Vendor: Google

Exam Code:PROFESSIONAL-CLOUD-SECURITY-ENGINEER

Exam Name: Professional Cloud Security Engineer

Version: Demo

QUESTION 1

Your organization has on-premises hosts that need to access Google Cloud APIs You must enforce private connectivity between these hosts minimize costs and optimize for operational efficiency What should you do?

A. Route all on-premises traffic to Google Cloud through an IPsec VPN tunnel to a VPC with Private Google Access enabled.

B. Set up VPC peering between the hosts on-premises and the VPC through the internet.

C. Enforce a security policy that mandates all applications to encrypt data with a Cloud Key Management. Service (KMS) key before you send it over the network.

D. Route all on-premises traffic to Google Cloud through a dedicated or Partner interconnect to a VPC with Private Google Access enabled.

Correct Answer: A

QUESTION 2

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

Correct Answer: AD

QUESTION 3

Your organization s customers must scan and upload the contract and their driver license into a web portal in Cloud Storage. You must remove all personally identifiable information (Pll) from files that are older than 12 months. Also you must archive the anonymized files for retention purposes.

What should you do?

A. Set a time to live (TTL) of 12 months for the files in the Cloud Storage bucket that removes PH and moves the files to the archive storage class.

B. Create a Cloud Data Loss Prevention (DLP) inspection job that de-identifies Pll in files created more than 12 months ago and archives them to another Cloud Storage bucket. Delete the original files.

C. Schedule a Cloud Key Management Service (KMS) rotation period of 12 months for the encryption keys of the Cloud Storage files containing Pll to de-identify them Delete the original keys.

D. Configure the Autoclass feature of the Cloud Storage bucket to de-identify Pll Archive the files that are older than 12 months Delete the original files.

Correct Answer: B

QUESTION 4

You manage a fleet of virtual machines (VMs) in your organization. You have encountered issues with lack of patching in many VMs. You need to automate regular patching in your VMs and view the patch management data across multiple projects.

What should you do? (Choose two.)

A. View patch management data in VM Manager by using OS patch management.

B. View patch management data in Artifact Registry.

C. View patch management data in a Security Command Center dashboard.

D. Deploy patches with Security Command Genter by using Rapid Vulnerability Detection.

E. Deploy patches with VM Manager by using OS patch management.

Correct Answer: AE

A. View patch management data in VM Manager by using OS patch management. VM Manager\\'s OS patch management feature allows you to view patch compliance and deployment data across multiple projects.

E. Deploy patches with VM Manager by using OS patch management. VM Manager\\'s OS patch management feature also allows you to automate the deployment of patches to your VMs.

QUESTION 5

Your DevOps team uses Packer to build Compute Engine images by using this process:

1 Create an ephemeral Compute Engine VM.

2 Copy a binary from a Cloud Storage bucket to the VM\\'s file system.

3 Update the VM\\'s package manager.

4 Install external packages from the internet onto the VM.

Your security team just enabled the organizational policy. consrraints/compure.vnExtemallpAccess. to restrict the usage of public IP Addresses on VMs. In response your DevOps team updated their scripts to remove public IP addresses on

the Compute Engine VMs however the build pipeline is failing due to connectivity issues.

What should you do? Choose 2 answers

A. Provision a Cloud NAT instance in the same VPC and region as the Compute Engine VM

B. Provision an HTTP load balancer with the VM in an unmanaged instance group to allow inbound connections from the internet to your VM.

C. Update the VPC routes to allow traffic to and from the internet.

D. Provision a Cloud VPN tunnel in the same VPC and region as the Compute Engine VM.

E. Enable Private Google Access on the subnet that the Compute Engine VM is deployed within.

Correct Answer: AE

QUESTION 6

You need to follow Google-recommended practices to leverage envelope encryption and encrypt data at the application layer. What should you do?

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

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

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

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

Correct Answer: A

Reference: https://cloud.google.com/kms/docs/envelope-encryption Envelope Encryption: https://cloud.google.com/kms/docs/envelope-encryption Here are best practices for managing DEKs:

1.

Generate DEKs locally.

2.

When stored, always ensure DEKs are encrypted at rest.

3.

For easy access, store the DEK near the data that it encrypts.

