Professional Cloud Security Engineer

Passing Score: 800
Time Limit: 120 min
File Version: 1

Professional Cloud Security Engineer

Exam A

QUESTION 1

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 2

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 3
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 4
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 5
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 6
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 7

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 8

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 9
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 10
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 11
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 12
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 13

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 14

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 15

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 16

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 17

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 18
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 19
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 20
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 21
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 22
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 23

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 24

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 25

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 26
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 27
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 work properly.
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 allowed for the application to work properly.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
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/

QUESTION 29

Your team needs to prevent users from creating projects in the organization. Only the DevOps team should be allowed to create projects on behalf of the requester. Which two tasks should your team perform to handle this request? (Choose two.)

A. Remove all users from the Project Creator role at the organizational level.
B. Create an Organization Policy constraint, and apply it at the organizational level.
C. Grant the Project Editor role at the organizational level to a designated group of users. D. Add a designated group of users to the Project Creator role at the organizational level.
E. Grant the billing account creator role to the designated DevOps team.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
A customer deployed an application on Compute Engine that takes advantage of the elastic nature of cloud computing.

How can you work with Infrastructure Operations Engineers to best ensure that Windows Compute Engine VMs are up to date with all the latest OS patches?
A. Build new base images when patches are available, and use a CI/CD pipeline to rebuild VMs, deploying incrementally.
B. Federate a Domain Controller into Compute Engine, and roll out weekly patches via Group Policy Object.
C. Use Deployment Manager to provision updated VMs into new serving Instance Groups (IGs).
D. Reboot all VMs during the weekly maintenance window and allow the StartUp Script to download the latest patches from the internet.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
An organization receives an increasing number of phishing emails.

Which method should be used to protect employee credentials in this situation?

A. Multifactor Authentication

B. A strict password policy
C. Captcha on login pages
D. Encrypted emails

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
A customer is collaborating with another company to build an application on Compute Engine. The customer is building the application tier in their GCP Organization, and the other company is building the storage tier in a different GCP Organization. This is a 3-tier web application. Communication between portions of the application must not traverse the public internet by any means.

Which connectivity option should be implemented?

A. VPC peering
B. Cloud VPN
C. Cloud Interconnect
D. Shared VPC

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Your team wants to make sure Compute Engine instances running in your production project do not have public IP addresses. The frontend application Compute Engine instances will require public IPs. The product engineers have the Editor role to modify resources. Your team wants to enforce this requirement.

How should your team meet these requirements?

A. Enable Private Access on the VPC network in the production project.
B. Remove the Editor role and grant the Compute Admin IAM role to the engineers.

C. Set up an organization policy to only permit public IPs for the front-end Compute Engine instances.
D. Set up a VPC network with two subnets: one with public IPs and one without public IPs.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://cloud.google.com/compute/docs/ip-addresses/reserve-static-external-ip-address

QUESTION 34
A patch for a vulnerability has been released, and a DevOps team needs to update their running containers in Google Kubernetes Engine (GKE)

How should the DevOps team accomplish this?

A. Use Puppet or Chef to push out the patch to the running container.
B. Verify that auto upgrade is enabled; if so, Google will upgrade the nodes in a GKE cluster.
C. Update the application code or apply a patch, build a new image, and redeploy it.
D. Configure containers to automatically upgrade when the base image is available in Container Registry. **Correct Answer:** B

Section: (none)
Explanation

Explanation/Reference:
Reference: https://cloud.google.com/kubernetes-engine/docs/security-bulletins

QUESTION 35
For compliance reasons, an organization needs to ensure that in-scope PCI Kubernetes Pods reside on “in-scope” Nodes only. These Nodes can only contain the “in-scope” Pods.

How should the organization achieve this objective?

A. Add a nodeSelector field to the pod configuration to only use the Nodes labeled inscope: true.
B. Create a node pool with the label inscope: true and a Pod Security Policy that only allows the Pods to run on Nodes with that label.
C. Place a taint on the Nodes with the label inscope: true and effect NoSchedule and a toleration to match in the Pod configuration.
D. Run all in-scope Pods in the namespace “in-scope-pci”.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36

In an effort for your company messaging app to comply with FIPS 140-2, a decision was made to use GCP compute and network services. The messaging app architecture includes a Managed Instance Group (MIG) that controls a cluster of Compute Engine instances. The instances use Local SSDs for data caching and UDP for instance-to-instance communications. The app development team is willing to make any changes necessary to comply with the standard Which options should you recommend to meet the requirements?

A. Encrypt all cache storage and VM-to-VM communication using the BoringCrypto module.
B. Set Disk Encryption on the Instance Template used by the MIG to `customer-managed key` and use BoringSSL for all data transit between instances.
C. Change the app instance-to-instance communications from UDP to TCP and enable BoringSSL on clients' TLS connections.
D. Set Disk Encryption on the Instance Template used by the MIG to `Google-managed Key` and use BoringSSL library on all instance-to-instance communications.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37

A customer has an analytics workload running on Compute Engine that should have limited internet access.

