Question #1

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.

Answer: A

Question #2

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.

Answer: D

Question #3

You are implementing data protection by design and in accordance with GDPR requirements. As part of design reviews, you are told that you need to manage the encryption key for a solution that includes workloads for Compute Engine, Google Kubernetes Engine, Cloud Storage, BigQuery, and Pub/Sub. Which option should you choose for this implementation?

- A. Cloud External Key Manager
- B. Customer-managed encryption keys
- C. Customer-supplied encryption keys

- D. Google default encryption

Answer: B

Question #4

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

Answer: A

Question #5

A customer wants to deploy a large number of 3-tier web applications on Compute Engine.
How should the customer ensure authenticated network separation between the different tiers of the application?

- A. Run each tier in its own Project, and segregate using Project labels.
- B. Run each tier with a different Service Account (SA), and use SA-based firewall rules.
- C. Run each tier in its own subnet, and use subnet-based firewall rules.
- D. Run each tier with its own VM tags, and use tag-based firewall rules.

Answer: B

Question #6

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.

Answer: D

Question #7

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.

Answer: C

Question #8

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.

Answer: BC

Question #9

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).

Answer: B

Question #10

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.

Answer: B

Question #11

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.

Answer: A

Question #12

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

Answer: CD

Question #13

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

Answer: D

Question #14

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.

Answer: C

Question #15

You want to evaluate your organization's Google Cloud instance 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

Answer: A

Question #16

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

Answer: A

Question #17

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

- A. Turn off the domain restriction sharing organization policy. Set the policy value to "Allow All."
- B. Turn off the domain restricted sharing organization policy. Provide the external partners with the required permissions using Google's Identity and Access Management (IAM) service.
- C. Turn off the domain restricted sharing organization policy. Add each partner's Google Workspace customer ID to a Google group, add the Google group as an exception under the organization policy, and then turn the policy back on.
- D. Turn off the domain restricted sharing organization policy. Set the policy value to "Custom." Add each external partner's Cloud Identity or Google Workspace customer ID as an exception under the organization policy, and then turn the policy back on.

Answer: D

Question #18

Which two security characteristics are related to the use of VPC peering to connect two VPC networks? (Choose two.)

- A. Central management of routes, firewalls, and VPNs for peered networks
- B. Non-transitive peered networks; where only directly peered networks can communicate
- C. Ability to peer networks that belong to different Google Cloud organizations
- D. Firewall rules that can be created with a tag from one peered network to another peered network
- E. Ability to share specific subnets across peered networks

Answer: BC

Question #19

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.

Answer: C

Question #20

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.

Answer: D

Question #21

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 ג€Lift & Shiftג€ 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 ג€Lift & Shiftג€ 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.

Answer: A

Question #22

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

Answer: B

Question #23

You're developing the incident response plan for your company. You need to define the access strategy that your DevOps team will use when reviewing and investigating a deployment issue in your Google Cloud environment. There are two main requirements:
☞ Least-privilege access must be enforced at all times.
☞ The DevOps team must be able to access the required resources only during the deployment issue.
How should you grant access while following Google-recommended best practices?

- A. Assign the Project Viewer Identity and Access Management (IAM) role to the DevOps team.
- B. Create a custom IAM role with limited list/view permissions, and assign it to the DevOps team.
- C. Create a service account, and grant it the Project Owner IAM role. Give the Service Account User Role on this service account to the DevOps team.
- D. Create a service account, and grant it limited list/view permissions. Give the Service Account User Role on this service account to the DevOps team.

Answer: D

Question #24

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.

Answer: A

Question #25

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.)

- 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: BD

Question #26

You are the project owner for a regulated workload that runs in a project you own and manage as an Identity and Access Management (IAM) admin. For an upcoming audit, you need to provide access reviews evidence. Which tool should you use?

- A. Policy Troubleshooter
- B. Policy Analyzer
- C. IAM Recommender
- D. Policy Simulator

Answer: B

Question #27

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

Answer: A

Question #28

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.

Answer: A

Question #29

A company is running their webshop on Google Kubernetes Engine and wants to analyze customer transactions in BigQuery. You need to ensure that no credit card numbers are stored in BigQuery
What should you do?

- A. Create a BigQuery view with regular expressions matching credit card numbers to query and delete affected rows.
- B. Use the Cloud Data Loss Prevention API to redact related infoTypes before data is ingested into BigQuery.
- C. Leverage Security Command Center to scan for the assets of type Credit Card Number in BigQuery.
- D. Enable Cloud Identity-Aware Proxy to filter out credit card numbers before storing the logs in BigQuery.

Answer: B

Question #30

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.

Answer: A

Question #31

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.

Answer: BC

Question #32

A customer is running an analytics workload on Google Cloud Platform (GCP) where Compute Engine instances are accessing data stored on Cloud Storage.
Your team wants to make sure that this workload will not be able to access, or be accessed from, the internet.
Which two strategies should your team use to meet these requirements? (Choose two.)

- A. Configure Private Google Access on the Compute Engine subnet
- B. Avoid assigning public IP addresses to the Compute Engine cluster.
- C. Make sure that the Compute Engine cluster is running on a separate subnet.
- D. Turn off IP forwarding on the Compute Engine instances in the cluster.
- E. Configure a Cloud NAT gateway.

Answer: AB

Question #33

A customer is running an analytics workload on Google Cloud Platform (GCP) where Compute Engine instances are accessing data stored on Cloud Storage.
Your team wants to make sure that this workload will not be able to access, or be accessed from, the internet.
Which two strategies should your team use to meet these requirements? (Choose two.)

- A. Configure Private Google Access on the Compute Engine subnet
- B. Avoid assigning public IP addresses to the Compute Engine cluster.
- C. Make sure that the Compute Engine cluster is running on a separate subnet.
- D. Turn off IP forwarding on the Compute Engine instances in the cluster.
- E. Configure a Cloud NAT gateway.

Answer: AB

Question #34

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).

Answer: C

Question #35

In a shared security responsibility model for IaaS, which two layers of the stack does the customer share responsibility for? (Choose two.)

- A. Hardware
- B. Network Security
- C. Storage Encryption
- D. Access Policies
- E. Boot

Answer: BD

Question #36

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

Answer: A

Question #37

You are backing up application logs to a shared Cloud Storage bucket that is accessible to both the administrator and analysts. Analysts should not have access to logs that contain any personally

identifiable information (PII). Log files containing PII should be stored in another bucket that is only accessible to the administrator. What should you do?

- A. Upload the logs to both the shared bucket and the bucket with PII that is only accessible to the administrator. Use the Cloud Data Loss Prevention API to create a job trigger. Configure the trigger to delete any files that contain PII from the shared bucket.
- B. On the shared bucket, configure Object Lifecycle Management to delete objects that contain PII.
- C. On the shared bucket, configure a Cloud Storage trigger that is only triggered when PII is uploaded. Use Cloud Functions to capture the trigger and delete the files that contain PII.
- D. Use Pub/Sub and Cloud Functions to trigger a Cloud Data Loss Prevention scan every time a file is uploaded to the administrator's bucket. If the scan does not detect PII, have the function move the objects into the shared Cloud Storage bucket.

Answer: D

Question #38

You are responsible for protecting highly sensitive data in BigQuery. Your operations teams need access to this data, but given privacy regulations, you want to ensure that they cannot read the sensitive fields such as email addresses and first names. These specific sensitive fields should only be available on a need-to- know basis to the Human Resources team. What should you do?

- A. Perform data masking with the Cloud Data Loss Prevention API, and store that data in BigQuery for later use.
- B. Perform data redaction with the Cloud Data Loss Prevention API, and store that data in BigQuery for later use.
- C. Perform data inspection with the Cloud Data Loss Prevention API, and store that data in BigQuery for later use.
- D. Perform tokenization for Pseudonymization with the Cloud Data Loss Prevention API, and store that data in BigQuery for later use.

Answer: D

Question #39

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.

Answer: A

Question #40

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.

Answer: B

Question #41

Your company's new CEO recently sold two of the company's divisions. Your Director asks you to help migrate the Google Cloud projects associated with those divisions to a new organization node. Which preparation steps are necessary before this migration occurs? (Choose two.)

- A. Remove all project-level custom Identity and Access Management (IAM) roles.
- B. Disallow inheritance of organization policies.
- C. Identify inherited Identity and Access Management (IAM) roles on projects to be migrated.
- D. Create a new folder for all projects to be migrated.
- E. Remove the specific migration projects from any VPC Service Controls perimeters and bridges.

Answer: DE

Question #42

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

Answer: AC

Question #43

You are a Security Administrator at your organization. You need to restrict service account creation capability within production environments. You want to accomplish this centrally across the organization. What should you do?

- A. Use Identity and Access Management (IAM) to restrict access of all users and service accounts that have access to the production environment.
- B. Use organization policy constraints/iam.disableServiceAccountKeyCreation boolean to disable the creation of new service accounts.
- C. Use organization policy constraints/iam.disableServiceAccountKeyUpload boolean to disable the creation of new service accounts.
- D. Use organization policy constraints/iam.disableServiceAccountCreation boolean to disable the creation of new service accounts.

