of this full review.

How should you advise this organization?

A. Use Forseti with Firewall filters to catch any unwanted configurations in production.
B. Mandate use of infrastructure as code and provide static analysis in the CI/CD pipelines to enforce policies.
C. Route all VPC traffic through customer-managed routers to detect malicious patterns in production.
D. All production applications will run on-premises. Allow developers free rein in GCP as their dev and QA platforms.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
An employer wants to track how bonus compensations have changed over time to identify employee outliers and correct earning disparities. This task must be performed without exposing the sensitive compensation data for any individual and must be reversible to identify the outlier.

Which Cloud Data Loss Prevention API technique should you use to accomplish this?

A. Generalization
B. Redaction
C. CryptoHashConfig
D. CryptoReplaceFfxFpeConfig

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
An organization adopts Google Cloud Platform (GCP) for application hosting services and needs guidance on setting up password requirements for their Cloud Identity account. The organization has a password policy requirement that corporate employee passwords must have a minimum number of characters.

Which Cloud Identity password guidelines can the organization use to inform their new requirements?

A. Set the minimum length for passwords to be 8 characters.
B. Set the minimum length for passwords to be 10 characters.
C. Set the minimum length for passwords to be 12 characters.
D. Set the minimum length for passwords to be 6 characters.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
You need to follow Google-recommended practices to leverage envelope encryption and encrypt data at the application layer.

What should you do?

A. Generate a data encryption key (DEK) locally to encrypt the data, and generate a new key encryption key (KEK) in Cloud KMS to encrypt the DEK. Store both the encrypted data and the encrypted DEK.
B. Generate a data encryption key (DEK) locally to encrypt the data, and generate a new key encryption key (KEK) in Cloud KMS to encrypt the DEK. Store both the encrypted data and the KEK.
C. Generate a new data encryption key (DEK) in Cloud KMS to encrypt the data, and generate a key encryption key (KEK) locally to encrypt the key. Store both the encrypted data and the encrypted DEK.
D. Generate a new data encryption key (DEK) in Cloud KMS to encrypt the data, and generate a key encryption key (KEK) locally to encrypt the key. Store both the encrypted data and the KEK.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://cloud.google.com/kms/docs/envelope-encryption

QUESTION 20 How should a customer reliably deliver Stackdriver logs from GCP to their on-premises
SIEM system?

A. Send all logs to the SIEM system via an existing protocol such as syslog.
B. Configure every project to export all their logs to a common BigQuery DataSet, which will be queried by the SIEM system.
C. Configure Organizational Log Sinks to export logs to a Cloud Pub/Sub Topic, which will be sent to the SIEM via Dataflow.
D. Build a connector for the SIEM to query for all logs in real time from the GCP RESTful JSON APIs.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
In order to meet PCI DSS requirements, a customer wants to ensure that all outbound traffic is authorized.

Which two cloud offerings meet this requirement without additional compensating controls? (Choose two.)

A. App Engine
B. Cloud Functions
C. Compute Engine
D. Google Kubernetes Engine
E. Cloud Storage

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://cloud.google.com/solutions/pci-dss-compliance-in-gcp

QUESTION 22
A website design company recently migrated all customer sites to App Engine. Some sites are still in progress and should only be visible to customers and company employees from any location.

Which solution will restrict access to the in-progress sites?

A. Upload an .htaccess file containing the customer and employee user accounts to App Engine.
B. Create an App Engine firewall rule that allows access from the customer and employee networks and denies all other traffic.
C. Enable Cloud Identity-Aware Proxy (IAP), and allow access to a Google Group that contains the customer and employee user accounts.
D. Use Cloud VPN to create a VPN connection between the relevant on-premises networks and the company's GCP Virtual Private Cloud (VPC) network.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
When working with agents in a support center via online chat, an organization's customers often share pictures of their documents with personally identifiable information (PII). The organization that owns the support center is concerned that the PII is being stored in their databases as part of the regular chat logs they retain for review by internal or external analysts for customer service trend analysis.

Which Google Cloud solution should the organization use to help resolve this concern for the customer while still maintaining data utility?

A. Use Cloud Key Management Service (KMS) to encrypt the PII data shared by customers before storing it for analysis.
B. Use Object Lifecycle Management to make sure that all chat records with PII in them are discarded and not saved for analysis.
C. Use the image inspection and redaction actions of the DLP API to redact PII from the images before storing them for analysis.
D. Use the generalization and bucketing actions of the DLP API solution to redact PII from the texts before storing them for analysis.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference; https://cloud.google.com/dlp/docs/deidentify-sensitive-data

QUESTION 24
A company's application is deployed with a user-managed Service Account key. You want to use Google-recommended practices to rotate the key.

What should you do?

