Google.Professional-Cloud-Security-Engineer.v2024-03-24.q252

Exam Code:	Professional-Cloud-Security-Engineer
Exam Name:	Google Cloud Certified - Professional Cloud Security Engineer Exam
Certification Provider:	Google
Free Question Number:	252
Version:	v2024-03-24
# of views:	505
# of Questions views:	2520
https://www.freeqas.com/qa/Google/Professional-Cloud-Security-Engineer/Google.Professional-Cloud-Security-Engineer.v2024-03-24.q252.html	

NEW QUESTION: 1
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: (SHOW ANSWER)
Explanation
Peering two VPCs does permit traffic to flow between the two shared networks, but it's only bi-directional. Peered VPC networks remain administratively separate.

NEW QUESTION: 2
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 hostname of the repository with a priority greater than 1000.
B. Create an egress firewall rule to allow traffic to the hostname of the repository with a priority less than 1000.
C. Create an egress firewall rule to allow traffic to the CIDR range of the repository with a priority greater than 1000.
D. Create an egress firewall rule to allow traffic to the CIDR range of the repository with a priority less than 1000.

Answer: (SHOW ANSWER)

NEW QUESTION: 3
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: A (LEAVE A REPLY)
https://cloud.google.com/iam/docs/audit-logging/examples-service-accounts

NEW QUESTION: 4
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 (LEAVE A REPLY)
Reference:
In dry run mode, requests that violate the perimeter policy are not denied, only logged. Dry run mode is used to test perimeter configuration and to monitor usage of services without preventing access to resources.
https://cloud.google.com/vpc-service-controls/docs/dry-run-mode

NEW QUESTION: 5
Your company conducts clinical trials and needs to analyze the results of a recent study that are stored in BigQuery. The interval when the medicine was taken contains start and stop dates The interval data is critical to the analysis, but specific dates may identify a particular batch and introduce bias You need to obfuscate the start and end dates for each row and preserve the interval data.
What should you do?
A. Use bucketing to shift values to a predetermined date based on the initial value.
B. Extract the date using TimePartConfig from each date field and append a random month and year
C. Use date shifting with the context set to the unique ID of the test subject
D. Use the FFX mode of format preserving encryption (FPE) and maintain data consistency
Answer: A (LEAVE A REPLY)
"Date shifting techniques randomly shift a set of dates but preserve the sequence and duration of a period of time. Shifting dates is usually done in context to an individual or an entity. That is, each individual's dates are shifted by an amount of time that is unique to that individual."

NEW QUESTION: 6
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 (LEAVE A REPLY)
https://cloud.google.com/resource-manager/docs/organization-policy/using-constraints#list-constraint

NEW QUESTION: 7
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: (SHOW ANSWER)
Explanation/Reference: https://cloud.google.com/solutions/migration-to-google-cloud-building-your-foundation

NEW QUESTION: 8
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. 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.
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. 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.
Section: (none)
Explanation
D. 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.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 9
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 "user email address" as the attribute to facilitate one-way sync.
B. Configure Google Cloud Directory Sync to sync security groups using LDAP search rules that have "user email address" 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: (SHOW ANSWER)
Explanation
search rules that have "user email address" as the attribute to facilitate one-way sync. Reference Links: https://support.google.com/a/answer/6126589?hl=en

NEW QUESTION: 10
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 (LEAVE A REPLY)

https://gsuite.google.com/learn-more/security/security-whitepaper/page-1.html Shared responsibility "Security of the Cloud" - GCP is responsible for protecting the infrastructure that runs all of the services offered in the GCP Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run GCP Cloud services.

NEW QUESTION: 11

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: (SHOW ANSWER)

https://cloud.google.com/blog/products/identity-security/using-your-existing-identity-management- system-with-google-cloud-platform

NEW QUESTION: 12

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 (LEAVE A REPLY)

Section: (none)

Explanation

NEW QUESTION: 13

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 (LEAVE A REPLY)
https://cloud.google.com/policy-intelligence/docs/policy-analyzer-overview Policy Analyzer lets you find out which principals (for example, users, service accounts, groups, and domains) have what access to which Google Cloud resources based on your IAM allow policies.

NEW QUESTION: 14
You are migrating an application into the cloud The application will need to read data from a Cloud Storage bucket. Due to local regulatory requirements, you need to hold the key material used for encryption fully under your control and you require a valid rationale for accessing the key material.
What should you do?
A. Encrypt the data in the Cloud Storage bucket by using Customer Managed Encryption Keys. Configure an 1AM deny policy for unauthorized groups
B. Encrypt the data in the Cloud Storage bucket by using Customer Managed Encryption Keys backed by a Cloud Hardware Security Module (HSM). Enable data access logs.
C. Generate a key in your on-premises environment and store it in a Hardware Security Module (HSM) that is managed on-premises Use this key as an external key in the Cloud Key Management Service (KMS). Activate Key Access Justifications (KAJ) and set the external key system to reject unauthorized accesses.
D. Generate a key in your on-premises environment to encrypt the data before you upload the data to the Cloud Storage bucket Upload the key to the Cloud Key ManagementService (KMS). Activate Key Access Justifications (KAJ) and have the external key system reject unauthorized accesses.
Answer: C (LEAVE A REPLY)
Explanation
By generating a key in your on-premises environment and storing it in an HSM that you manage, you're ensuring that the key material is fully under your control. Using the key as an external key in Cloud KMS allows you to use the key with Google Cloud services without having the key stored on Google Cloud.
Activating Key Access Justifications (KAJ) provides a reason every time the key is accessed, and you can configure the external key system to reject unauthorized access attempts.

NEW QUESTION: 15
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: (SHOW ANSWER)
Explanation
Only Forseti security can have both 'past' and 'present' (i.e. historical) records of the resources.
https://forsetisecurity.org/about/

NEW QUESTION: 16
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: B,D (LEAVE A REPLY)
Reference:
"Google Workspace Login Audit: Login Audit logs track user sign-ins to your domain. These logs only record the login event. They don't record which system was used to perform the login action."
https://cloud.google.com/logging/docs/audit/gsuite-audit-logging#services

NEW QUESTION: 17
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 VPN
B. Cloud Armor
C. Cloud Identity-Aware Proxy
D. Cloud Endpoints

Answer: A (LEAVE A REPLY)

NEW QUESTION: 18
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 (LEAVE A REPLY)
https://cloud.google.com/security/compliance/fips-140-2-validated
Google Cloud Platform uses a FIPS 140-2 validated encryption module called BoringCrypto (certificate 3318) in our production environment. This means that both data in transit to the customer and between data centers, and data at rest are encrypted using FIPS 140-2 validated encryption. The module that achieved FIPS 140-2 validation is part of our BoringSSL library.

NEW QUESTION: 19
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: (SHOW ANSWER)

NEW QUESTION: 20
In a shared security responsibility model for IaaS, which two layers of the stack does the customer share responsibility for? (Choose two.)
A. Access Policies
B. Network Security
C. Hardware
D. Storage Encryption
E. Boot
Answer: (SHOW ANSWER)

NEW QUESTION: 21
Your customer has an on-premises Public Key Infrastructure (PKI) with a certificate authority (CA). You need to issue certificates for many HTTP load balancer frontends. The on-premises PKI should be minimally affected due to many manual processes, and the solution needs to scale.
What should you do?
A. Use Certificate Manager to issue Google managed public certificates and configure it at HTTP the load balancers in your infrastructure as code (laC).
B. Use Certificate Manager to import certificates issued from on-premises PKI and for the frontends.
Leverage the gcloud tool for importing
C. Use a subordinate CA in the Google Certificate Authority Service from the on-premises PKI system to issue certificates for the load balancers.
D. Use the web applications with PKCS12 certificates issued from subordinate CA based on OpenSSL on-premises Use the gcloud tool for importing. Use the External TCP/UDP Network load balancer instead of an external HTTP Load Balancer.
Answer: C (LEAVE A REPLY)
Explanation
This approach allows you to leverage your existing on-premises PKI infrastructure while minimizing its impact and manual processes. By creating a subordinate CA in Google's Certificate Authority Service, you can automate the process of issuing certificates for your HTTP load balancer frontends. This solution scales well as the number of load balancers increases.