Answer: D

Question #44

You work for a large organization where each business unit has thousands of users. You need to delegate management of access control permissions to each business unit. You have the following requirements:
☞ Each business unit manages access controls for their own projects.
☞ Each business unit manages access control permissions at scale.
☞ Business units cannot access other business units' projects.
☞ Users lose their access if they move to a different business unit or leave the company.
☞ Users and access control permissions are managed by the on-premises directory service.
What should you do? (Choose two.)

- A. Use VPC Service Controls to create perimeters around each business unit's project.
- B. Organize projects in folders, and assign permissions to Google groups at the folder level.
- C. Group business units based on Organization Units (OUs) and manage permissions based on OUs
- D. Create a project naming convention, and use Google's IAM Conditions to manage access based on the prefix of project names.
- E. Use Google Cloud Directory Sync to synchronize users and group memberships in Cloud Identity.

Answer: BE

Question #45

You need to enforce a security policy in your Google Cloud organization that prevents users from exposing objects in their buckets externally. There are currently no buckets in your organization. Which solution should you implement proactively to achieve this goal with the least operational overhead?

- A. Create an hourly cron job to run a Cloud Function that finds public buckets and makes them private.
- B. Enable the constraints/storage.publicAccessPrevention constraint at the organization level.
- C. Enable the constraints/storage.uniformBucketLevelAccess constraint at the organization level.

- D. Create a VPC Service Controls perimeter that protects the storage.googleapis.com service in your projects that contains buckets. Add any new project that contains a bucket to the perimeter.

Answer: B

Question #46

Your company's cloud security policy dictates that VM instances should not have an external IP address. You need to identify the Google Cloud service that will allow VM instances without external IP addresses to connect to the internet to update the VMs. Which service should you use?

- A. Identity Aware-Proxy
- B. Cloud NAT
- C. TCP/UDP Load Balancing
- D. Cloud DNS

Answer: B

Question #47

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

Answer: C

Question #48

Your company has just launched a new critical revenue-generating web application. You deployed the application for scalability using managed instance groups, autoscaling, and a network load balancer as frontend. One day, you notice severe bursty traffic that the caused autoscaling to reach the maximum number of instances, and users of your application cannot complete transactions. After an investigation, you think it as a DDOS attack. You want to quickly restore user access to your application and allow successful transactions while minimizing cost.
Which two steps should you take? (Choose two.)

- A. Use Cloud Armor to blacklist the attacker's IP addresses.
- B. Increase the maximum autoscaling backend to accommodate the severe bursty traffic.
- C. Create a global HTTP(s) load balancer and move your application backend to this load balancer.

- D. Shut down the entire application in GCP for a few hours. The attack will stop when the application is offline.
- E. SSH into the backend compute engine instances, and view the auth logs and syslogs to further understand the nature of the attack.

Answer: AB

Question #49

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?

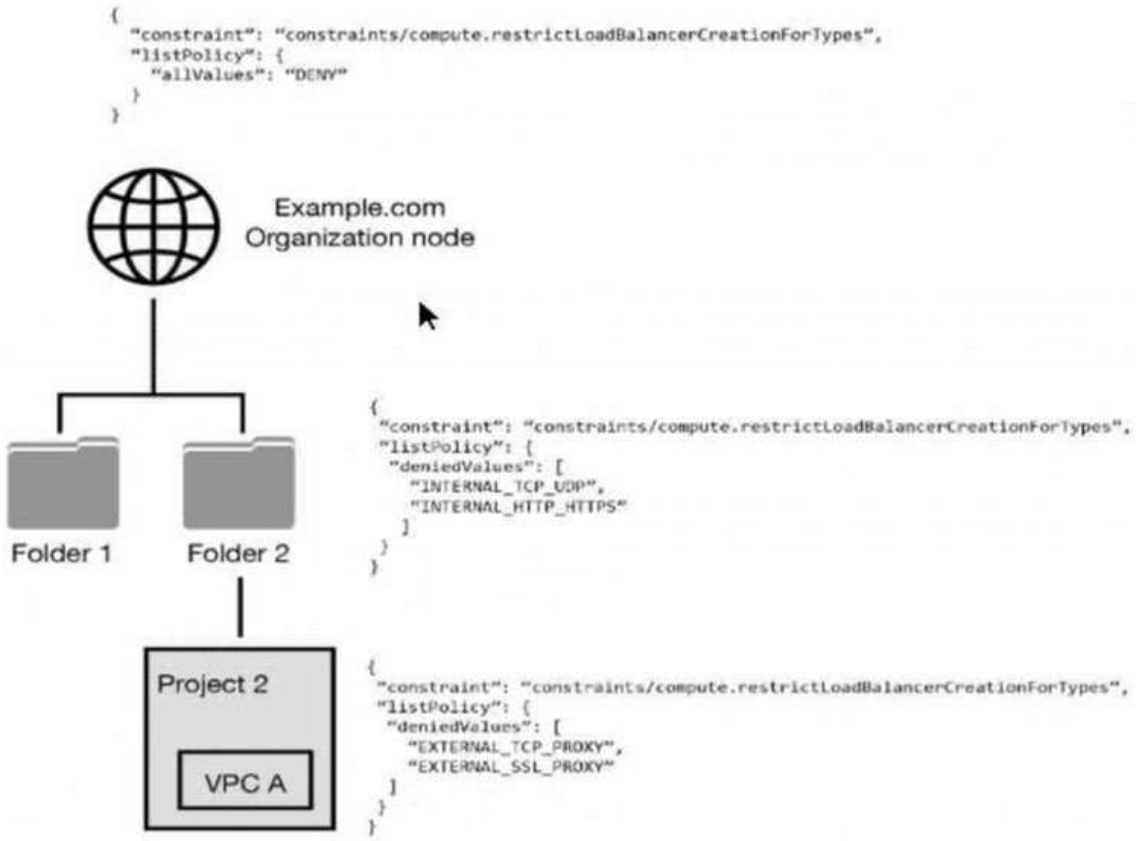
- A. Use Cloud Source Repositories, and store secrets in Cloud SQL.
- B. Encrypt the secrets with a Customer-Managed Encryption Key (CMEK), and store them in Cloud Storage.
- C. Run the Cloud Data Loss Prevention API to scan the secrets, and store them in Cloud SQL.
- D. Deploy the SCM to a Compute Engine VM with local SSDs, and enable preemptible VMs.

Answer: B

Question #50

You have the following resource hierarchy. There is an organization policy at each node in the hierarchy as shown. Which load balancer types are denied in VPC

A?



- A. All load balancer types are denied in accordance with the global node's policy.
- B. INTERNAL_TCP_UDP, INTERNAL_HTTP_HTTPS is denied in accordance with the folder's policy.
- C. EXTERNAL_TCP_PROXY, EXTERNAL_SSL_PROXY are denied in accordance with the project's policy.
- D. EXTERNAL_TCP_PROXY, EXTERNAL_SSL_PROXY, INTERNAL_TCP_UDP, and INTERNAL_HTTP_HTTPS are denied in accordance with the folder and project's policies.

Answer: A

Question #51

You need to audit the network segmentation for your Google Cloud footprint. You currently operate Production and Non-Production infrastructure-as-a-service
(IaaS) environments. All your VM instances are deployed without any service account customization. After observing the traffic in your custom network, you notice that all instances can communicate freely `" despite tag-based VPC firewall rules in place to segment traffic properly `" with a priority of 1000. What are the most likely reasons for this behavior?

- A. All VM instances are missing the respective network tags.
- B. All VM instances are residing in the same network subnet.
- C. All VM instances are configured with the same network route.

- D. A VPC firewall rule is allowing traffic between source/targets based on the same service account with priority 999. E . A VPC firewall rule is allowing traffic between source/targets based on the same service account with priority 1001.

Answer: AD

Question #52

Your company plans to move most of its IT infrastructure to Google Cloud. They want to leverage their existing on-premises Active Directory as an identity provider for Google Cloud. Which two steps should you take to integrate the company's on-premises Active Directory with Google Cloud and configure access management? (Choose two.)

- A. Use Identity Platform to provision users and groups to Google Cloud.
- B. Use Cloud Identity SAML integration to provision users and groups to Google Cloud.
- C. Install Google Cloud Directory Sync and connect it to Active Directory and Cloud Identity.
- D. Create Identity and Access Management (IAM) roles with permissions corresponding to each Active Directory group.
- E. Create Identity and Access Management (IAM) groups with permissions corresponding to each Active Directory group.

Answer: CE

Question #53

You will 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.
What should you do?

- A. Create an Instance Template, and allow the Service Account Read Only access for the Compute Engine Access Scope.
- B. Create a custom role with the permission compute.instances.list and grant the Service Account this role.
- C. Give the Service Account the role of Compute Viewer, and use the new Service Account for all instances.
- D. Give the Service Account the role of Project Viewer, and use the new Service Account for all instances.