A. Open Cloud Shell and run `gcloud iam service-accounts enable-auto-rotate --iam-account=IAM_ACCOUNT`.
B. Open Cloud Shell and run `gcloud iam service-accounts keys rotate --iam-account=IAM_ACCOUNT --key=NEW_KEY`.
C. Create a new key, and use the new key in the application. Delete the old key from the Service Account.
D. Create a new key, and use the new key in the application. Store the old key on the system as a backup key.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://cloud.google.com/iam/docs/understanding-service-accounts

QUESTION 25
Your team needs to configure their Google Cloud Platform (GCP) environment so they can centralize the control over networking resources like firewall rules, subnets, and routes. They also have an on-premises environment where resources need access back to the GCP resources through a private VPN connection. The networking resources will need to be controlled by the network security team.

Which type of networking design should your team use to meet these requirements?

A. Shared VPC Network with a host project and service projects
B. Grant Compute Admin role to the networking team for each engineering project
C. VPC peering between all engineering projects using a hub and spoke model
D. Cloud VPN Gateway between all engineering projects using a hub and spoke model

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations#centralize_network_control

QUESTION 26
An organization is migrating from their current on-premises productivity software systems to G Suite. Some network security controls were in place that were mandated by a regulatory body in their region for their previous on-premises system. The organization's risk team wants to ensure that network security controls are maintained and effective in G Suite. A security architect supporting this migration has been asked to ensure that network security controls are in place as part of the new shared responsibility model between the organization and Google Cloud.

What solution would help meet the requirements?

A. Ensure that firewall rules are in place to meet the required controls.
B. Set up Cloud Armor to ensure that network security controls can be managed for G Suite.
C. Network security is a built-in solution and Google's Cloud responsibility for SaaS products like G Suite.
D. Set up an array of Virtual Private Cloud (VPC) networks to control network security as mandated by the relevant regulation.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
A customer's company has multiple business units. Each business unit operates independently, and each has their own engineering group. Your team wants visibility into all projects created within the company and wants to organize their Google Cloud Platform (GCP) projects based on different business units. Each business unit also requires separate sets of IAM permissions.

Which strategy should you use to meet these needs?

A. Create an organization node, and assign folders for each business unit.

B. Establish standalone projects for each business unit, using gmail.com accounts.
C. Assign GCP resources in a project, with a label identifying which business unit owns the resource.
D. Assign GCP resources in a VPC for each business unit to separate network access.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
A company has redundant mail servers in different Google Cloud Platform regions and wants to route customers to the nearest mail server based on location.

How should the company accomplish this?

A. Configure TCP Proxy Load Balancing as a global load balancing service listening on port 995.
B. Create a Network Load Balancer to listen on TCP port 995 with a forwarding rule to forward traffic based on location.
C. Use Cross-Region Load Balancing with an HTTP(S) load balancer to route traffic to the nearest region.
D. Use Cloud CDN to route the mail traffic to the closest origin mail server based on client IP address.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Your team sets up a Shared VPC Network where project co-vpc-prod is the host project. Your team has configured the firewall rules, subnets, and VPN gateway on the host project. They need to enable Engineering Group A to attach a Compute Engine instance to only the 10.1.1.0/24 subnet.

What should your team grant to Engineering Group A to meet this requirement?

A. Compute Network User Role at the host project level.
B. Compute Network User Role at the subnet level.
C. Compute Shared VPC Admin Role at the host project level.
D. Compute Shared VPC Admin Role at the service project level.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://cloud.google.com/vpc/docs/shared-vpc

QUESTION 30
A company migrated their entire data/center to Google Cloud Platform. It is running thousands of instances across multiple projects managed by different departments. You want to have a historical record of what was running in Google Cloud Platform at any point in time.

What should you do?

A. Use Resource Manager on the organization level.
B. Use Forseti Security to automate inventory snapshots.
C. Use Stackdriver to create a dashboard across all projects.
D. Use Security Command Center to view all assets across the organization.

Correct Answer: C

Section: (none)
Explanation
Explanation/Reference:

QUESTION 31
An organization is starting to move its infrastructure from its on-premises environment to Google Cloud Platform (GCP). The first step the organization wants to take is to migrate its current data backup and disaster recovery solutions to GCP for later analysis. The organization's production environment will remain on-premises for an indefinite time. The organization wants a scalable and cost-efficient solution.

Which GCP solution should the organization use?

A. BigQuery using a data pipeline job with continuous updates
B. Cloud Storage using a scheduled task and gsutil
C. Compute Engine Virtual Machines using Persistent Disk
D. Cloud Datastore using regularly scheduled batch upload jobs

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
You are creating an internal App Engine application that needs to access a user's Google Drive on the user's behalf. Your company does not want to rely on the current user's credentials. It also wants to follow Google-recommended practices.

What should you do?