NEW QUESTION: 22
You manage one of your organization's Google Cloud projects (Project A). AVPC Service Control (SC) perimeter is blocking API access requests to this project including Pub/Sub. A resource running under a service account in another project (Project B) needs to collect messages from a Pub/Sub topic in your project Project B is not included in a VPC SC perimeter. You need to provide access from Project B to the Pub/Sub topic in Project A using the principle of least Privilege.
What should you do?
A. Remove the Pub/Sub API from the list of restricted services in the perimeter configuration for Project A.
B. Create an access level that allows a developer in Project B to subscribe to the Pub/Sub topic that is located in Project A.
C. Configure an ingress policy for the perimeter in Project A and allow access for the service account in Project B to collect messages.
D. Create a perimeter bridge between Project A and Project B to allow the required communication between both projects.
Answer: (SHOW ANSWER)

NEW QUESTION: 23

Your company is moving to Google Cloud. You plan to sync your users first by using Google Cloud Directory Sync (GCDS). Some employees have already created Google Cloud accounts by using their company email addresses that were created outside of GCDS. You must create your users on Cloud Identity.
What should you do?
A. Configure GCDS and use GCDS search rules lo sync these users.
B. Use the transfer tool to migrate unmanaged users.
C. Configure GCDS and use GCDS exclusion rules to ensure users are not suspended.
D. Write a custom script to identify existing Google Cloud users and call the Admin SDK Directory API to transfer their account.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 24
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: (SHOW ANSWER)
"This encryption method is reversible, which helps to maintain referential integrity across your database and has no character-set limitations." https://cloud.google.com/blog/products/identity-security/take-charge-of-your-data-how-tokenization-makes-data-usable-without-sacrificing-privacy
https://cloud.google.com/dlp/docs/pseudonymization
FPE provides fewer security guarantees compared to other deterministic encryption methods such as AES-SIV. For these reasons, Google strongly recommends using deterministic encryption with AES-SIV instead of FPE for all security sensitive use cases. Other methods like deterministic encryption using AES-SIV provide these stronger security guarantees and are recommended for tokenization use cases unless length and character set preservation are strict requirements-for example, for backward compatibility with a legacy data system.

NEW QUESTION: 25
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: (SHOW ANSWER)
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

NEW QUESTION: 26
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. Enable Access Transparency logs with Access Approval requests for Google employees.
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. Use customer-managed encryption keys.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 27
You want to use the gcloud command-line tool to authenticate using a third-party single sign-on (SSO) SAML identity provider. Which options are necessary to ensure that authentication is supported by the third-party identity provider (IdP)? (Choose two.)
A. SSO SAML as a third-party IdP
B. Identity Platform
C. OpenID Connect
D. Identity-Aware Proxy
E. Cloud Identity
Answer: A,C (LEAVE A REPLY)
Explanation

To provide users with SSO-based access to selected cloud apps, Cloud Identity as your IdP supports the OpenID Connect (OIDC) and Security Assertion Markup Language 2.0 (SAML) protocols.https://cloud.google.com/identity/solutions/enable-sso

NEW QUESTION: 28
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 (1AM) 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: C,E (LEAVE A REPLY)
Explanation
https://cloud.google.com/resource-manager/docs/super-admin-best-practices#discourage_super_admin_account_
- Use a security key or other physical authentication device to enforce two-step verification - Give super admins a separate account that requires a separate login

NEW QUESTION: 29
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: (SHOW ANSWER)
https://cloud.google.com/bigquery/docs/encryption-at-rest

NEW QUESTION: 30
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.viewer

B. roles/logging.admin
C. roles/logging.privateLogViewer
D. roles/viewer
Answer: B (LEAVE A REPLY)

NEW QUESTION: 31
You are in charge of migrating a legacy application from your company datacenters to GCP before the current maintenance contract expires. You do not know what ports the application is using and no documentation is available for you to check. You want to complete the migration without putting your environment at risk.
What should you do?
A. Migrate the application into an isolated project using a "Lift & Shift" approach. Enable all internal TCP traffic using VPC Firewall rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.
B. Migrate the application into an isolated project using a "Lift & Shift" approach in a custom network. Disable all traffic within the VPC and look at the Firewall logs to determine what traffic should be allowed for the application to work properly.
C. Refactor the application into a micro-services architecture in a GKE cluster. Disable all traffic from outside the cluster using Firewall Rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.
D. Refactor the application into a micro-services architecture hosted in Cloud Functions in an isolated project. Disable all traffic from outside your project using Firewall Rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.
Answer: (SHOW ANSWER)
Explanation/Reference:

NEW QUESTION: 32
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 (LEAVE A REPLY)

Explanation

https://cloud.google.com/load-balancing/docs/load-balancing-overview

https://cloud.google.com/load-balancing/docs/load-balancing-overview#choosing_a_load_balancer

NEW QUESTION: 33

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 (LEAVE A REPLY)

Scenarios for exporting Cloud Logging data: Splunk This scenario shows how to export selected logs from Cloud Logging to Pub/Sub for ingestion into Splunk. Splunk is a security information and event management (SIEM) solution that supports several ways of ingesting data, such as receiving streaming data out of Google Cloud through Splunk HTTP Event Collector (HEC) or by fetching data from Google Cloud APIs through Splunk Add-on for Google Cloud. Using the Pub/Sub to Splunk Dataflow template, you can natively forward logs and events from a Pub/Sub topic into Splunk HEC. If Splunk HEC is not available in your Splunk deployment, you can use the Add-on to collect the logs and events from the Pub/Sub topic. https://cloud.google.com/solutions/exporting-stackdriver-logging-for-splunk

NEW QUESTION: 34

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 (LEAVE A REPLY)

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

NEW QUESTION: 35

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: D,E (LEAVE A REPLY)
Explanation
https://cloud.google.com/armor/docs/security-policy-overview#requirements says: The backend service's load balancing scheme must be EXTERNAL, or EXTERNAL_MANAGED *** if you are using global external HTTP(S) load balancer ***.

NEW QUESTION: 36
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 (LEAVE A REPLY)
Explanation
in PaaS the customer is responsible for web app security, deployment, usage, access policy, and content.https://cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate

NEW QUESTION: 37
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 (LEAVE A REPLY)
Explanation
https://youtu.be/MI4iG2GIZMA

NEW QUESTION: 38

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 (LEAVE A REPLY)
"However, even though it is possible to uses tags for target filtering in this manner, we recommend that you use service accounts where possible. Target tags are not access-controlled and can be changed by someone with the instanceAdmin role while VMs are in service. Service accounts are access-controlled, meaning that a specific user must be explicitly authorized to use a service account. There can only be one service account per instance, whereas there can be multiple tags. Also, service accounts assigned to a VM can only be changed when the VM is stopped"

NEW QUESTION: 39
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 Shared VPC.
B. Configure the project with Cloud VPN.
C. Configure the project with Cloud Interconnect.
D. Configure the project with VPC peering.
E. Configure all Compute Engine instances with Private Access.
Answer: (SHOW ANSWER)

NEW QUESTION: 40
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 (LEAVE A REPLY)
Explanation
Scenarios for exporting Cloud Logging data: Splunk This scenario shows how to export selected logs from Cloud Logging to Pub/Sub for ingestion into Splunk. Splunk is a security information and event management (SIEM) solution that supports several ways of ingesting data, such as receiving streaming data out of Google Cloud

through Splunk HTTP Event Collector (HEC) or by fetching data from Google Cloud APIs through Splunk Add-on for Google Cloud. Using the Pub/Sub to Splunk Dataflow template, you can natively forward logs and events from a Pub/Sub topic into Splunk HEC. If Splunk HEC is not available in your Splunk deployment, you can use the Add-on to collect the logs and events from the Pub/Sub topic.https://cloud.google.com/solutions/exporting-stackdriver-logging-for-splunk

NEW QUESTION: 41
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 theuse of the default networks in your organization while following Google-recommended best practices. What should you do?
A. Enable theconstraints/compute.skipDefaultNetworkCreationorganization 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 thecompute.googleapis.comAPI.
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 (LEAVE A REPLY)
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.