Your team created an egress firewall rule to deny (priority 1000) all traffic to the internet.

The Compute Engine instances now need to reach out to the public repository to get security updates.

What should your team do?

A. Create an egress firewall rule to allow traffic to the CIDR range of the repository with a priority greater than 1000.
B. Create an egress firewall rule to allow traffic to the CIDR range of the repository with a priority less than 1000.
C. Create an egress firewall rule to allow traffic to the hostname of the repository with a priority greater than 1000.

D. Create an egress firewall rule to allow traffic to the hostname of the repository with a priority less than 1000.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
You want data on Compute Engine disks to be encrypted at rest with keys managed by Cloud Key Management Service (KMS). Cloud Identity and Access Management (IAM) permissions to these keys must be managed in a grouped way because the permissions should be the same for all keys.

What should you do?

A. Create a single KeyRing for all persistent disks and all Keys in this KeyRing. Manage the IAM permissions at the Key level.
B. Create a single KeyRing for all persistent disks and all Keys in this KeyRing. Manage the IAM permissions at the KeyRing level.
C. Create a KeyRing per persistent disk, with each Keying containing a single Key. Manage the IAM permissions at the Key level.
D. Create a KeyRing per persistent disk, with each KeyRing containing a single Key. Manage the IAM permissions at the KeyRing level.

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:

QUESTION 39
A customer terminates an engineer and needs to make sure the engineer's Google account is automatically deprovisioned.

What should the customer do?

A. Use the Cloud SDK with their directory service to remove their IAM permissions in Cloud Identity.
B. Use the Cloud SDK with their directory service to provision and deprovision users from Cloud Identity.
C. Configure Cloud Directory Sync with their directory service to provision and deprovision users from Cloud Identity.
D. Configure Cloud Directory Sync with their directory service to remove their IAM permissions in Cloud Identity.

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Which international compliance standard provides guidelines for information security controls applicable to the provision and use of cloud services?

A. ISO 27001
B. ISO 27002
C. ISO 27017
D. ISO 27018

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Create a new Service Account that should be able to list the Compute Engine instances in the project. You want to follow Google-recommended practices.

QUESTION 41
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 ongoing data backup and disaster recovery solutions to GCP. The organization's on-premises production environment is going to be the next phase for migration to GCP. Stable networking connectivity between the on-premises environment and GCP is also being implemented.

Which GCP solution should the organization use?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://cloud.google.com/solutions/migration-to-google-cloud-building-your-foundation

QUESTION 42
What are the steps to encrypt data using envelope encryption?

A. ▪ Generate a data encryption key (DEK) locally.
▪ Use a key encryption key (KEK) to wrap the DEK.
▪ Encrypt data with the KEK.
▪ Store the encrypted data and the wrapped KEK.

B. ▪ Generate a key encryption key (KEK) locally.
▪ Use the KEK to generate a data encryption key (DEK).
▪ Encrypt data with the DEK.
▪ Store the encrypted data and the wrapped DEK.

C. ▪ Generate a data encryption key (DEK) locally. ▪ Encrypt data with the DEK.
▪ Use a key encryption key (KEK) to wrap the DEK. ▪
Store the encrypted data and the wrapped DEK.

D. ▪ Generate a key encryption key (KEK) locally.
▪ Generate a data encryption key (DEK) locally.
▪ Encrypt data with the KEK

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:
Reference: https://cloud.google.com/kms/docs/envelope-encryption

QUESTION 43
A customer wants to make it convenient for their mobile workforce to access a CRM web interface that is hosted on Google Cloud Platform (GCP). The CRM can only be accessed by someone on the corporate network. The customer wants to make it available over the internet. Your team requires an authentication layer in front of the application that supports two-factor authentication

Which GCP product should the customer implement to meet these requirements?

A. Cloud Identity-Aware Proxy
B. Cloud Armor

C. Cloud Endpoints
D. Cloud VPN

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Your company is storing sensitive data in Cloud Storage. You want a key generated on-premises to be used in the encryption process.

What should you do?

A. Use the Cloud Key Management Service to manage a data encryption key (DEK).
B. Use the Cloud Key Management Service to manage a 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:
Reference: https://cloud.google.com/security/encryption-at-rest/default-encryption/

QUESTION 45
Your team wants to limit users with administrative privileges at the organization level

Which two roles should your team restrict? (Choose two.)

A. Organization Administrator
B. Super Admin
C. GKE Cluster Admin
D. Compute Admin
E. Organization Role Viewer

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Reference: https://cloud.google.com/resource-manager/docs/creating-managing-organization.