A. Create a new Service account, and give all application users the role of Service Account User.
B. Create a new Service account, and add all application users to a Google Group. Give this group the role of Service Account User.
C. Use a dedicated G Suite Admin account, and authenticate the application's operations with these G Suite credentials.
D. Create a new service account, and grant it G Suite domain-wide delegation. Have the application use it to impersonate the user.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
A customer wants to move their sensitive workloads to a Compute Engine-based cluster using Managed Instance Groups (MIGs). The jobs are bursty and must be completed quickly. They have a requirement to be able to manage and rotate the encryption keys.

Which boot disk encryption solution should you use on the cluster to meet this customer's requirements?

A. Customer-supplied encryption keys (CSEK)
B. Customer-managed encryption keys (CMEK) using Cloud Key Management Service (KMS)C. Encryption by default
D. Pre-encrypting files before transferring to Google Cloud Platform (GCP) for analysis

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference https://cloud.google.com/kubernetes-engine/docs/how-to/dynamic-provisioning-cmek

QUESTION 34

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).

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
You are a member of the security team at an organization. Your team has a single GCP project with credit card payment processing systems alongside web applications and data processing systems. You want to reduce the scope of systems subject to PCI audit standards.

What should you do?

A. Use multi-factor authentication for admin access to the web application.
B. Use only applications certified compliant with PA-DSS.
C. Move the cardholder data environment into a separate GCP project.
D. Use VPN for all connections between your office and cloud environments.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://cloud.google.com/solutions/pci-dss-compliance-in-gcp

QUESTION 36
A retail customer allows users to upload comments and product reviews. The customer needs to make sure the text does not include sensitive data before the comments or reviews are published.

Which Google Cloud Service should be used to achieve this?

A. Cloud Key Management Service
B. Cloud Data Loss Prevention API
C. BigQuery
D. Cloud Security Scanner

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
A company allows every employee to use Google Cloud Platform. Each department has a Google Group, with all department members as group members. If a department member creates a new project, all members of that department should automatically have read-only access to all new project resources. Members of any other department should not have access to the project. You need to configure this behavior.

What should you do to meet these requirements?

A. Create a Folder per department under the Organization. For each department's Folder, assign the Project Viewer role to the Google Group related to that department.

B. Create a Folder per department under the Organization. For each department's Folder, assign the Project Browser role to the Google Group related to that department.
C. Create a Project per department under the Organization. For each department's Project, assign the Project Viewer role to the Google Group related to that department.
D. Create a Project per department under the Organization. For each department's Project, assign the Project Browser role to the Google Group related to that department.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
A customer's internal security team must manage its own encryption keys for encrypting data on Cloud Storage and decides to use customer-supplied encryption keys (CSEK).

How should the team complete this task?

A. Upload the encryption key to a Cloud Storage bucket, and then upload the object to the same bucket.
B. Use the gsutil command line tool to upload the object to Cloud Storage, and specify the location of the encryption key.
C. Generate an encryption key in the Google Cloud Platform Console, and upload an object to Cloud Storage using the specified key.
D. Encrypt the object, then use the gsutil command line tool or the Google Cloud Platform Console to upload the object to Cloud Storage.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://cloud.google.com/storage/docs/encryption/customer-supplied-keys

QUESTION 39
A customer has 300 engineers. The company wants to grant different levels of access and efficiently manage IAM permissions between users in the development and production environment projects. Which two steps should the company take to meet these requirements? (Choose two.)

A. Create a project with multiple VPC networks for each environment.
B. Create a folder for each development and production environment.
C. Create a Google Group for the Engineering team, and assign permissions at the folder level.
D. Create an Organizational Policy constraint for each folder environment.
E. Create projects for each environment, and grant IAM rights to each engineering user.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40 You want to evaluate GCP for PCI compliance. You need to identify Google's inherent controls.

Which document should you review to find the information?

A. Google Cloud Platform: Customer Responsibility Matrix
B. PCI DSS Requirements and Security Assessment Procedures
C. PCI SSC Cloud Computing Guidelines
D. Product documentation for Compute Engine

Correct Answer: C
Section: (none)

Explanation
Explanation/Reference:
Reference: https://cloud.google.com/solutions/pci-dss-compliance-in-gcp

QUESTION 41
Your company runs a website that will store PII on Google Cloud Platform. To comply with data privacy regulations, this data can only be stored for a specific amount of time and must be fully deleted after this specific period. Data that has not yet reached the time period should not be deleted. You want to automate the process of complying with this regulation.

What should you do?

A. Store the data in a single Persistent Disk, and delete the disk at expiration time.
B. Store the data in a single BigQuery table and set the appropriate table expiration time.
C. Store the data in a single Cloud Storage bucket and configure the bucket's Time to Live.
D. Store the data in a single BigTable table and set an expiration time on the column families.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42 A DevOps team will create a new container to run on Google Kubernetes Engine. As the application will be internet-facing, they want to minimize the attack surface of the container.

