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

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

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

Correct Answer: D

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

What should you do?

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

Correct Answer: C

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

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

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

Correct Answer: A

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

What solution would help meet the requirements?

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

Correct Answer: B

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

Which strategy should you use to meet these needs?

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

Correct Answer: A

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

How should the company accomplish this?

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

Correct Answer: D

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

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

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

Correct Answer: C

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

What should you do?

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

Correct Answer: C

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

Which GCP solution should the organization use?

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

Correct Answer: A

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

What should you do?

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

Correct Answer: A

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

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

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

Correct Answer: B