NEW QUESTION: 42
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 (LEAVE A REPLY)

NEW QUESTION: 43

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: (SHOW ANSWER)
https://cloud.google.com/compute/docs/images/restricting-image-access

NEW QUESTION: 44
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 (LEAVE A REPLY)
restricted.googleapis.com (199.36.153.4/30) only provides access to Cloud and Developer APIs that support VPC Service Controls. VPC Service Controls are enforced for these services
https://cloud.google.com/vpc/docs/configure-private-google-access-hybrid

NEW QUESTION: 45
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 (LEAVE A REPLY)
Explanation
https://cloud.google.com/resource-manager/docs/organization-policy/using-constraints#list-constraint

NEW QUESTION: 46
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: (SHOW ANSWER)
Explanation
Multiple network interfaces. The simplest way to connect multiple VPC networks through a virtual appliance is by using multiple network interfaces, with each interface connecting to one of the VPC networks. Internet and on-premises connectivity is provided over one or two separate network interfaces. With many NGFW products, internet connectivity is connected through an interface marked as untrusted in the NGFW software.
https://cloud.google.com/architecture/best-practices-vpc-design#l7
This architecture has multiple VPC networks that are bridged by an L7 next-generation firewall (NGFW) appliance, which functions as a multi-NIC bridge between VPC networks. An untrusted, outside VPC network is introduced to terminate hybrid interconnects and internet-based connections that terminate on the outside leg of the L7 NGFW for inspection. There are many variations on this design, but the key principle is to filter traffic through the firewall before the traffic reaches trusted VPC networks.

NEW QUESTION: 47
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. Register a new domain name, and use that for the new Cloud Identity domain.
B. Ask customer's management to discover any other uses of Google managed services, and work with the existing Super Administrator.
C. Contact Google Support and initiate the Domain Contestation Process to use the domain name in your new Cloud Identity domain.
D. Ask Google to provision the data science manager's account as a Super Administrator in the existing domain.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 48
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: (SHOW ANSWER)
Explanation
Secret Manager is a secure and convenient storage system for API keys, passwords, certificates, and other sensitive data. Secret Manager provides a central place and single source of truth to manage, access, and audit secrets across Google Cloud. https://cloud.google.com/secret-manager

NEW QUESTION: 49
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 (LEAVE A REPLY)
Explanation
https://cloud.google.com/load-balancing/docs/ssl - SSL Proxy Load Balancing is a reverse proxy load balancer that distributes SSL traffic coming from the internet to virtual machine (VM) instances in your Google Cloud VPC network.

NEW QUESTION: 50
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 a Shared VPC where the security team manages the firewall rules, and share the network with developers via service projects.
B. 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.
C. Set up VPC Network Peering, and allow developers to peer their network with a Shared VPC.
D. Set up multiple VPC networks, and set up multi-NIC virtual appliances to connect the networks.
Answer: (SHOW ANSWER)

NEW QUESTION: 51
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. Cloud Storage using a scheduled task and gsutil via Cloud Interconnect
B. BigQuery using a data pipeline job with continuous updates via Cloud VPN
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 (LEAVE A REPLY)

NEW QUESTION: 52
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. Use the Admin SDK to create groups and assign IAM permissions from Active Directory.
C. Use the Cloud Identity and Access Management API to create groups and IAM permissions from Active Directory.
D. Set up SAML 2.0 Single Sign-On (SSO), and assign IAM permissions to the groups.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 53
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 (LEAVE A REPLY)
https://cloud.google.com/access-transparency Access approval Explicitly approve access to your data or configurations on Google Cloud. Access Approval requests, when combined with Access Transparency logs, can be used to audit an end-to-end chain from support ticket to access request to approval, to eventual access.

NEW QUESTION: 54
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 (LEAVE A REPLY)
https://cloud.google.com/nat/docs/overview "Cloud NAT (network address translation) lets certain resources without external IP addresses create outbound connections to the internet."

NEW QUESTION: 55
Your company is storing files on Cloud Storage. To comply with local regulations, you want to ensure that uploaded files cannot be deleted within the first 5 years. It should not be possible to lower the retention period after it has been set. What should you do?
A. Apply a retention period of 5 years to the bucket, and lock the bucket.
B. Enable Temporary hold and apply a retention period of 5 years to the bucket.
C. Use Cloud IAM to ensure that nobody has an IAM role that has the permissions to delete files from Cloud Storage.
D. Create an object lifecycle rule using the Age condition and the Delete action. Set the Age condition to 5 years.
Answer: A (LEAVE A REPLY)
A is correct because Bucket Lock allows you to configure a data retention policy for a Cloud Storage bucket that governs how long objects in the bucket must be retained. The feature also allows you to lock the data retention policy, permanently preventing the policy from being reduced or removed.
B is not correct because object holds can be easily released by operators/admins.

C is not correct because an admin can grant themselves or someone else enough rights to tamper with the files in Cloud Storage.
D is not correct because Age condition and a Delete action does not prevent objects from being manually deleted before the Age condition is met.
https://cloud.google.com/storage/docs/bucket-lock

NEW QUESTION: 56
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: (SHOW ANSWER)
https://cloud.google.com/storage/docs/public-access-prevention
Public access prevention protects Cloud Storage buckets and objects from being accidentally exposed to the public. If your bucket is contained within an organization, you can enforce public access prevention by using the organization policy constraint storage.publicAccessPrevention at the project, folder, or organization level.

NEW QUESTION: 57
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 hostname 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 greater than 1000.
C. Create an egress firewall rule to allow traffic to the hostname of the repository with a priority less than 1000.
D. Create an egress firewall rule to allow traffic to the CIDR range of the repository with a priority less than 1000.
Answer: (SHOW ANSWER)

NEW QUESTION: 58
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 (LEAVE A REPLY)

Explanation

"Isolate VMs using service accounts when possible" "even though it is possible to uses tags for target filtering in this manner, we recommend that you use service accounts where possible. Target tags are not access-controlled and can be changed by someone with the instanceAdmin role while VMs are in service.

Service accounts are access-controlled, meaning that a specific user must be explicitly authorized to use a service account. There can only be one service account per instance, whereas there can be multiple tags. Also, service accounts assigned to a VM can only be changed when the VM isstopped."https://cloud.google.com/solutions/best-practices-vpc-design#isolate-vms-service-accounts

NEW QUESTION: 59

An organization is working on their GDPR compliance strategy. It wants to ensure that controls are in place to ensure that customer PII is stored in Cloud Storage buckets without third-party exposure. Which Google Cloud solution should the organization use to verify that PII is stored in the correct place without exposing PII internally?