What should they do?

A. Use Cloud Build to build the container images.
B. Build small containers using small base images.
C. Delete non-used versions from Container Registry.
D. Use a Continuous Delivery tool to deploy the application.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://cloud.google.com/solutions/best-practices-for-building-containers

QUESTION 43
While migrating your organization's infrastructure to GCP, a large number of users will need to access GCP Console. The Identity Management team already has a well-established way to manage your users and want to keep using your existing Active Directory or LDAP server along with the existing SSO password.

What should you do?

A. Manually synchronize the data in Google domain with your existing Active Directory or LDAP server.
B. Use Google Cloud Directory Sync to synchronize the data in Google domain with your existing Active Directory or LDAP server.
C. Users sign in directly to the GCP Console using the credentials from your on-premises Kerberos compliant identity provider.
D. Users sign in using OpenID (OIDC) compatible IdP, receive an authentication token, then use that token to log in to the GCP Console.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://cloud.google.com/blog/products/identity-security/using-your-existing-identity-management-system-with-google-cloud-platform

QUESTION 44

Your company is using GSuite and has developed an application meant for internal usage on Google App Engine. You need to make sure that an external user cannot gain access to the application even when an employee's password has been compromised.

What should you do?

A. Enforce 2-factor authentication in GSuite for all users.
B. Configure Cloud Identity-Aware Proxy for the App Engine Application.
C. Provision user passwords using GSuite Password Sync.
D. Configure Cloud VPN between your private network and GCP.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
A large financial institution is moving its Big Data analytics to Google Cloud Platform. They want to have maximum control over the encryption process of data stored at rest in BigQuery.

What technique should the institution use?

A. Use Cloud Storage as a federated Data Source.
B. Use a Cloud Hardware Security Module (Cloud HSM).
C. Customer-managed encryption keys (CMEK).
D. Customer-supplied encryption keys (CSEK).

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://cloud.google.com/bigquery/docs/encryption-at-rest

QUESTION 46 A company is deploying their application on Google Cloud Platform. Company policy requires long-term data to be stored using a solution that can automatically replicate data over at least two geographic places.

Which Storage solution are they allowed to use?

A. Cloud Bigtable
B. Cloud BigQuery
C. Compute Engine SSD Disk
D. Compute Engine Persistent Disk

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://cloud.google.com/bigquery/docs/locations

QUESTION 47 A large e-retailer is moving to Google Cloud Platform with its ecommerce website. The company wants to ensure payment information is encrypted between the customer's browser and GCP when the customers checkout online.

What should they do?

A. Configure an SSL Certificate on an L7 Load Balancer and require encryption.
B. Configure an SSL Certificate on a Network TCP Load Balancer and require encryption.

C. Configure the firewall to allow inbound traffic on port 443, and block all other inbound traffic.
D. Configure the firewall to allow outbound traffic on port 443, and block all other outbound traffic.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
Applications often require access to “secrets” - small pieces of sensitive data at build or run time. The administrator managing these secrets on GCP wants to keep a track of “who did what, where, and when?” within their GCP projects.

Which two log streams would provide the information that the administrator is looking for? (Choose two.)

A. Admin Activity logs
B. System Event logs
C. Data Access logs
D. VPC Flow logs
E. Agent logs

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://cloud.google.com/kms/docs/secret-management

QUESTION 49
You are in charge of migrating a legacy application from your company datacenters to GCP before the current maintenance contract expires. You do not know what ports the application is using and no documentation is available for you to check. You want to complete the migration without putting your environment at risk.

What should you do?

A. Migrate the application into an isolated project using a “Lift & Shift” approach. Enable all internal TCP traffic using VPC Firewall rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly. B. Migrate the application into an isolated project using a “Lift & Shift” approach in a custom network. Disable all traffic within the VPC and look at the Firewall logs to determine what traffic should be allowed for the application to work properly.
C. Refactor the application into a micro-services architecture in a GKE cluster. Disable all traffic from outside the cluster using Firewall Rules. Use VPC Flow logs to determine what traffic should be allowed for the application to workproperly.
D. Refactor the application into a micro-services architecture hosted in Cloud Functions in an isolated project. Disable all traffic from outside your project using Firewall Rules. Use VPC Flow logs to determine what traffic should be allowedfor the application to work properly.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Your company has deployed an application on Compute Engine. The application is accessible by clients on port 587. You need to balance the load between the different instances running the application. The connection should be secured using TLS, and terminated by the Load Balancer.

What type of Load Balancing should you use?

A. Network Load Balancing
B. HTTP(S) Load Balancing
C. TCP Proxy Load Balancing
D. SSL Proxy Load Balancing
Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Reference: https://cloud.google.com/load-balancing/docs/ssl/