Answer: B

Question #54

Your company wants to determine what products they can build to help customers improve their credit scores depending on their age range. To achieve this, you need to join user information in the company's banking app with customers' credit score data received from a third party. While using this raw data will allow you to complete this task, it exposes sensitive data, which could be propagated into new systems.
This risk needs to be addressed using de-identification and tokenization with Cloud Data Loss

Prevention while maintaining the referential integrity across the database. Which cryptographic token format should you use to meet these requirements?

- A. Deterministic encryption
- B. Secure, key-based hashes
- C. Format-preserving encryption
- D. Cryptographic hashing

Answer: A

Question #55

You need to implement an encryption at-rest strategy that reduces key management complexity for non-sensitive data and protects sensitive data while providing the flexibility of controlling the key residency and rotation schedule. FIPS 140-2 L1 compliance is required for all data types. What should you do?

- A. Encrypt non-sensitive data and sensitive data with Cloud External Key Manager.
- B. Encrypt non-sensitive data and sensitive data with Cloud Key Management Service
- C. Encrypt non-sensitive data with Google default encryption, and encrypt sensitive data with Cloud External Key Manager.
- D. Encrypt non-sensitive data with Google default encryption, and encrypt sensitive data with Cloud Key Management Service.

Answer: D

Question #56

You are creating a new infrastructure CI/CD pipeline to deploy hundreds of ephemeral projects in your Google Cloud organization to enable your users to interact with Google Cloud. You want to restrict the use of the default networks in your organization while following Google-recommended best practices. What should you do?

- A. Enable the constraints/compute.skipDefaultNetworkCreation organization policy constraint at the organization level.
- B. Create a cron job to trigger a daily Cloud Function to automatically delete all default networks for each project.
- C. Grant your users the IAM Owner role at the organization level. Create a VPC Service Controls perimeter around the project that restricts the compute.googleapis.com API.
- D. Only allow your users to use your CI/CD pipeline with a predefined set of infrastructure templates they can deploy to skip the creation of the default networks.

Answer: A

Question #57

Your organization's Google Cloud VMs are deployed via an instance template that configures them with a public IP address in order to host web services for external users. The VMs reside in a service project that is attached to a host (VPC) project containing one custom Shared VPC for the VMs. You

have been asked to reduce the exposure of the VMs to the internet while continuing to service external users. You have already recreated the instance template without a public IP address configuration to launch the managed instance group (MIG). What should you do?

- A. Deploy a Cloud NAT Gateway in the service project for the MIG.
- B. Deploy a Cloud NAT Gateway in the host (VPC) project for the MIG.
- C. Deploy an external HTTP(S) load balancer in the service project with the MIG as a backend.
- D. Deploy an external HTTP(S) load balancer in the host (VPC) project with the MIG as a backend.

Answer: C

Question #58

You have noticed an increased number of phishing attacks across your enterprise user accounts. You want to implement the Google 2-Step Verification (2SV) option that uses a cryptographic signature to authenticate a user and verify the URL of the login page. Which Google 2SV option should you use?

- A. Titan Security Keys
- B. Google prompt
- C. Google Authenticator app
- D. Cloud HSM keys

Answer: A

Question #59

Your company's chief information security officer (CISO) is requiring business data to be stored in specific locations due to regulatory requirements that affect the company's global expansion plans. After working on a plan to implement this requirement, you determine the following:

☞ The services in scope are included in the Google Cloud data residency requirements.

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

☞ The folder structure can contain multiple data residency locations.

☞ The projects are aligned to specific locations.

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

- A. Organization
- B. Resource
- C. Project
- D. Folder

Answer: C

Question #60

You need to implement an encryption-at-rest strategy that protects sensitive data and reduces key management complexity for non-sensitive data. Your solution has the following requirements:
☞ Schedule key rotation for sensitive data.
☞ Control which region the encryption keys for sensitive data are stored in.
☞ Minimize the latency to access encryption keys for both sensitive and non-sensitive data.
What should you do?

- A. Encrypt non-sensitive data and sensitive data with Cloud External Key Manager.
- B. Encrypt non-sensitive data and sensitive data with Cloud Key Management Service.
- C. Encrypt non-sensitive data with Google default encryption, and encrypt sensitive data with Cloud External Key Manager.
- D. Encrypt non-sensitive data with Google default encryption, and encrypt sensitive data with Cloud Key Management Service.

Answer: D

Question #61

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

- A. Enable Private Google Access on the regional subnets and global dynamic routing mode.
- B. Set up a Private Service Connect endpoint IP address with the API bundle of "all-apis", which is advertised as a route over the Cloud interconnect connection.
- C. Use private.googleapis.com to access Google APIs using a set of IP addresses only routable from within Google Cloud, which are advertised as routes over the connection.
- D. Use restricted googleapis.com to access Google APIs using a set of IP addresses only routable from within Google Cloud, which are advertised as routes over the Cloud Interconnect connection.

Answer: D

Question #62

You need to use Cloud External Key Manager to create an encryption key to encrypt specific BigQuery data at rest in Google Cloud. Which steps should you do first?

- A. 1. Create or use an existing key with a unique uniform resource identifier (URI) in your Google Cloud project. 2. Grant your Google Cloud project access to a supported external key management partner system.
- B. 1. Create or use an existing key with a unique uniform resource identifier (URI) in Cloud Key Management Service (Cloud KMS). 2. In Cloud KMS, grant your Google Cloud project access to use the key.
- C. 1. Create or use an existing key with a unique uniform resource identifier (URI) in a supported external key management partner system. 2. In the external key management partner system, grant access for this key to use your Google Cloud project.

- D. 1. Create an external key with a unique uniform resource identifier (URI) in Cloud Key Management Service (Cloud KMS). 2. In Cloud KMS, grant your Google Cloud project access to use the key.

Answer: C

Question #63

You are part of a security team that wants to ensure that a Cloud Storage bucket in Project A can only be readable from Project B. You also want to ensure that data in the Cloud Storage bucket cannot be accessed from or copied to Cloud Storage buckets outside the network, even if the user has the correct credentials.
What should you do?

- A. Enable VPC Service Controls, create a perimeter with Project A and B, and include Cloud Storage service.
- B. Enable Domain Restricted Sharing Organization Policy and Bucket Policy Only on the Cloud Storage bucket.
- C. Enable Private Access in Project A and B networks with strict firewall rules to allow communication between the networks.
- D. Enable VPC Peering between Project A and B networks with strict firewall rules to allow communication between the networks.

Answer: A

Question #64

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.

Answer: A

Question #65

An engineering team is launching a web application that will be public on the internet. The web application is hosted in multiple GCP regions and will be directed to the respective backend based on the URL request.
Your team wants to avoid exposing the application directly on the internet and wants to deny traffic

from a specific list of malicious IP addresses.
Which solution should your team implement to meet these requirements?

- A. Cloud Armor
- B. Network Load Balancing
- C. SSL Proxy Load Balancing
- D. NAT Gateway

Answer: A

Question #66

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

Answer: B

Question #67

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.

Answer: B

Question #68

A manager wants to start retaining security event logs for 2 years while minimizing costs. You write a filter to select the appropriate log entries.
Where should you export the logs?

- A. BigQuery datasets
- B. Cloud Storage buckets
- C. StackDriver logging
- D. Cloud Pub/Sub topics

Answer: B

Question #69

Your security team uses encryption keys to ensure confidentiality of user data. You want to establish a process to reduce the impact of a potentially compromised symmetric encryption key in Cloud Key Management Service (Cloud KMS).
Which steps should your team take before an incident occurs? (Choose two.)

- A. Disable and revoke access to compromised keys.
- B. Enable automatic key version rotation on a regular schedule.
- C. Manually rotate key versions on an ad hoc schedule.
- D. Limit the number of messages encrypted with each key version.
- E. Disable the Cloud KMS API.

Answer: BD

Question #70

An organization is evaluating the use of Google Cloud Platform (GCP) for certain IT workloads. A well-established directory service is used to manage user identities and lifecycle management. This directory service must continue for the organization to use as the `source of truth` directory for identities.
Which solution meets the organization's requirements?

- A. Google Cloud Directory Sync (GCDS)
- B. Cloud Identity
- C. Security Assertion Markup Language (SAML)
- D. Pub/Sub

Answer: A

Question #71

You are in charge of creating a new Google Cloud organization for your company. Which two actions should you take when creating the super administrator accounts? (Choose two.)

- A. Create an access level in the Google Admin console to prevent super admin from logging in to Google Cloud.

- B. Disable any Identity and Access Management (IAM) roles for super admin at the organization level in the Google Cloud Console.
- C. Use a physical token to secure the super admin credentials with multi-factor authentication (MFA).
- D. Use a private connection to create the super admin accounts to avoid sending your credentials over the Internet.
- E. Provide non-privileged identities to the super admin users for their day-to-day activities.

Answer: CE

Question #72

You want to make sure that your organization's Cloud Storage buckets cannot have data publicly available to the internet. You want to enforce this across all
Cloud Storage buckets. What should you do?