A. Cloud Storage Bucket Lock

B. Cloud Data Loss Prevention API

C. VPC Service Controls

D. Cloud Security Scanner

Answer: B (LEAVE A REPLY)

A is not correct because Bucket Lock feature is for protecting the data retention policy and doesn't address the use case.

B is correct because Cloud Data Loss Prevention API can be used to inspect Cloud Storage buckets for PII.

C is not correct because while VPC Service Controls can allow customers to define security perimeters around Cloud Storage Buckets in order to mitigate data exfiltration risks, it's not a tool to locate PIIs hence doesn't address this use case.

D is not correct because Cloud Security Scanner is a web security scanner for App Engine, Compute Engine, and Google Kubernetes Engine applications and doesn't address the use case.

https://cloud.google.com/storage/docs/bucket-lock

https://cloud.google.com/dlp/docs/inspecting-storage#inspecting-gcs

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

https://cloud.google.com/security-scanner/

NEW QUESTION: 60

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. Enable Cloud Identity-Aware Proxy to filter out credit card numbers before storing the logs in BigQuery.

D. Leverage Security Command Center to scan for the assets of type Credit Card Number in BigQuery.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 61
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: (SHOW ANSWER)
https://cloud.google.com/load-balancing/docs/load-balancing-overview
https://cloud.google.com/load-balancing/docs/load-balancing-overview#choosing_a_load_balancer

NEW QUESTION: 62
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 (LEAVE A REPLY)
Explanation
https://gsuite.google.com/learn-more/security/security-whitepaper/page-1.html Shared responsibility "Security of the Cloud" - GCP is responsible for protecting the infrastructure that runs all of the services offered in the GCP

Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run GCP Cloud services.

NEW QUESTION: 63
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 (LEAVE A REPLY)
Explanation
- 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

NEW QUESTION: 64
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 (LEAVE A REPLY)
https://cloud.google.com/vpc/docs/private-service-connect
An API bundle:
All APIs (all-apis): most Google APIs
(same as private.googleapis.com).
VPC-SC (vpc-sc): APIs that VPC Service Controls supports
(same as restricted.googleapis.com).
VMs in the same VPC network as the endpoint (all regions)
On-premises systems that are connected to the VPC network that contains the endpoint

NEW QUESTION: 65
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 (LEAVE A REPLY)
Explanation
This PD and bucket data is encrypted using a Google-generated data encryption key (DEK) and key encryption key (KEK). The CMEK feature allows you to create, use, and revoke the key encryption key (KEK). Google still controls the data encryption key (DEK). For more information on Google data encryption keys, see Encryption at Rest.
https://cloud.google.com/dataproc/docs/concepts/configuring-clusters/customer-managed-encryption
https://codelabs.developers.google.com/codelabs/encrypt-and-decrypt-data-with-cloud-kms#0

NEW QUESTION: 66
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 (LEAVE A REPLY)
Explanation
https://support.google.com/a/answer/9176734
Use backup codes for account recovery If you need to recover an account, use backup codes. Accounts are still protected by 2-Step Verification, and backup codes are easy to generate.

NEW QUESTION: 67
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. Cloud VPN

B. Cloud Interconnect

C. VPC peering

D. Shared VPC

Answer: A (LEAVE A REPLY)

NEW QUESTION: 68

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. IAM Network User Role

C. Static routes

D. IP Forwarding

E. Private Google Access

Answer: C,E (LEAVE A REPLY)

NEW QUESTION: 69

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

Explanation/Reference: https://cloud.google.com/kms/docs/envelope-encryption

NEW QUESTION: 70

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 (LEAVE A REPLY)
Explanation
https://cloud.google.com/recommender/docs/tutorial-iac

NEW QUESTION: 71
When creating a secure container image, which two items should you incorporate into the build if possible? (Choose two.)
A. Use many container image layers to hide sensitive information.
B. Use public container images as a base image for the app.
C. Ensure that the app does not run as PID 1.
D. Package a single app as a container.
E. Remove any unnecessary tools not needed by the app.
Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 72
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 (LEAVE A REPLY)
https://cloud.google.com/sql/docs/mysql/cmek
"You might have situations where you want to permanently destroy data encrypted with CMEK. To do this, you destroy the customer-managed encryption key version. You can't destroy the keyring or key, but you can destroy key versions of the key."

NEW QUESTION: 73
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: A,C (LEAVE A REPLY)
https://cloud.google.com/solutions/pci-dss-compliance-in-gcp

NEW QUESTION: 74
You are routing all your internet facing traffic from Google Cloud through your on-premises internet connection. You want to accomplish this goal securely and with the highest bandwidth possible.
What should you do?
A. Create a routing VM in Compute Engine Configure the default route with the VM as the next hop.
B. Configure Cloud Interconnect with HA VPN Replace the default 0 0 0 0/0 route to an on-premises destination.
C. Create an HA VPN connection to Google Cloud Replace the default 0 0 0 0/0 route.
D. Configure Cloud Interconnect and route traffic through an on-premises firewall.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 75
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: (SHOW ANSWER)
https://cloud.google.com/solutions/best-practices-for-building-containers

NEW QUESTION: 76
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: (SHOW ANSWER)
https://cloud.google.com/kms/docs/ekm#how_it_works
- First, you create or use an existing key in a supported external key management partner system. This key has a unique URI or key path.
- Next, you grant your Google Cloud project access to use the key, in the external key management partner system.
- In your Google Cloud project, you create a Cloud EKM key, using the URI or key path for the externally-managed key.

NEW QUESTION: 77
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. Use Google Cloud Directory Sync to synchronize users and group memberships in Cloud Identity.
C. Group business units based on Organization Units (OUs) and manage permissions based on OUs.
D. Organize projects in folders, and assign permissions to Google groups at the folder level.
E. Create a project naming convention, and use Google's IAM Conditions to manage access based on the prefix of project names.
Answer: (SHOW ANSWER)

NEW QUESTION: 78
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: A,B (LEAVE A REPLY)
Explanation
Implied IPv4 allow egress rule. An egress rule whose action is allow, destination is 0.0.0.0/0, and priority is the lowest possible (65535) lets any instance send traffic to any destination Implied IPv4 deny ingress rule. An ingress rule whose action is deny, source is 0.0.0.0/0, and priority is the lowest possible (65535) protects all instances by blocking incoming connections to them.
https://cloud.google.com/vpc/docs/firewalls?hl=en#default_firewall_rules

NEW QUESTION: 79
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: (SHOW ANSWER)
https://youtu.be/MI4iG2GIZMA

NEW QUESTION: 80
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 (LEAVE A REPLY)
Explanation

https://cloud.google.com/vpc-service-controls/docs/service-perimeters#secure-google-managed-resources If you're using Shared VPC, you must include the host project in a service perimeter along with any projects that belong to the Shared VPC.