The DEK is encrypted (also known as wrapped) by a key encryption key (KEK). The process of encrypting a key with another key is known as envelope encryption.

Here are best practices for managing KEKs:

1.

Store KEKs centrally. (KMS)

2.

Set the granularity of the DEKs they encrypt based on their use case.

For example, consider a workload that requires multiple DEKs to encrypt the workload\\'s data chunks.

You could use a single KEK to wrap all DEKs that are responsible for that workload\\'s encryption.

Rotate keys regularly, and also after a suspected incident.

QUESTION 7

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

Correct Answer: A

https://cloud.google.com/iap/docs/concepts-overview "Use IAP when you want to enforce access control policies for applications and resources."

QUESTION 8

A business unit at a multinational corporation signs up for GCP and starts moving workloads into GCP. The business unit creates a Cloud Identity domain with an organizational resource that has hundreds of projects.

Your team becomes aware of this and wants to take over managing permissions and auditing the domain resources. Which type of access should your team grant to meet this requirement?

A. Organization Administrator

B. Security Reviewer

C. Organization Role Administrator

D. Organization Policy Administrator

Correct Answer: C

Here are the permissions available to organizationRoleAdmin

iam.roles.create iam.roles.delete iam.roles.undelete iam.roles.get iam.roles.list iam.roles.update resourcemanager.projects.get resourcemanager.projects.getIamPolicy resourcemanager.projects.list resourcemanager.organizations.get resourcemanager.organizations.getIamPolicy

There are sufficient as per least privilege policy. You can do user management as well as auditing. https://cloud.google.com/iam/docs/understanding-custom-roles

QUESTION 9

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

How can you work with Infrastructure Operations Engineers to best ensure that Windows Compute Engine VMs are up to date with all the latest OS patches?

A. Build new base images when patches are available, and use a CI/CD pipeline to rebuild VMs, deploying incrementally.

B. Federate a Domain Controller into Compute Engine, and roll out weekly patches via Group Policy Object.

C. Use Deployment Manager to provision updated VMs into new serving Instance Groups (IGs).

D. Reboot all VMs during the weekly maintenance window and allow the StartUp Script to download the latest patches from the internet.

Correct Answer: A

Compute Engine doesn\\'t automatically update the OS or the software on your deployed instances. You will need to patch or update your deployed Compute Engine instances when necessary. However, in the cloud it is not recommended that you patch or update individual running instances. Instead it is best to patch the image that was used to launch the instance and then replace each affected instance with a new copy.

QUESTION 10

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.

Correct Answer: C

-Uniform bucket-level access:

https://cloud.google.com/storage/docs/uniform-bucket-level-access#should-you-use -Domain Restricted Sharing: https://cloud.google.com/resource-manager/docs/organization-policy/ restricting-domains#public_data_sharing

---

QUESTION 11

You manage a mission-critical workload for your organization, which is in a highly regulated industry. The workload uses Compute Engine VMs to analyze and process the sensitive data after it is uploaded to Cloud Storage from the endpoint

computers. Your compliance team has detected that this workload does not meet the data protection requirements for sensitive data. You need to meet these requirements:

Manage the data encryption key (DEK) outside the Google Cloud boundary.

Maintain full control of encryption keys through a third-party provider.

Encrypt the sensitive data before uploading it to Cloud Storage.

Decrypt the sensitive data during processing in the Compute Engine VMs.

Encrypt the sensitive data in memory while in use in the Compute Engine VMs.

What should you do? (Choose two.)

A. Configure Customer Managed Encryption Keys to encrypt the sensitive data before it is uploaded to Cloud Storage, and decrypt the sensitive data after it is downloaded into your VMs.

B. Configure Cloud External Key Manager to encrypt the sensitive data before it is uploaded to Cloud Storage, and decrypt the sensitive data after it is downloaded into your VMs.

C. Create Confidential VMs to access the sensitive data.

D. Migrate the Compute Engine VMs to Confidential VMs to access the sensitive data.

E. Create a VPC Service Controls service perimeter across your existing Compute Engine VMs and Cloud Storage buckets.

Correct Answer: BC

QUESTION 12

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: B

Only Forseti security can have both \\'past\\' and \\'present\\' (i.e. historical) records of the resources. https://forsetisecurity.org/about/