- A. Remove Owner roles from end users, and configure Cloud Data Loss Prevention.
- B. Remove Owner roles from end users, and enforce domain restricted sharing in an organization policy.
- C. Configure uniform bucket-level access, and enforce domain restricted sharing in an organization policy.
- D. Remove *.setIamPolicy permissions from all roles, and enforce domain restricted sharing in an organization policy.

Answer: C

Question #73

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 ג€in-scope-pciג€.

Answer: A

Question #74

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.

Answer: A

Question #75

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. Web Security Scanner

Answer: B

Question #76

A customer wants to run a batch processing system on VMs and store the output files in a Cloud Storage bucket. The networking and security teams have decided that no VMs may reach the public internet.
How should this be accomplished?

- A. Create a firewall rule to block internet traffic from the VM.
- B. Provision a NAT Gateway to access the Cloud Storage API endpoint.
- C. Enable Private Google Access.
- D. Mount a Cloud Storage bucket as a local filesystem on every VM.

Answer: C

Question #77

Your company operates an application instance group that is currently deployed behind a Google Cloud load balancer in us-central-1 and is configured to use the
Standard Tier network. The infrastructure team wants to expand to a second Google Cloud region, us-east-2. You need to set up a single external IP address to distribute new requests to the instance groups in both regions.
What should you do?

- A. Change the load balancer backend configuration to use network endpoint groups instead of instance groups.
- B. Change the load balancer frontend configuration to use the Premium Tier network, and add the new instance group.
- C. Create a new load balancer in us-east-2 using the Standard Tier network, and assign a static external IP address.
- D. Create a Cloud VPN connection between the two regions, and enable Google Private Access.

Answer: B

Question #78

You are part of a security team investigating a compromised service account key. You need to audit which new resources were created by the service account.
What should you do?

- A. Query Data Access logs.
- B. Query Admin Activity logs.
- C. Query Access Transparency logs.
- D. Query Stackdriver Monitoring Workspace.

Answer: B

Question #79

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.

Answer: A

Question #80

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.

Answer: C

Question #81

When working with agents in the support center via online chat, your organization's customers often share pictures of their documents with personally identifiable information (PII). Your leadership team is concerned that this PII is being stored as part of the regular chat logs, which are reviewed by internal or external analysts for customer service trends.
You want to resolve this concern while still maintaining data utility. What should you do?

- A. Use Cloud Key Management Service to encrypt PII shared by customers before storing it for analysis.
- B. Use Object Lifecycle Management to make sure that all chat records containing PII 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.

Answer: C

Question #82

You are the Security Admin in your company. You want to synchronize all security groups that have an email address from your LDAP directory in Cloud IAM.
What should you do?

- A. Configure Google Cloud Directory Sync to sync security groups using LDAP search rules that have ƛ€user email addressƛ€ as the attribute to facilitate one-way sync.
- B. Configure Google Cloud Directory Sync to sync security groups using LDAP search rules that have ƛ€user email addressƛ€ as the attribute to facilitate bidirectional sync.
- C. Use a management tool to sync the subset based on the email address attribute. Create a group in the Google domain. A group created in a Google domain will automatically have an explicit Google Cloud Identity and Access Management (IAM) role.
- D. Use a management tool to sync the subset based on group object class attribute. Create a group in the Google domain. A group created in a Google domain will automatically have an explicit Google Cloud Identity and Access Management (IAM) role.

Answer: A

Question #83

Last week, a company deployed a new App Engine application that writes logs to BigQuery. No other workloads are running in the project. You need to validate that all data written to BigQuery was done using the App Engine Default Service Account.
What should you do?

- A. 1. Use Cloud Logging and filter on BigQuery Insert Jobs. 2. Click on the email address in line with the App Engine Default Service Account in the authentication field. 3. Click Hide Matching Entries. 4. Make sure the resulting list is empty.
- B. 1. Use Cloud Logging and filter on BigQuery Insert Jobs. 2. Click on the email address in line with the App Engine Default Service Account in the authentication field. 3. Click Show Matching Entries. 4. Make sure the resulting list is empty.
- C. 1. In BigQuery, select the related dataset. 2. Make sure that the App Engine Default Service Account is the only account that can write to the dataset.
- D. 1. Go to the Identity and Access Management (IAM) section of the project. 2. Validate that the App Engine Default Service Account is the only account that has a role that can write to BigQuery.

Answer: A

Question #84

You are consulting with a client that requires end-to-end encryption of application data (including data in transit, data in use, and data at rest) within Google Cloud.
Which options should you utilize to accomplish this? (Choose two.)

- A. External Key Manager
- B. Customer-supplied encryption keys
- C. Hardware Security Module
- D. Confidential Computing and Istio
- E. Client-side encryption

Answer: DE

Question #85

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

Answer: AB

Question #86

An organization's security and risk management teams are concerned about where their responsibility lies for certain production workloads they are running in

Google Cloud and where Google's responsibility lies. They are mostly running workloads using Google Cloud's platform-as-a-Service (PaaS) offerings, including
App Engine primarily.
Which area in the technology stack should they focus on as their primary responsibility when using App Engine?

- A. Configuring and monitoring VPC Flow Logs
- B. Defending against XSS and SQLi attacks
- C. Managing the latest updates and security patches for the Guest OS
- D. Encrypting all stored data

Answer: B

Question #87

You have been tasked with configuring Security Command Center for your organization's Google Cloud environment. Your security team needs to receive alerts of potential crypto mining in the organization's compute environment and alerts for common Google Cloud misconfigurations that impact security. Which Security
Command Center features should you use to configure these alerts? (Choose two.)

- A. Event Threat Detection
- B. Container Threat Detection
- C. Security Health Analytics
- D. Cloud Data Loss Prevention
- E. Google Cloud Armor

Answer: AC

Question #88

Your company requires the security and network engineering teams to identify all network anomalies within and across VPCs, internal traffic from VMs to VMs, traffic between end locations on the internet and VMs, and traffic between VMs to Google Cloud services in production. Which method should you use?

- A. Define an organization policy constraint.
- B. Configure packet mirroring policies.
- C. Enable VPC Flow Logs on the subnet.
- D. Monitor and analyze Cloud Audit Logs.

Answer: B

Question #89

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

Answer: A

Question #90

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.

Answer: C

Question #91

You manage your organization's Security Operations Center (SOC). You currently monitor and detect network traffic anomalies in your VPCs based on network logs. However, you want to explore your environment using network payloads and headers. Which Google Cloud product should you use?

- A. Cloud IDS
- B. VPC Service Controls logs
- C. VPC Flow Logs
- D. Google Cloud Armor
- E. Packet Mirroring

Answer: E

Question #92

You want to limit the images that can be used as the source for boot disks. These images will be stored in a dedicated project.
What should you do?

- A. Use the Organization Policy Service to create a compute.trustedimageProjects constraint on the organization level. List the trusted project as the whitelist in an allow operation.

- B. Use the Organization Policy Service to create a compute.trustedimageProjects constraint on the organization level. List the trusted projects as the exceptions in a deny operation.
- C. In Resource Manager, edit the project permissions for the trusted project. Add the organization as member with the role: Compute Image User.
- D. In Resource Manager, edit the organization permissions. Add the project ID as member with the role: Compute Image User.

Answer: A

Question #93

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.

Answer: A

Question #94

You are deploying a web application hosted on Compute Engine. A business requirement mandates that application logs are preserved for 12 years and data is kept within European boundaries. You want to implement a storage solution that minimizes overhead and is cost-effective. What should you do?

- A. Create a Cloud Storage bucket to store your logs in the EUROPE-WEST1 region. Modify your application code to ship logs directly to your bucket for increased efficiency.
- B. Configure your Compute Engine instances to use the Google Cloud's operations suite Cloud Logging agent to send application logs to a custom log bucket in the EUROPE-WEST1 region with a custom retention of 12 years.
- C. Use a Pub/Sub topic to forward your application logs to a Cloud Storage bucket in the EUROPE-WEST1 region.
- D. Configure a custom retention policy of 12 years on your Google Cloud's operations suite log bucket in the EUROPE-WEST1 region.

Answer: B

Question #95

Your organization acquired a new workload. The Web and Application (App) servers will be running on Compute Engine in a newly created custom VPC. You are responsible for configuring a secure network communication solution that meets the following requirements:

☞ Only allows communication between the Web and App tiers.
☞ Enforces consistent network security when autoscaling the Web and App tiers.
☞ Prevents Compute Engine Instance Admins from altering network traffic.
What should you do?

- A. 1. Configure all running Web and App servers with respective network tags. 2. Create an allow VPC firewall rule that specifies the target/source with respective network tags.
- B. 1. Configure all running Web and App servers with respective service accounts. 2. Create an allow VPC firewall rule that specifies the target/source with respective service accounts.
- C. 1. Re-deploy the Web and App servers with instance templates configured with respective network tags. 2. Create an allow VPC firewall rule that specifies the target/source with respective network tags.
- D. 1. Re-deploy the Web and App servers with instance templates configured with respective service accounts. 2. Create an allow VPC firewall rule that specifies the target/source with respective service accounts.