NEW QUESTION: 81
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: (SHOW ANSWER)
https://cloud.google.com/vpc/docs/shared-vpc#svc_proj_admins

NEW QUESTION: 82
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 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.
B. 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.
C. 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.
D. 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.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 83
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 (LEAVE A REPLY)
Explanation

https://cloud.google.com/armor/docs/security-policy-overview#edge-security

NEW QUESTION: 84
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 (LEAVE A REPLY)
If the environment variable GOOGLE_APPLICATION_CREDENTIALS is set, ADC uses the service account key or configuration file that the variable points to. If the environment variable GOOGLE_APPLICATION_CREDENTIALS isn't set, ADC uses the service account that is attached to the resource that is running your code.
https://cloud.google.com/docs/authentication/production#passing_the_path_to_the_service_account_key_in_code

NEW QUESTION: 85
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: A,C (LEAVE A REPLY)
A) IPsec VPN tunels: https://cloud.google.com/network-connectivity/docs/vpn/concepts/overview Interconnect https://cloud.google.com/network-connectivity/docs/interconnect/concepts/dedicated-overview

NEW QUESTION: 86
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. Delete non-used versions from Container Registry.
C. Use a Continuous Delivery tool to deploy the application.
D. Build small containers using small base images.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 87
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. 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.
B. 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.
C. Migrate the application into an isolated project using a "Lift & Shift" approach. Enable all internal TCP traffic using VPC Firewall rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.
D. Migrate the application into an isolated project using a "Lift & Shift" approach in a custom network. Disable all traffic within the VPC and look at the Firewall logs to determine what traffic should be allowed for the application to work properly.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 88
As adoption of the Cloud Data Loss Prevention (DLP) API grows within the company, you need to optimize usage to reduce cost. 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: (SHOW ANSWER)
https://cloud.google.com/dlp/docs/inspecting-storage#sampling https://cloud.google.com/dlp/docs/best-practices-costs#limit_scans_of_files_in_to_only_relevant_files

NEW QUESTION: 89

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 endpomt 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 2 answers
A. Create a VPC Service Controls service perimeter across your existing Compute Engine VMs and Cloud Storage buckets
B. Migrate the Compute Engine VMs to Confidential VMs to access the sensitive data.
C. 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
D. Create Confidential VMs to access the sensitive data.
E. 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.
Answer: (SHOW ANSWER)
Explanation
https://cloud.google.com/confidential-computing/confidential-vm/docs/creating-cvm-instance#considerations Confidential VM does not support live migration. You can only enable Confidential Computing on a VM when you first create the instance.https://cloud.google.com/confidential-computing/confidential-vm/docs/creating-cvm-instance

NEW QUESTION: 90
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 (LEAVE A REPLY)
Explanation
https://cloud.google.com/logging/docs/export/aggregated_sinks#supported-destinations You can use aggregated sinks to route logs within or between the same organizations and folders to the following destinations: - Another Cloud Logging bucket: Log entries held in Cloud Logging log buckets.

NEW QUESTION: 91

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.
Section: (none)
Explanation
Answer: D (LEAVE A REPLY)
Reference:
https://cloud.google.com/solutions/best-practices-for-building-containers

NEW QUESTION: 92
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 KeyRing level.
D. Create a KeyRing per persistent disk, with each KeyRing containing a single Key. Manage the IAM permissions at the Key level.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 93
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. 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.
B. Use Google Cloud Directory Sync to synchronize your local identity management system to Cloud Identity.
C. Use the Google Admin console to view which managed users are using a personal account for their recovery email.
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. Add users to your managed Google account and force users to change the email addresses associated with their personal accounts.
Answer: (SHOW ANSWER)

NEW QUESTION: 94
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 (LEAVE A REPLY)
https://cloud.google.com/docs/enterprise/best-practices-for-enterprise- organizations#centralize_network_control

NEW QUESTION: 95
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. Folder
C. Project

D. Resource
Answer: C (LEAVE A REPLY)

NEW QUESTION: 96
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: (SHOW ANSWER)
https://cloud.google.com/logging/docs/audit/#data-access "Data Access audit logs contain API calls that read the configuration or metadata of resources, as well as user-driven API calls that create, modify, or read user-provided resource data."

NEW QUESTION: 97
You want to protect the default VPC network from all inbound and outbound internet traffic. What action should you take?
A. Create a Deny All inbound internet firewall rule.
B. Create a Deny All outbound internet firewall rule.
C. Create a new subnet in the VPC network with private Google access enabled.
D. Create instances without external IP addresses only.
Answer: B (LEAVE A REPLY)
A is not correct because a Deny All inbound firewall is already part of the standard configuration and does not need to be added.
B is correct because all inbound traffic is already blocked, but all egress traffic is allowed by default. To prevent any outbound traffic an extra rule needs to be added.
C is not correct because private Google allows calls to Google managed APIs from private IP addresses, but it does neither prevent you from providing external IPs or any other outgoing traffic from your instances.
D is not correct because as outbound traffic can still be coming from instances with private IPs if Cloud NAT is used.
https://cloud.google.com/nat/docs/overview
https://cloud.google.com/vpc/docs/private-access-options
https://cloud.google.com/vpc/docs/using-firewalls

NEW QUESTION: 98
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 an HTTP load balancer with the VM in an unmanaged instance group to allow inbound connections from the internet to your VM.
B. Enable Private Google Access on the subnet that the Compute Engine VM is deployed within.
C. Provision a Cloud VPN tunnel in the same VPC and region as the Compute Engine VM.
D. Update the VPC routes to allow traffic to and from the internet.
E. Provision a Cloud NAT instance in the same VPC and region as the Compute Engine VM
Answer: (SHOW ANSWER)

NEW QUESTION: 99
As adoption of the Cloud Data Loss Prevention (DLP) API grows within the company, you need to optimize usage to reduce cost. 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 (LEAVE A REPLY)
https://cloud.google.com/dlp/docs/reference/rest/v2/InspectJobConfig

NEW QUESTION: 100
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 (LEAVE A REPLY)
Reference:
https://cloud.google.com/iam/docs/understanding-service-accounts

NEW QUESTION: 101
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: (SHOW ANSWER)
https://cloud.google.com/armor/docs/security-policy-concepts

NEW QUESTION: 102
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 x-forwarded-for headers 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 user's unique identifier headers in the HTTP requests.
D. Make sure that the ERP system can validate the JWT assertion in the HTTP requests.
Answer: (SHOW ANSWER)

NEW QUESTION: 103
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: (SHOW ANSWER)
"Your team needs to obtain a unified log view of all development cloud projects in your SIEM" - This means we are ONLY interested in development projects. "The development projects are under the NONPROD organization

folder with the test and pre-production projects" - We will need to filter out development from others i.e test and pre-prod. "The development projects share the ABC-BILLING billing account with the rest of the organization." - This is unnecessary information.

NEW QUESTION: 104
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 (1AM) roles.
B. Disallow inheritance of organization policies.
C. Identify inherited Identity and Access Management (1AM) 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: (SHOW ANSWER)
Explanation
https://cloud.google.com/resource-manager/docs/project-migration#plan_policy When you migrate your project, it will no longer inherit the policies from its current place in the resource hierarchy, and will be subject to the effective policy evaluation at its destination. We recommend making sure that the effective policies at the project's destination match as much as possible the policies that the project had in its source location.
https://cloud.google.com/resource-manager/docs/project-migration#import_export_folders Policy inheritance can cause unintended effects when you are migrating a project, both in the source and destination organization resources. You can mitigate this risk by creating specific folders to hold only projects for export and import, and ensuring that the same policies are inherited by the folders in both organization resources. You can also set permissions on these folders that will be inherited to the projects moved within them, helping to accelerate the project migration process.

NEW QUESTION: 105
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 (LEAVE A REPLY)
With Google Cloud Directory Sync (GCDS), you can synchronize the data in your Google Account with your Microsoft Active Directory or LDAP server. GCDS doesn't migrate any content (such as email messages, calendar events, or files) to your Google Account. You use GCDS to synchronize your Google users, groups, and shared contacts to match the information in your LDAP server.
https://support.google.com/a/answer/106368?hl=en

NEW QUESTION: 106
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 (LEAVE A REPLY)
Explanation
https://cloud.google.com/vpc/docs/private-service-connect
An API bundle:
All APIs (all-apis): most Google APIs
(same as private.googleapis.com).
VPC-SC (vpc-sc): APIs that VPC Service Controls supports
(same as restricted.googleapis.com).
VMs in the same VPC network as the endpoint (all regions)
On-premises systems that are connected to the VPC network that contains the endpoint

NEW QUESTION: 107
Your organization develops software involved in many open source projects and is concerned about software supply chain threats You need to deliver provenance for the build to demonstrate the software is untampered. What should you do?
A. * 1- Generate Supply Chain Levels for Software Artifacts (SLSA) level 3 assurance by using Cloud Build.
* 2. View the build provenance in the Security insights side panel within the Google Cloud console.

