Free Questions for Professional-Cloud-Security-Engineer by braindumpscollection

Shared by Hatfield on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

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 45days.

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?

Options:

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

Explanation:

https://cloud.google.com/docs/security/key-management-deep-dive https://cloud.google.com/kms/docs/faq

Question 2

Question Type: **MultipleChoice**

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?

Options:

A- Assign the Project Viewer Identity and Access Management (1AM) role to the DevOps team.

B- Create a custom 1AM role with limited list/view permissions, and assign it to the DevOps team.

C- Create a service account, and grant it the Project Owner 1AM 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 3

Question Type: **MultipleChoice**

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.)

Options:

A- Grant users the compuce.imageUser role in their own projects.

B- Grant users the compuce.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 projects 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:

B, D

Explanation:

https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints - constraints/compute.trustedImageProjects

This list constraint defines the set of projects that can be used for image storage and disk instantiation for Compute Engine. If this constraint is active, only images from trusted projects will be allowed as the source for boot disks for new instances.

Question 4

Question Type: MultipleChoice

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?

Options:

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

Explanation:

https://support.google.com/a/answer/6178640?hl=en

The transfer tool enables you to see what unmanaged users exist, and then invite those unmanaged users to the domain.

Question 5

Question Type: MultipleChoice

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?

Options:

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 6

Question Type: MultipleChoice

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?

Options:

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

Explanation:

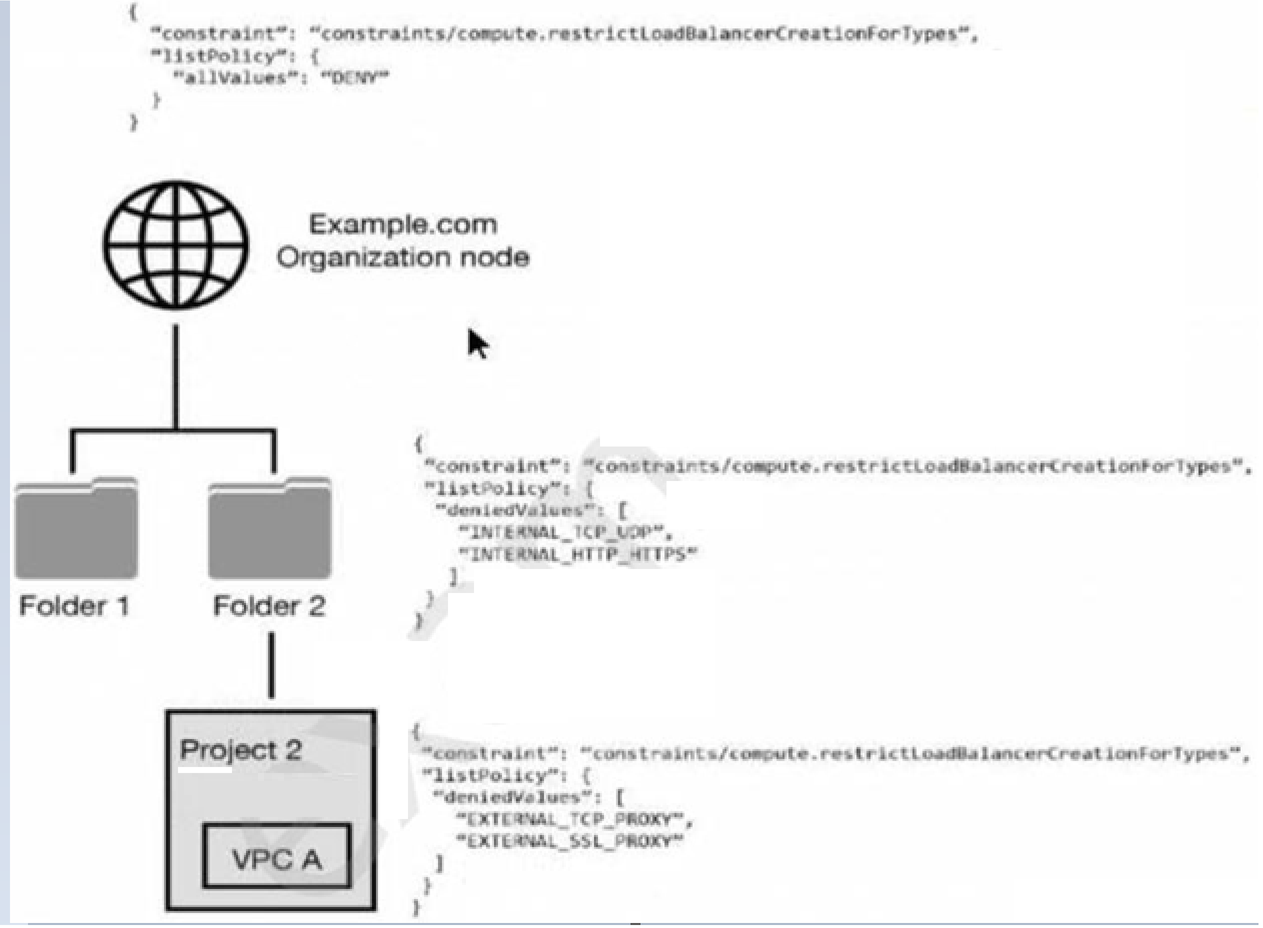
VPC Peering is between organizations not between Projects in an organization. That is Shared VPC. In this case, both projects are in same organization so having VPC Service Controls around both projects with necessary rules should be fine.