Answer: D

Question #96

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

Answer: A

Question #97

Your company's Chief Information Security Officer (CISO) creates a requirement that business data must be stored in specific locations due to regulatory requirements that affect the company's global expansion plans. After working on the details to implement this requirement, you determine the following:
☞ The services in scope are included in the Google Cloud Data Residency Terms.
☞ The business data remains within specific locations under the same organization.
☞ The folder structure can contain multiple data residency locations.
You plan to use the Resource Location Restriction organization policy constraint. At which level in the resource hierarchy should you set the constraint?

- A. Folder
- B. Resource
- C. Project
- D. Organization

Answer: A

Question #98

You are working with a client who plans to migrate their data to Google Cloud. You are responsible for recommending an encryption service to manage their encrypted keys. You have the following requirements:
☞ The master key must be rotated at least once every 45 days.
☞ The solution that stores the master key must be FIPS 140-2 Level 3 validated.
☞ The master key must be stored in multiple regions within the US for redundancy.
Which solution meets these requirements?

- A. Customer-managed encryption keys with Cloud Key Management Service
- B. Customer-managed encryption keys with Cloud HSM
- C. Customer-supplied encryption keys
- D. Google-managed encryption keys

Answer: B

Question #99

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.

Answer: B

Question #100

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?

- 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

Question #101

Your organization hosts a financial services application running on Compute Engine instances for a third-party company. The third-party company's servers that will consume the application also run on Compute Engine in a separate Google Cloud organization. You need to configure a secure network connection between the Compute Engine instances. You have the following requirements:
☞ The network connection must be encrypted.
☞ The communication between servers must be over private IP addresses.
What should you do?

- A. Configure a Cloud VPN connection between your organization's VPC network and the third party's that is controlled by VPC firewall rules.
- B. Configure a VPC peering connection between your organization's VPC network and the third party's that is controlled by VPC firewall rules.
- C. Configure a VPC Service Controls perimeter around your Compute Engine instances, and provide access to the third party via an access level.
- D. Configure an Apigee proxy that exposes your Compute Engine-hosted application as an API, and is encrypted with TLS which allows access only to the third party.

Answer: B

Question #102

You work for an organization in a regulated industry that has strict data protection requirements. The organization backs up their data in the cloud. To comply with data privacy regulations, this data can only be stored for a specific length of time and must be deleted after this specific period.
You want to automate the compliance with this regulation while minimizing storage costs. What should you do?

- A. Store the data in a persistent disk, and delete the disk at expiration time.
- B. Store the data in a Cloud Bigtable table, and set an expiration time on the column families.
- C. Store the data in a BigQuery table, and set the table's expiration time.
- D. Store the data in a Cloud Storage bucket, and configure the bucket's Object Lifecycle Management feature.

Answer: D

Question #103

Your team needs to make sure that their backend database can only be accessed by the frontend application and no other instances on the network.
How should your team design this network?

- A. Create an ingress firewall rule to allow access only from the application to the database using firewall tags.
- B. Create a different subnet for the frontend application and database to ensure network isolation.
- C. Create two VPC networks, and connect the two networks using Cloud VPN gateways to ensure network isolation.
- D. Create two VPC networks, and connect the two networks using VPC peering to ensure network isolation.

Answer: A

Question #104

An office manager at your small startup company is responsible for matching payments to invoices and creating billing alerts. For compliance reasons, the office manager is only permitted to have the Identity and Access Management (IAM) permissions necessary for these tasks. Which two IAM roles should the office manager have? (Choose two.)

- A. Organization Administrator
- B. Project Creator
- C. Billing Account Viewer
- D. Billing Account Costs Manager
- E. Billing Account User

Answer: CD

Question #105

You need to provide a corporate user account in Google Cloud for each of your developers and operational staff who need direct access to GCP resources.
Corporate policy requires you to maintain the user identity in a third-party identity management provider and leverage single sign-on. You learn that a significant number of users are using their corporate domain email addresses for personal Google accounts, and you need to follow Google recommended practices to convert existing unmanaged users to managed accounts.
Which two actions should you take? (Choose two.)

- A. Use Google Cloud Directory Sync to synchronize your local identity management system to Cloud Identity.
- B. Use the Google Admin console to view which managed users are using a personal account for their recovery email.
- C. Add users to your managed Google account and force users to change the email addresses associated with their personal accounts.
- D. Use the Transfer Tool for Unmanaged Users (TTUU) to find users with conflicting accounts and ask them to transfer their personal Google accounts.
- E. Send an email to all of your employees and ask those users with corporate email addresses for personal Google accounts to delete the personal accounts immediately.

Answer: AD

Question #106

The security operations team needs access to the security-related logs for all projects in their organization. They have the following requirements:
☞ Follow the least privilege model by having only view access to logs.
☞ Have access to Admin Activity logs.
☞ Have access to Data Access logs.
☞ Have access to Access Transparency logs.
Which Identity and Access Management (IAM) role should the security operations team be granted?

- A. roles/logging.privateLogViewer
- B. roles/logging.admin
- C. roles/viewer
- D. roles/logging.viewer

Answer: A

Question #107

You are troubleshooting access denied errors between Compute Engine instances connected to a Shared VPC and BigQuery datasets. The datasets reside in a project protected by a VPC Service Controls perimeter. What should you do?

- A. Add the host project containing the Shared VPC to the service perimeter.
- B. Add the service project where the Compute Engine instances reside to the service perimeter.
- C. Create a service perimeter between the service project where the Compute Engine instances reside and the host project that contains the Shared VPC.
- D. Create a perimeter bridge between the service project where the Compute Engine instances reside and the perimeter that contains the protected BigQuery datasets.

Answer: A

Question #108

You have created an OS image that is hardened per your organization's security standards and is being stored in a project managed by the security team. As a
Google Cloud administrator, you need to make sure all VMs in your Google Cloud organization can only use that specific OS image while minimizing operational overhead. What should you do? (Choose two.)

- A. Grant users the compute.imageUser role in their own projects.
- B. Grant users the compute.imageUser role in the OS image project.
- C. Store the image in every project that is spun up in your organization.
- D. Set up an image access organization policy constraint, and list the security team managed project in the project's allow list.
- E. Remove VM instance creation permission from users of the projects, and only allow you and your team to create VM instances.

Answer: BD

Question #109

You are a security administrator at your company and are responsible for managing access controls (identification, authentication, and authorization) on Google
Cloud. Which Google-recommended best practices should you follow when configuring authentication and authorization? (Choose two.)

- A. Use Google default encryption.
- B. Manually add users to Google Cloud.
- C. Provision users with basic roles using Google's Identity and Access Management (IAM) service.
- D. Use SSO/SAML integration with Cloud Identity for user authentication and user lifecycle management.
- E. Provide granular access with predefined roles.

Answer: DE

Question #110

You have an application where the frontend is deployed on a managed instance group in subnet A and the data layer is stored on a mysql Compute Engine virtual machine (VM) in subnet B on the same VPC. Subnet A and Subnet B hold several other Compute Engine VMs. You only want to allow the application frontend to access the data in the application's mysql instance on port 3306.
What should you do?

- A. Configure an ingress firewall rule that allows communication from the src IP range of subnet A to the tag "data-tag" that is applied to the mysql Compute Engine VM on port 3306.
- B. Configure an ingress firewall rule that allows communication from the frontend's unique service account to the unique service account of the mysql Compute Engine VM on port 3306.
- C. Configure a network tag "fe-tag" to be applied to all instances in subnet A and a network tag "data-tag" to be applied to all instances in subnet B. Then configure an egress firewall rule that allows communication from Compute Engine VMs tagged with data-tag to destination Compute Engine VMs tagged fe- tag.
- D. Configure a network tag "fe-tag" to be applied to all instances in subnet A and a network tag "data-tag" to be applied to all instances in subnet B. Then configure an ingress firewall rule that allows communication from Compute Engine VMs tagged with fe-tag to destination Compute Engine VMs tagged with data-tag.

Answer: B

Question #111

Which Identity-Aware Proxy role should you grant to an Identity and Access Management (IAM) user to access HTTPS resources?

- A. Security Reviewer
- B. IAP-Secured Tunnel User
- C. IAP-Secured Web App User
- D. Service Broker Operator

Answer: C

Question #112

Your company requires the security and network engineering teams to identify all network anomalies and be able to capture payloads within VPCs. Which method should you use?

- A. Define an organization policy constraint.
- B. Configure packet mirroring policies.
- C. Enable VPC Flow Logs on the subnet.
- D. Monitor and analyze Cloud Audit Logs.

Answer: B

Question #113

Your company has been creating users manually in Cloud Identity to provide access to Google Cloud resources. Due to continued growth of the environment, you want to authorize the Google Cloud Directory Sync (GCDS) instance and integrate it with your on-premises LDAP server to onboard hundreds of users. You are required to:
☞ Replicate user and group lifecycle changes from the on-premises LDAP server in Cloud Identity.
☞ Disable any manually created users in Cloud Identity.
You have already configured the LDAP search attributes to include the users and security groups in scope for Google Cloud. What should you do next to complete this solution?