B. * 1. Review the software process.
* 2. Generate private and public key pairs and use Pretty Good Privacy (PGP) protocols to sign the output software artifacts together with a file containing the address of your enterprise and point of contact.
* 3. Publish the PGP signed attestation to your public web page.
C. * 1, Publish the software code on GitHub as open source.
* 2. Establish a bug bounty program, and encourage the open source community to review, report, and fix the vulnerabilities.
D. * 1. Hire an external auditor to review and provide provenance
* 2. Define the scope and conditions.
* 3. Get support from the Security department or representative.
Answer: A (LEAVE A REPLY)
* 4. Publish the attestation to your public web page.
Explanation:
https://cloud.google.com/build/docs/securing-builds/view-build-provenance

NEW QUESTION: 108
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: (SHOW ANSWER)
Explanation
https://cloud.google.com/vpc-service-controls/docs/overview#isolate

NEW QUESTION: 109
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 (LEAVE A REPLY)

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.

NEW QUESTION: 110
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 (LEAVE A REPLY)
Multiple network interfaces. The simplest way to connect multiple VPC networks through a virtual appliance is by using multiple network interfaces, with each interface connecting to one of the VPC networks. Internet and on-premises connectivity is provided over one or two separate network interfaces. With many NGFW products, internet connectivity is connected through an interface marked as untrusted in the NGFW software.
https://cloud.google.com/architecture/best-practices-vpc-design#l7
This architecture has multiple VPC networks that are bridged by an L7 next-generation firewall (NGFW) appliance, which functions as a multi-NIC bridge between VPC networks. An untrusted, outside VPC network is introduced to terminate hybrid interconnects and internet-based connections that terminate on the outside leg of the L7 NGFW for inspection. There are many variations on this design, but the key principle is to filter traffic through the firewall before the traffic reaches trusted VPC networks.

NEW QUESTION: 111
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 (LEAVE A REPLY)

You can rotate a key by creating a new key, updating applications to use the new key, and deleting the old key. Use the serviceAccount.keys.create() method and serviceAccount.keys.delete() method together to automate the rotation.

NEW QUESTION: 112
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 (LEAVE A REPLY)
Google encrypts and authenticates data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. All VM-to-VM traffic within a VPC network and peered VPC networks is encrypted. https://cloud.google.com/docs/security/encryption-in-transit#cio-level_summary

NEW QUESTION: 113
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 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.
B. 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.
C. 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.
D. 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.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 114
Your company wants to collect and analyze CVE information for packages in container images, and wants to prevent images with known security issues from running in your Google Kubernetes Engine environment. Which two security features does Google recommend including in a container build pipeline?
A. Deployment policies
B. Password policies
C. Vulnerability scanning
D. Network isolation
Answer: A (LEAVE A REPLY)
A is correct because deployment policies defined in Binary Authorization ensure that only trusted images can be deployed in Google Kubernetes Engine clusters. Binary Authorization can integrate with Container Analysis which scans container images stored in Container Registry for vulnerabilities and stores trusted metadata used in the authorization process.
B is not correct because it doesn't address the use case.
C is correct because vulnerability scanning can be performed by Container Analysis to discover package vulnerability information in container base images and obtain CVE data from respective Linux distributions.
D is not correct because it doesn't address the use case.
https://cloud.google.com/binary-authorization/docs/overview
https://cloud.google.com/container-registry/docs/container-analysis

NEW QUESTION: 115
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 (LEAVE A REPLY)
Reference:
https://cloud.google.com/blog/products/gcp/dnssec-now-available-in-cloud-dns

NEW QUESTION: 116

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

NEW QUESTION: 117
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. Configure a custom retention policy of 12 years on your Google Cloud's operations suite log bucket in the EUROPE-WEST1 region.
B. Use a Pub/Sub topic to forward your application logs to a Cloud Storage bucket in the EUROPE-WEST1 region.
C. 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.
D. 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.
Answer: (SHOW ANSWER)

NEW QUESTION: 118
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 projects as the exceptions in a deny operation.
B. In Resource Manager, edit the organization permissions. Add the project ID as member with the role: Compute Image User.
C. In Resource Manager, edit the project permissions for the trusted project. Add the organization as member with the role: Compute Image User.
D. 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.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 119

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: (SHOW ANSWER)
Explanation/Reference: https://cloud.google.com/solutions/secure-data-workloads-use-cases

NEW QUESTION: 120
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: C (LEAVE A REPLY)
Explanation/Reference: https://cloud.google.com/vpc/docs/shared-vpc

NEW QUESTION: 121
You are auditing all your Google Cloud resources in the production project. You want to identity all principals who can change firewall rules.
What should you do?
A. Use Firewall Insights to understand your firewall rules usage patterns.
B. Reference the Security Health Analytics - Firewall Vulnerability Findings in the Security Command Center.
C. Use Policy Analyzer lo query the permissions compute, firewalls, create of compute, firewalls. Create of compute,firewalls.delete.
D. Use Policy Analyzer to query the permissions compute, firewalls, get of compute, firewalls, list.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 122
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: D (LEAVE A REPLY)
Explanation/Reference:
Reference; https://cloud.google.com/dlp/docs/deidentify-sensitive-data

NEW QUESTION: 123
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 (LEAVE A REPLY)
Explanation/Reference: https://cloud.google.com/security-scanner/

NEW QUESTION: 124
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 (LEAVE A REPLY)
Reference:
https://cloud.google.com/kms/docs/envelope-encryption

NEW QUESTION: 125
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: B,D (LEAVE A REPLY)
https://cloud.google.com/blog/products/containers-kubernetes/exploring-container-security-the-shared-responsibility-model-in-gke-container-security-shared-responsibility-model-gke

NEW QUESTION: 126
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 (LEAVE A REPLY)
Explanation
"In order to be able to keep using the existing identity management system, identities need to be synchronized between AD and GCP IAM. To do so google provides a tool called Cloud Directory Sync. This tool will read all identities in AD and replicate those within GCP. Once the identities have been replicated then it's possible to apply IAM permissions on the groups. After that you will configure SAML so google can act as a service provider and either you ADFS or other third party tools like Ping or Okta will act as the identity provider. This way you effectively delegate the authentication from Google to something that is under your control."

NEW QUESTION: 127

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 (LEAVE A REPLY)
Explanation
Reference https://cloud.google.com/kubernetes-engine/docs/how-to/dynamic-provisioning-cmek

NEW QUESTION: 128
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: (SHOW ANSWER)
Explanation
https://cloud.google.com/compute/docs/access/iam

NEW QUESTION: 129
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 (1AM) roles with permissions corresponding to each Active Directory group.
E. Create Identity and Access Management (1AM) groups with permissions corresponding to each Active Directory group.
Answer: C,E (LEAVE A REPLY)
https://cloud.google.com/architecture/identity/federating-gcp-with-active-directory-synchronizing-user-accounts?hl=en

https://cloud.google.com/architecture/identity/federating-gcp-with-active-directory-synchronizing-user-accounts?hl=en#deciding_where_to_deploy_gcds

NEW QUESTION: 130
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: (SHOW ANSWER)
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

NEW QUESTION: 131
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: (SHOW ANSWER)
Explanation
https://cloud.google.com/access-transparency Access approval Explicitly approve access to your data or configurations on Google Cloud. Access Approval requests, when combined with Access Transparency logs, can be used to audit an end-to-end chain from support ticket to access request to approval, to eventual access.