https://cloud.google.com/vpc-service-controls/docs/overview

Question 7

Question Type: **MultipleChoice**

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?



```
{
  "constraint": "constraints/compute.restrictLoadBalancerCreationForTypes",
  "listPolicy": {
    "allValues": "DENY"
  }
}
```

```
{
 "constraint": "constraints/compute.restrictLoadBalancerCreationForTypes",
 "listPolicy": {
  "deniedValues": [
    "INTERNAL_TCP_UDP",
    "INTERNAL_HTTP_HTTPS"
  ]
 }
}
```

```
{
 "constraint": "constraints/compute.restrictLoadBalancerCreationForTypes",
 "listPolicy": {
  "deniedValues": [
    "EXTERNAL_TCP_PROXY",
    "EXTERNAL_SSL_PROXY"
  ]
 }
}
```

Options:

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:

D

Question 8

Question Type: **MultipleChoice**

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

Options:

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

Explanation:

https://cloud.google.com/vpc/docs/packet-mirroring

Packet Mirroring clones the traffic of specified instances in your Virtual Private Cloud (VPC) network and forwards it for examination. Packet Mirroring captures all traffic and packet data, including payloads and headers.

Question 9

Question Type: MultipleChoice

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.)

Options:

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 (1AM) service.

D- Use SSO/SAML integration with Cloud Identity for user authentication and user lifecycle management.

E- Provide granular access with predefined roles.

Answer:

D, E

Explanation:

https://cloud.google.com/iam/docs/using-iam-securely#least_privilege Basic roles include thousands of permissions across all Google Cloud services. In production environments, do not grant basic roles unless there is no alternative. Instead, grant the most limited predefined roles or custom roles that meet your needs.

Question 10

Question Type: **MultipleChoice**

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?

Options:

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 1AM 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

Explanation:

Enable the constraints/compute.skipDefaultNetworkCreation organization policy constraint at the organization level.

https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints - constraints/compute.skipDefaultNetworkCreation This boolean constraint skips the creation of the default network and related resources during Google Cloud Platform Project resource creation where this constraint is set to True. By default, a default network and supporting resources are automatically created when creating a Project resource.

Question 11

Question Type: MultipleChoice

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?

Options:

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:

A, D

Question 12

Question Type: **MultipleChoice**

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

Options:

A- Security Reviewer

B- IAP-Secured Tunnel User

C- IAP-Secured Web App User

D- Service Broker Operator

Answer:

C

Explanation:

IAP-Secured Tunnel User: Grants access to tunnel resources that use IAP. IAP-Secured Web App User: Access HTTPS resources which use Identity-Aware Proxy, Grants access to App Engine, Cloud Run, and Compute Engine resources.

https://cloud.google.com/iap/docs/managing-access#roles

20%
DISCOUNT