- A. 1. Configure the option to suspend domain users not found in LDAP. 2. Set up a recurring GCDS task.
- B. 1. Configure the option to delete domain users not found in LDAP. 2. Run GCDS after user and group lifecycle changes.
- C. 1. Configure the LDAP search attributes to exclude manually created Cloud Identity users not found in LDAP. 2. Set up a recurring GCDS task.
- D. 1. Configure the LDAP search attributes to exclude manually created Cloud Identity users not found in LDAP. 2. Run GCDS after user and group lifecycle changes.

Answer: A

Question #114

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.

Answer: C

Question #115

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

Answer: B

Question #116

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.

Answer: C

Question #117

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

Answer: C

Question #118

You are onboarding new users into Cloud Identity and discover that some users have created consumer user accounts using the corporate domain name. How should you manage these consumer user accounts with Cloud Identity?

- A. Use Google Cloud Directory Sync to convert the unmanaged user accounts.
- B. Create a new managed user account for each consumer user account.
- C. Use the transfer tool for unmanaged user accounts.
- D. Configure single sign-on using a customer's third-party provider.

Answer: C

Question #119

You need to create a VPC that enables your security team to control network resources such as firewall rules. How should you configure the network to allow for separation of duties for network resources?

- A. Set up multiple VPC networks, and set up multi-NIC virtual appliances to connect the networks.
- B. Set up VPC Network Peering, and allow developers to peer their network with a Shared VPC.
- C. Set up a VPC in a project. Assign the Compute Network Admin role to the security team, and assign the Compute Admin role to the developers.
- D. Set up a Shared VPC where the security team manages the firewall rules, and share the network with developers via service projects.

Answer: D

Question #120

You have been tasked with inspecting IP packet data for invalid or malicious content. What should you do?

- A. Use Packet Mirroring to mirror traffic to and from particular VM instances. Perform inspection using security software that analyzes the mirrored traffic.
- B. Enable VPC Flow Logs for all subnets in the VPC. Perform inspection on the Flow Logs data using Cloud Logging.
- C. Configure the Fluentd agent on each VM Instance within the VPC. Perform inspection on the log data using Cloud Logging.
- D. Configure Google Cloud Armor access logs to perform inspection on the log data.

Answer: A

Question #121

You are working with a client that is concerned about control of their encryption keys for sensitive data. The client does not want to store encryption keys at rest in the same cloud service provider

(CSP) as the data that the keys are encrypting. Which Google Cloud encryption solutions should you recommend to this client?
(Choose two.)

- A. Customer-supplied encryption keys.
- B. Google default encryption
- C. Secret Manager
- D. Cloud External Key Manager
- E. Customer-managed encryption keys

Answer: AD

Question #122

You discovered that sensitive personally identifiable information (PII) is being ingested to your Google Cloud environment in the daily ETL process from an on- premises environment to your BigQuery datasets. You need to redact this data to obfuscate the PII, but need to re-identify it for data analytics purposes. Which components should you use in your solution? (Choose two.)

- A. Secret Manager
- B. Cloud Key Management Service
- C. Cloud Data Loss Prevention with cryptographic hashing
- D. Cloud Data Loss Prevention with automatic text redaction
- E. Cloud Data Loss Prevention with deterministic encryption using AES-SIV

Answer: BE

Question #123

You need to centralize your team's logs for production projects. You want your team to be able to search and analyze the logs using Logs Explorer. What should you do?

- A. Enable Cloud Monitoring workspace, and add the production projects to be monitored.
- B. Use Logs Explorer at the organization level and filter for production project logs.
- C. Create an aggregate org sink at the parent folder of the production projects, and set the destination to a Cloud Storage bucket.
- D. Create an aggregate org sink at the parent folder of the production projects, and set the destination to a logs bucket.

Answer: D

Question #124

You want to update your existing VPC Service Controls perimeter with a new access level. You need to avoid breaking the existing perimeter with this change, and ensure the least disruptions to users while minimizing overhead. What should you do?

- A. Create an exact replica of your existing perimeter. Add your new access level to the replica. Update the original perimeter after the access level has been vetted.

- B. Update your perimeter with a new access level that never matches. Update the new access level to match your desired state one condition at a time to avoid being overly permissive.
- C. Enable the dry run mode on your perimeter. Add your new access level to the perimeter configuration. Update the perimeter configuration after the access level has been vetted.
- D. Enable the dry run mode on your perimeter. Add your new access level to the perimeter dry run configuration. Update the perimeter configuration after the access level has been vetted.

Answer: D

Question #125

Which Google Cloud service should you use to enforce access control policies for applications and resources?

- A. Identity-Aware Proxy
- B. Cloud NAT
- C. Google Cloud Armor
- D. Shielded VMs

Answer: A

Question #126

You are responsible for managing your company's identities in Google Cloud. Your company enforces 2-Step Verification (2SV) for all users. You need to reset a user's access, but the user lost their second factor for 2SV. You want to minimize risk. What should you do?

- A. On the Google Admin console, select the appropriate user account, and generate a backup code to allow the user to sign in. Ask the user to update their second factor.
- B. On the Google Admin console, temporarily disable the 2SV requirements for all users. Ask the user to log in and add their new second factor to their account. Re-enable the 2SV requirement for all users.
- C. On the Google Admin console, select the appropriate user account, and temporarily disable 2SV for this account. Ask the user to update their second factor, and then re-enable 2SV for this account.
- D. On the Google Admin console, use a super administrator account to reset the user account's credentials. Ask the user to update their credentials after their first login.

Answer: A

Question #127

Your security team wants to reduce the risk of user-managed keys being mismanaged and compromised. To achieve this, you need to prevent developers from creating user-managed service account keys for projects in their organization. How should you enforce this?

- A. Configure Secret Manager to manage service account keys.

- B. Enable an organization policy to disable service accounts from being created.
- C. Enable an organization policy to prevent service account keys from being created.
- D. Remove the iam.serviceAccounts.getAccessToken permission from users.

Answer: C

Question #128

You are a consultant for an organization that is considering migrating their data from its private cloud to Google Cloud. The organization's compliance team is not familiar with Google Cloud and needs guidance on how compliance requirements will be met on Google Cloud. One specific compliance requirement is for customer data at rest to reside within specific geographic boundaries. Which option should you recommend for the organization to meet their data residency requirements on Google Cloud?

- A. Organization Policy Service constraints
- B. Shielded VM instances
- C. Access control lists
- D. Geolocation access controls
- E. Google Cloud Armor

Answer: A

Question #129

A database administrator notices malicious activities within their Cloud SQL instance. The database administrator wants to monitor the API calls that read the configuration or metadata of resources. Which logs should the database administrator review?

- A. Admin Activity
- B. System Event
- C. Access Transparency
- D. Data Access

Answer: D

Question #130

You perform a security assessment on a customer architecture and discover that multiple VMs have public IP addresses. After providing a recommendation to remove the public IP addresses, you are told those VMs need to communicate to external sites as part of the customer's typical operations. What should you recommend to reduce the need for public IP addresses in your customer's VMs?

- A. Google Cloud Armor
- B. Cloud NAT
- C. Cloud Router
- D. Cloud VPN

Answer: B

Question #131

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

- A. The load balancer must be an external SSL proxy load balancer.
- B. Google Cloud Armor Policy rules can only match on Layer 7 (L7) attributes.
- C. The load balancer must use the Premium Network Service Tier.
- D. The backend service's load balancing scheme must be EXTERNAL.
- E. The load balancer must be an external HTTP(S) load balancer.

Answer: DE

Question #132

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

- A. Enable Firewall Rules Logging on the latest rules that were changed. Use Logs Explorer to analyze whether the rules are working correctly.
- B. Connect to a bastion host in your VPC. Use a network traffic analyzer to determine at which point your requests are being blocked.
- C. In a pre-production environment, disable all firewall rules individually to determine which one is blocking user traffic.
- D. Enable VPC Flow Logs in your VPC. Use Logs Explorer to analyze whether the rules are working correctly.

Answer: A

Question #133

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

- A. compute.restrictSharedVpcHostProjects
- B. compute.restrictXpnProjectLienRemoval
- C. compute.restrictSharedVpcSubnetworks
- D. compute.sharedReservationsOwnerProjects

Answer: B

Question #134

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

- A. SSL Proxy
- B. TCP Proxy
- C. Internal TCP/UDP
- D. TCP/UDP Network

Answer: D

Question #135

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

Must be cloud-native -

▪

☞ Must be cost-efficient

☞ Minimize operational overhead

How should you accomplish this? (Choose two.)