NEW QUESTION: 132
You have defined subnets in a VPC within Google Cloud Platform. You need multiple projects to create Compute Engine instances with IP addresses from these subnets. What should you do?
A. Configure Cloud VPN between the projects.
B. Set up VPC peering between all related projects.
C. Change the VPC subnets to enable private Google access.
D. Use Shared VPC to share the subnets with the other projects.
Answer: D (LEAVE A REPLY)
A is not correct as Cloud VPN between projects does not provide you the functionality to share a subnet to host resources on.

B is not correct because peering two VPCs does allow traffic between the two shared networks, but it's only bi-directional. Peered VPC networks remain administratively separate.
C is not correct because private Google access allows you to access APIs from a private IP, but it does not have any impact on creating Compute instances on a specific subnet.
D is correct because s Shared VPC allows you to share a VPC into multiple projects, keep administrative oversight in the host project, while restricting the other projects to only create VMs on IPs in the shared VPC.
https://cloud.google.com/vpc/docs/shared-vpc
https://cloud.google.com/vpc/docs/vpc-peering

NEW QUESTION: 133
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 anddata 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: (SHOW ANSWER)
Explanation
https://cloud.google.com/solutions/best-practices-vpc-design
"Setting up your payment-processing environment" section
inhttps://cloud.google.com/solutions/pci-dss-compliance-in-gcp.

NEW QUESTION: 134
Your company is concerned about unauthorized parties gaming access to the Google Cloud environment by using a fake login page. You must implement a solution to protect against person-in-the-middle attacks.
Which security measure should you use?
A. Text message or phone call code
B. Security key
C. Google Authenticator application
D. Google prompt
Answer: B (LEAVE A REPLY)
Explanation
A security key is a physical device that you can use for two-step verification, providing an additional layer of security for your Google Account. Security keys can defend against phishing and man-in-the-middle attacks, making your login process more secure.

NEW QUESTION: 135
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. Use a private connection to create the super admin accounts to avoid sending your credentials over the Internet.
B. Disable any Identity and Access Management (1AM) 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. Provide non-privileged identities to the super admin users for their day-to-day activities.
E. Create an access level in the Google Admin console to prevent super admin from logging in to Google Cloud.
Answer: C,E (LEAVE A REPLY)

NEW QUESTION: 136
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 Project per department under the Organization. For each department's Project, assign the Project Browser role to the Google Group related to that department.
B. 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.
C. 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.
D. 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.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 137
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 (LEAVE A REPLY)
https://cloud.google.com/vpc-service-controls/docs/overview#benefits
https://github.com/terraform-google-modules/terraform-google-vpc-service-controls/tree/master/examples/automatic_folder

NEW QUESTION: 138
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: (SHOW ANSWER)
Reference:
https://cloud.google.com/dlp/docs/deidentify-sensitive-data

NEW QUESTION: 139
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: B (LEAVE A REPLY)
Explanation/Reference: https://cloud.google.com/solutions/federating-gcp-with-active-directory-introduction

NEW QUESTION: 140
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: (SHOW ANSWER)
https://cloud.google.com/security-scanner/

NEW QUESTION: 141
Your organization previously stored files in Cloud Storage by using Google Managed Encryption Keys (GMEK). but has recently updated the internal policy to require Customer Managed Encryption Keys (CMEK). You need to re-encrypt the files quickly and efficiently with minimal cost.
What should you do?
A. Encrypt the files locally, and then use gsutil to upload the files to a new bucket.
B. Copy the files to a new bucket with CMEK enabled in a secondary region
C. Reupload the files to the same Cloud Storage bucket specifying a key file by using gsutil.
D. Change the encryption type on the bucket to CMEK, and rewrite the objects
Answer: D (LEAVE A REPLY)
Rewriting the objects in-place within the same bucket, specifying the new CMEK for encryption, allows you to re-encrypt the data without downloading and re-uploading it, thus minimizing costs and time.
https://cloud.google.com/storage/docs/encryption/using-customer-managed-keys

NEW QUESTION: 142
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 (LEAVE A REPLY)

Explanation

nodeSelector is the simplest recommended form of node selection constraint. You can add the nodeSelector field to your Pod specification and specify the node labels you want the target node to have. Kubernetes only schedules the Pod onto nodes that have each of the labels you specify. => https://kubernetes.io/docs/concepts/scheduling-eviction/assign-pod-node/#nodeselector Tolerations are applied to pods. Tolerations allow the scheduler to schedule pods with matching taints. Tolerations allow scheduling but don't guarantee scheduling: the scheduler also evaluates other parameters as part of its function. => https://kubernetes.io/docs/concepts/scheduling-eviction/taint-and-toleration/

NEW QUESTION: 143

You define central security controls in your Google Cloud environment for one of the folders in your organization you set an organizational policy to deny the assignment of external IP addresses to VMs. Two days later you receive an alert about a new VM with an external IP address under that folder.

What could have caused this alert?

A. The organizational policy constraint wasn't properly enforced and is running in "dry run mode.

B. The VM was created with a static external IP address that was reserved in the project before the organizational policy rule was set.

C. At project level, the organizational policy control has been overwritten with an 'allow' value.

D. The policy constraint on the folder level does not have any effect because of an allow" value for that constraint on the organizational level.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 144

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: (SHOW ANSWER)

Explanation

https://cloud.google.com/iam/docs/understanding-roles#project-roles

NEW QUESTION: 145
You are in charge of migrating a legacy application from your company datacenters to GCP before the current maintenance contract expires. You do not know what ports the application is using and no documentation is available for you to check. You want to complete the migration without putting your environment at risk.
What should you do?
A. Migrate the application into an isolated project using a "Lift & Shift" approach. Enable all internal TCP traffic using VPC Firewall rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.
B. Migrate the application into an isolated project using a "Lift & Shift" approach in a custom network. Disable all traffic within the VPC and look at the Firewall logs to determine what traffic should be allowed for the application to work properly.
C. Refactor the application into a micro-services architecture in a GKE cluster. Disable all traffic from outside the cluster using Firewall Rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.
D. Refactor the application into a micro-services architecture hosted in Cloud Functions in an isolated project. Disable all traffic from outside your project using Firewall Rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.
Answer: A (LEAVE A REPLY)
Explanation
Migrate the application into an isolated project using a "Lift & Shift" approach. Enable all internal TCP traffic using VPC Firewall rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.

NEW QUESTION: 146
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: (SHOW ANSWER)
Explanation
https://cloud.google.com/storage/docs/public-access-prevention
Public access prevention protects Cloud Storage buckets and objects from being accidentally exposed to the public. If your bucket is contained within an organization, you can enforce public access prevention by using the organization policy constraint storage.publicAccessPrevention at the project, folder, or organization level.

NEW QUESTION: 147

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: (SHOW ANSWER)

Explanation

https://cloud.google.com/logging/docs/audit/#data-access "Data Access audit logs contain API calls that read the configuration or metadata of resources, as well as user-driven API calls that create, modify, or read user-provided resource data."

NEW QUESTION: 148

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 (LEAVE A REPLY)

https://cloud.google.com/bigquery#:~:text=BigQuery%20transparently%20and%20automatically%20provides,charge%20and%20no%20additional%20setup.&text=BigQuery%20also%20provides%20ODBC%20and,interact%20with%20its%20powerful%20engine.