- A. Create a Cloud Build pipeline that will monitor changes to your container templates in a Cloud Source Repositories repository. Add a step to analyze Container Analysis results before allowing the build to continue.
- B. Use a Cloud Function triggered by log events in Google Cloud's operations suite to automatically scan your container images in Container Registry.
- C. Use a cron job on a Compute Engine instance to scan your existing repositories for known vulnerabilities and raise an alert if a non-compliant container image is found.
- D. Deploy Jenkins on GKE and configure a CI/CD pipeline to deploy your containers to Container Registry. Add a step to validate your container images before deploying your container to the cluster.
- E. In your CI/CD pipeline, add an attestation on your container image when no vulnerabilities have been found. Use a Binary Authorization policy to block deployments of containers with no attestation in your cluster.

Answer: AE

Question #136

You are working with protected health information (PHI) for an electronic health record system. The privacy officer is concerned that sensitive data is stored in the analytics system. You are tasked with anonymizing the sensitive data in a way that is not reversible. Also, the anonymized data should not preserve the character set and length. Which Google Cloud solution should you use?

- A. Cloud Data Loss Prevention with deterministic encryption using AES-SIV
- B. Cloud Data Loss Prevention with format-preserving encryption
- C. Cloud Data Loss Prevention with cryptographic hashing
- D. Cloud Data Loss Prevention with Cloud Key Management Service wrapped cryptographic keys

Answer: D

Question #137

You need to connect your organization's on-premises network with an existing Google Cloud environment that includes one Shared VPC with two subnets named
Production and Non-Production. You are required to:
☞ Use a private transport link.
☞ Configure access to Google Cloud APIs through private API endpoints originating from on-premises environments.
☞ Ensure that Google Cloud APIs are only consumed via VPC Service Controls.
What should you do?

- A. 1. Set up a Cloud VPN link between the on-premises environment and Google Cloud. 2. Configure private access using the restricted.googleapis.com domains in on-premises DNS configurations.
- B. 1. Set up a Partner Interconnect link between the on-premises environment and Google Cloud. 2. Configure private access using the private.googleapis.com domains in on-premises DNS configurations.
- C. 1. Set up a Direct Peering link between the on-premises environment and Google Cloud. 2. Configure private access for both VPC subnets.
- D. 1. Set up a Dedicated Interconnect link between the on-premises environment and Google Cloud. 2. Configure private access using the restricted.googleapis.com domains in on-premises DNS configurations.

Answer: D

Question #138

You recently joined the networking team supporting your company's Google Cloud implementation. You are tasked with familiarizing yourself with the firewall rules configuration and providing recommendations based on your networking and Google Cloud experience. What product should you recommend to detect firewall rules that are overlapped by attributes from other firewall rules with higher or equal priority?

- A. Security Command Center
- B. Firewall Rules Logging
- C. VPC Flow Logs
- D. Firewall Insights

Answer: D

Question #139

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?

- 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

Question #140

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?

- 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

Question #141

You are a member of your company's security team. You have been asked to reduce your Linux bastion host external attack surface by removing all public IP addresses. Site Reliability Engineers (SREs) require access to the bastion host from public locations so they can access the internal VPC while off-site. How should you enable this access?

- A. Implement Cloud VPN for the region where the bastion host lives.
- B. Implement OS Login with 2-step verification for the bastion host.
- C. Implement Identity-Aware Proxy TCP forwarding for the bastion host.
- D. Implement Google Cloud Armor in front of the bastion host.

Answer: C

Question #142

You need to enable VPC Service Controls and allow changes to perimeters in existing environments without preventing access to resources. Which VPC Service
Controls mode should you use?

- A. Cloud Run
- B. Native
- C. Enforced
- D. Dry run

Answer: D

Question #143

You manage your organization's Security Operations Center (SOC). You currently monitor and detect network traffic anomalies in your Google Cloud VPCs based on packet header information. However, you want the capability to explore network flows and their payload to aid investigations. Which Google Cloud product should you use?

- A. Marketplace IDS
- B. VPC Flow Logs
- C. VPC Service Controls logs
- D. Packet Mirroring
- E. Google Cloud Armor Deep Packet Inspection

Answer: D

Question #144

You are exporting application logs to Cloud Storage. You encounter an error message that the log sinks don't support uniform bucket-level access policies. How should you resolve this error?

- A. Change the access control model for the bucket
- B. Update your sink with the correct bucket destination.
- C. Add the roles/logging.logWriter Identity and Access Management (IAM) role to the bucket for the log sink identity.
- D. Add the roles/logging.bucketWriter Identity and Access Management (IAM) role to the bucket for the log sink identity.

Answer: A

Question #145

Your organization has had a few recent DDoS attacks. You need to authenticate responses to domain name lookups. Which Google Cloud service should you use?

- A. Cloud DNS with DNSSEC
- B. Cloud NAT
- C. HTTP(S) Load Balancing
- D. Google Cloud Armor

Answer: A

Question #146

An organization is moving applications to Google Cloud while maintaining a few mission-critical applications on-premises. The organization must transfer the data at a bandwidth of at least 50 Gbps. What should they use to ensure secure continued connectivity between sites?

- A. Dedicated Interconnect
- B. Cloud Router
- C. Cloud VPN
- D. Partner Interconnect

Answer: A

Question #147

Your organization recently deployed a new application on Google Kubernetes Engine. You need to deploy a solution to protect the application. The solution has the following requirements:
☞ Scans must run at least once per week
☞ Must be able to detect cross-site scripting vulnerabilities
☞ Must be able to authenticate using Google accounts
Which solution should you use?

- A. Google Cloud Armor
- B. Web Security Scanner
- C. Security Health Analytics
- D. Container Threat Detection

Answer: B

Question #148

You are designing a new governance model for your organization's secrets that are stored in Secret Manager. Currently, secrets for Production and Non-
Production applications are stored and accessed using service accounts. Your proposed solution must:
☞ Provide granular access to secrets
☞ Give you control over the rotation schedules for the encryption keys that wrap your secrets
☞ Maintain environment separation
☞ Provide ease of management
Which approach should you take?

- A. 1. Use separate Google Cloud projects to store Production and Non-Production secrets. 2. Enforce access control to secrets using project-level identity and Access Management (IAM) bindings. 3. Use customer-managed encryption keys to encrypt secrets.
- B. 1. Use a single Google Cloud project to store both Production and Non-Production secrets. 2. Enforce access control to secrets using secret-level Identity and Access Management (IAM) bindings. 3. Use Google-managed encryption keys to encrypt secrets.

- C. 1. Use separate Google Cloud projects to store Production and Non-Production secrets. 2. Enforce access control to secrets using secret-level Identity and Access Management (IAM) bindings. 3. Use Google-managed encryption keys to encrypt secrets.
- D. 1. Use a single Google Cloud project to store both Production and Non-Production secrets. 2. Enforce access control to secrets using project-level Identity and Access Management (IAM) bindings. 3. Use customer-managed encryption keys to encrypt secrets.

Answer: A

Question #149

You are asked to recommend a solution to store and retrieve sensitive configuration data from an application that runs on Compute Engine. Which option should you recommend?

- A. Cloud Key Management Service
- B. Compute Engine guest attributes
- C. Compute Engine custom metadata
- D. Secret Manager

Answer: D

Question #150

You have been tasked with implementing external web application protection against common web application attacks for a public application on Google Cloud.
You want to validate these policy changes before they are enforced. What service should you use?

- A. Google Cloud Armor's preconfigured rules in preview mode
- B. Prepopulated VPC firewall rules in monitor mode
- C. The inherent protections of Google Front End (GFE)
- D. Cloud Load Balancing firewall rules
- E. VPC Service Controls in dry run mode

Answer: A

Question #151

Your organization has implemented synchronization and SAML federation between Cloud Identity and Microsoft Active Directory. You want to reduce the risk of
Google Cloud user accounts being compromised. What should you do?

- A. Create a Cloud Identity password policy with strong password settings, and configure 2-Step Verification with security keys in the Google Admin console.
- B. Create a Cloud Identity password policy with strong password settings, and configure 2-Step Verification with verification codes via text or phone call in the Google Admin console.
- C. Create an Active Directory domain password policy with strong password settings, and configure post-SSO (single sign-on) 2-Step Verification with security keys in the Google Admin console.

- D. Create an Active Directory domain password policy with strong password settings, and configure post-SSO (single sign-on) 2-Step Verification with verification codes via text or phone call in the Google Admin console.

Answer: C

Question #152

You are on your company's development team. You noticed that your web application hosted in staging on GKE dynamically includes user data in web pages without first properly validating the inputted data. This could allow an attacker to execute gibberish commands and display arbitrary content in a victim user's browser in a production environment.
How should you prevent and fix this vulnerability?

- A. Use Cloud IAP based on IP address or end-user device attributes to prevent and fix the vulnerability.
- B. Set up an HTTPS load balancer, and then use Cloud Armor for the production environment to prevent the potential XSS attack.
- C. Use Web Security Scanner to validate the usage of an outdated library in the code, and then use a secured version of the included library.
- D. Use Web Security Scanner in staging to simulate an XSS injection attack, and then use a templating system that supports contextual auto-escaping.

Answer: D

Question #153

You are the security admin of your company. You have 3,000 objects in your Cloud Storage bucket. You do not want to manage access to each object individually.
You also do not want the uploader of an object to always have full control of the object. However, you want to use Cloud Audit Logs to manage access to your bucket.
What should you do?

- A. Set up an ACL with OWNER permission to a scope of allUsers.
- B. Set up an ACL with READER permission to a scope of allUsers.
- C. Set up a default bucket ACL and manage access for users using IAM.
- D. Set up Uniform bucket-level access on the Cloud Storage bucket and manage access for users using IAM.

Answer: D

Question #154

Your team uses a service account to authenticate data transfers from a given Compute Engine virtual machine instance of to a specified Cloud Storage bucket. An engineer accidentally deletes the service account, which breaks application functionality. You want to recover the application as quickly as possible without compromising security.
What should you do?

- A. Temporarily disable authentication on the Cloud Storage bucket.
- B. Use the undelete command to recover the deleted service account.
- C. Create a new service account with the same name as the deleted service account.
- D. Update the permissions of another existing service account and supply those credentials to the applications.

Answer: B

Question #155

As adoption of the Cloud Data Loss Prevention (Cloud DLP) API grows within your company, you need to optimize usage to reduce cost. Cloud DLP target data is stored in Cloud Storage and BigQuery. The location and region are identified as a suffix in the resource name.
Which cost reduction options should you recommend?

- A. Set appropriate rowsLimit value on BigQuery data hosted outside the US and set appropriate bytesLimitPerFile value on multiregional Cloud Storage buckets.
- B. Set appropriate rowsLimit value on BigQuery data hosted outside the US, and minimize transformation units on multiregional Cloud Storage buckets.
- C. Use rowsLimit and bytesLimitPerFile to sample data and use CloudStorageRegexFileSet to limit scans.
- D. Use FindingLimits and TimespanContfig to sample data and minimize transformation units.

Answer: C

Question #156

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

Answer: AB

Question #157

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.
Store the encrypted data and the wrapped DEK.
▪

Answer: C

Question #158

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.

Answer: C

Question #159

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.

Answer: C

Question #160

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.

Answer: AD

Question #161

Your privacy team uses crypto-shredding (deleting encryption keys) as a strategy to delete personally identifiable information (PII). You need to implement this practice on Google Cloud while still utilizing the majority of the platform's services and minimizing operational overhead. What should you do?

- A. Use client-side encryption before sending data to Google Cloud, and delete encryption keys on-premises.
- B. Use Cloud External Key Manager to delete specific encryption keys.
- C. Use customer-managed encryption keys to delete specific encryption keys.
- D. Use Google default encryption to delete specific encryption keys.

Answer: C

Question #162

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

Answer: C

Question #163

A company is backing up application logs to a Cloud Storage bucket shared with both analysts and the administrator. Analysts should only have access to logs that do not contain any personally identifiable information (PII). Log files containing PII should be stored in another bucket that is only accessible by the administrator.
What should you do?

- A. Use Cloud Pub/Sub and Cloud Functions to trigger a Data Loss Prevention scan every time a file is uploaded to the shared bucket. If the scan detects PII, have the function move into a Cloud Storage bucket only accessible by the administrator.
- B. Upload the logs to both the shared bucket and the bucket only accessible by the administrator. Create a job trigger using the Cloud Data Loss Prevention API. Configure the trigger to delete any files from the shared bucket that contain PII.
- C. On the bucket shared with both the analysts and the administrator, configure Object Lifecycle Management to delete objects that contain any PII.
- D. On the bucket shared with both the analysts and the administrator, configure a Cloud Storage Trigger that is only triggered when PII data is uploaded. Use Cloud Functions to capture the trigger and delete such files.

Answer: A

Question #164

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 KeyRing 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.

Answer: B

Question #165

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.

Answer: C

Question #166

You are the security admin of your company. Your development team creates multiple GCP projects under the "implementation" folder for several dev, staging, and production workloads. You want to prevent data exfiltration by malicious insiders or compromised code by setting up a security perimeter. However, you do not want to restrict communication between the projects.
What should you do?

- A. Use a Shared VPC to enable communication between all projects, and use firewall rules to prevent data exfiltration.
- B. Create access levels in Access Context Manager to prevent data exfiltration, and use a shared VPC for communication between projects.
- C. Use an infrastructure-as-code software tool to set up a single service perimeter and to deploy a Cloud Function that monitors the "implementation" folder via Stackdriver and Cloud Pub/Sub. When the function notices that a new project is added to the folder, it executes Terraform to add the new project to the associated perimeter.
- D. Use an infrastructure-as-code software tool to set up three different service perimeters for dev, staging, and prod and to deploy a Cloud Function that monitors the "implementation" folder via Stackdriver and Cloud Pub/Sub. When the function notices that a new project is added to the folder, it executes Terraform to add the new project to the respective perimeter.

Answer: C

Question #167

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.

Answer: B

Question #168

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.

Answer: A

Question #169

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).

Answer: B

Question #170

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.

Answer: C

Question #171

You perform a security assessment on a customer architecture and discover that multiple VMs have public IP addresses. After providing a recommendation to remove the public IP addresses, you are told those VMs need to communicate to external sites as part of the customer's typical operations. What should you recommend to reduce the need for public IP addresses in your customer's VMs?

- A. Google Cloud Armor
- B. Cloud NAT
- C. Cloud Router
- D. Cloud VPN

Answer: B

Question #172

You work for a large organization where each business unit has thousands of users. You need to delegate management of access control permissions to each business unit. You have the following requirements:
☞ Each business unit manages access controls for their own projects.
Each business unit manages access control permissions at scale.
▪
☞ Business units cannot access other business units' projects.
☞ Users lose their access if they move to a different business unit or leave the company.
☞ Users and access control permissions are managed by the on-premises directory service.
What should you do? (Choose two.)

- A. Use VPC Service Controls to create perimeters around each business unit's project.
- B. Organize projects in folders, and assign permissions to Google groups at the folder level.
- C. Group business units based on Organization Units (OUs) and manage permissions based on OUs
- D. Create a project naming convention, and use Google's IAM Conditions to manage access based on the prefix of project names.
- E. Use Google Cloud Directory Sync to synchronize users and group memberships in Cloud Identity.

Answer: BE

Question #173

Last week, a company deployed a new App Engine application that writes logs to BigQuery. No other workloads are running in the project. You need to validate that all data written to BigQuery was done using the App Engine Default Service Account.
What should you do?

- A. 1. Use StackDriver Logging and filter on BigQuery Insert Jobs. 2. Click on the email address in line with the App Engine Default Service Account in the authentication field. 3. Click Hide Matching Entries. 4. Make sure the resulting list is empty.
- B. 1. Use StackDriver Logging and filter on BigQuery Insert Jobs. 2. Click on the email address in line with the App Engine Default Service Account in the authentication field. 3. Click Show Matching Entries. 4. Make sure the resulting list is empty.
- C. 1. In BigQuery, select the related dataset. 2. Make sure the App Engine Default Service Account is the only account that can write to the dataset.
- D. 1. Go to the IAM section on the project. 2. Validate that the App Engine Default Service Account is the only account that has a role that can write to BigQuery.

Answer: A

Question #174

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

Answer: D

Question #175

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

Answer: AC

Question #176

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).

Answer: C

Question #177

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.

Answer: A

Question #178

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.

Answer: B

Question #179

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.

Answer: B

Question #180

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 control the key lifecycle.
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

Answer: B

Question #181

You are responsible for protecting highly sensitive data in BigQuery. Your operations teams need access to this data, but given privacy regulations, you want to ensure that they cannot read the sensitive fields such as email addresses and first names. These specific sensitive fields should only be available on a need-to- know basis to the HR team. What should you do?

- A. Perform data masking with the DLP API and store that data in BigQuery for later use.
- B. Perform data redaction with the DLP API and store that data in BigQuery for later use.
- C. Perform data inspection with the DLP API and store that data in BigQuery for later use.
- D. Perform tokenization for Pseudonymization with the DLP API and store that data in BigQuery for later use.

Answer: C

Question #182

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.

Answer: B

Question #183

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.

Answer: C

Question #184

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.

Answer: C

Question #185

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.

Answer: A

Question #186

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.

Answer: AC

Question #187

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. Web Security Scanner
- D. Anomaly Detection

Answer: C

Question #188

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".

Answer: A

Question #189

An organization's security and risk management teams are concerned about where their responsibility lies for certain production workloads they are running in
Google Cloud Platform (GCP), and where Google's responsibility lies. They are mostly running workloads using Google Cloud's Platform-as-a-Service (PaaS) offerings, including App Engine primarily.
Which one of these areas in the technology stack would they need to focus on as their primary responsibility when using App Engine?

- A. Configuring and monitoring VPC Flow Logs
- B. Defending against XSS and SQLi attacks
- C. Manage the latest updates and security patches for the Guest OS
- D. Encrypting all stored data

Answer: B

Question #190

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?

- 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

Question #191

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

Answer: B

Question #192

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

Answer: C

Question #193

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

Answer: A

Question #194

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).

Answer: C