NEW QUESTION: 149

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 (LEAVE A REPLY)

Explanation

https://cloud.google.com/load-balancing/docs/load-balancing-overview#external_versus_internal_load_balancing

NEW QUESTION: 150

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. Data Access

C. System Event

D. Access Transparency

Answer: D (LEAVE A REPLY)

NEW QUESTION: 151

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: A,B (LEAVE A REPLY)

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

NEW QUESTION: 152

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: C (LEAVE A REPLY)

https://cloud.google.com/solutions/pci-dss-compliance-in-gcp

NEW QUESTION: 153

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 (LEAVE A REPLY)
Reference:
https://cloud.google.com/docs/enterprise/best-practices-for-enterprise- organizations#centralize_network_control

NEW QUESTION: 154
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. 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.
B. 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.
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: (SHOW ANSWER)

NEW QUESTION: 155
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 (LEAVE A REPLY)

https://cloud.google.com/vpc/docs/shared-vpc#svc_proj_admins
https://cloud.google.com/vpc/docs/shared-vpc#svc_proj_admins

NEW QUESTION: 156
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. 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.
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 Hide Matching Entries.
4.Make sure the resulting list is empty.
C. 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.
D. 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.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 157
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. 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.
B. 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.
C. 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%.
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: B (LEAVE A REPLY)

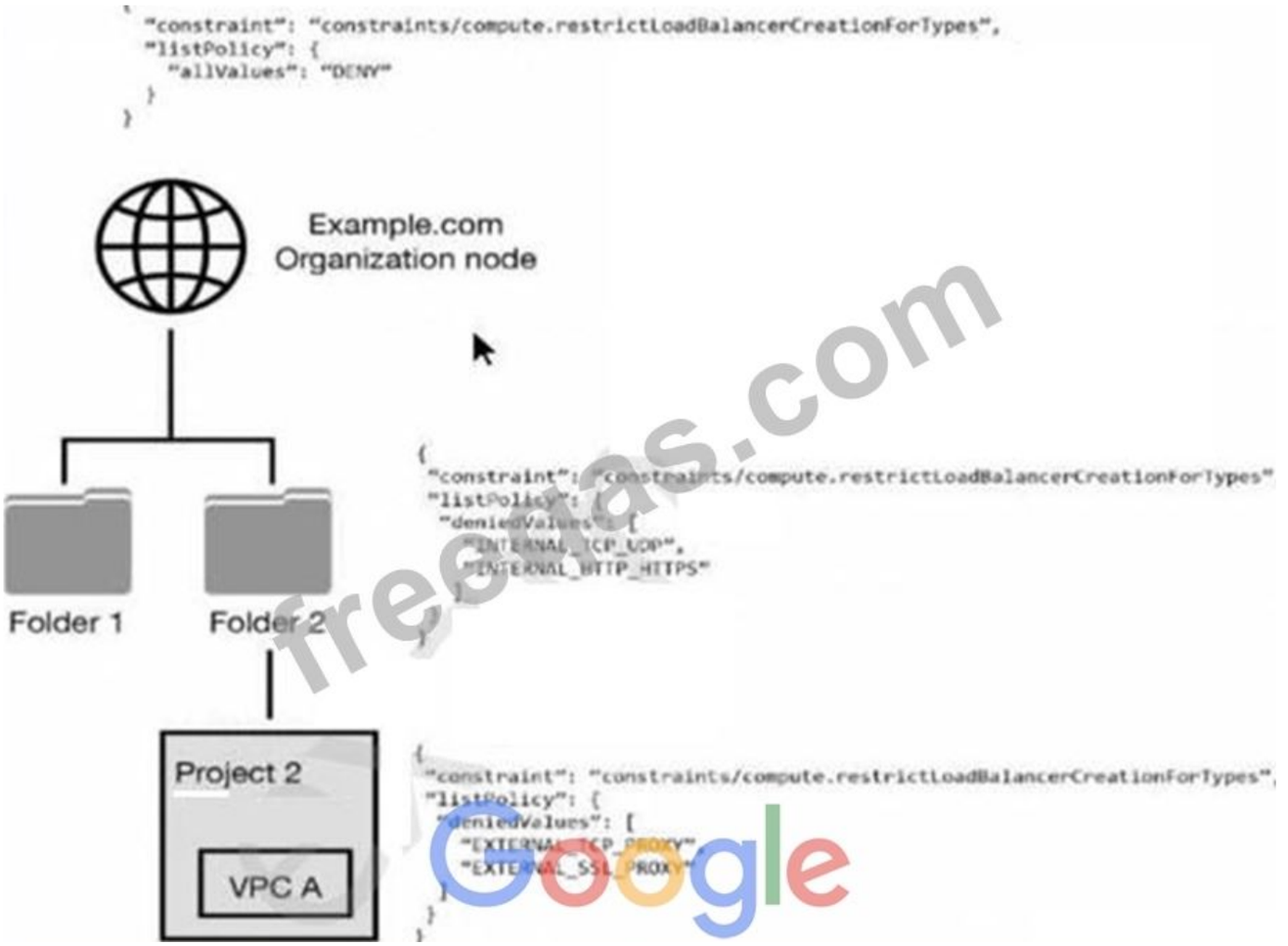
NEW QUESTION: 158
Which international compliance standard provides guidelines for information security controls applicable to the provision and use of cloud services?

A. ISO 27017
B. ISO 27001
C. ISO 27002
D. ISO 27018
Answer: A (LEAVE A REPLY)

NEW QUESTION: 159
Your organization is transitioning to Google Cloud You want to ensure that only trusted container images are deployed on Google Kubernetes Engine (GKE) clusters in a project. The containers must be deployed from a centrally managed. Container Registry and signed by a trusted authority.
What should you do?
Choose 2 answers
A. Configure the trusted image organization policy constraint for the project.
B. Enable Container Threat Detection in the Security Command Center (SCC) for the project.
C. Configure the Binary Authorization policy with respective attestations for the project.
D. Enable Pod Security standards and set them to Restricted.
E. Create a custom organization policy constraint to enforce Binary Authorization for Google Kubernetes Engine (GKE).
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 160
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: B (LEAVE A REPLY)
https://cloud.google.com/kubernetes-engine/docs/security-bulletins

NEW QUESTION: 161
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. EXTERNAL_TCP_PROXY, EXTERNAL_SSL_PROXY are denied in accordance with the project's policy.
C. EXTERNAL_TCP_PROXY, EXTERNAL_SSL_PROXY, INTERNAL_TCP_UDP, and INTERNAL_HTTP_HTTPS are denied in accordance with the folder and project's policies.
D. INTERNAL_TCP_UDP, INTERNAL_HTTP_HTTPS is denied in accordance with the folder's policy.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 162
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 (LEAVE A REPLY)
https://cloud.google.com/vpc/docs/firewalls#service-accounts-vs-tags
https://cloud.google.com/vpc/docs/firewalls#service-accounts-vs-tags
A service account represents an identity associated with an instance. Only one service account can be associated with an instance. You control access to the service account by controlling the grant of the Service Account User role for other IAM principals. For an IAM principal to start an instance by using a service account, that principal must have the Service Account User role to at least use that service account and appropriate permissions to create instances (for example, having the Compute Engine Instance Admin role to the project).

NEW QUESTION: 163
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 (LEAVE A REPLY)
Explanation
Only Forseti security can have both 'past' and 'present' (i.e. historical) records of the resources.https://forsetisecurity.org/about/

NEW QUESTION: 164
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: (SHOW ANSWER)
Explanation

"This encryption method is reversible, which helps to maintain referential integrity across your database and has no character-set limitations."
https://cloud.google.com/blog/products/identity-security/take-charge-of-your-data-how-tokenization-makes-data
https://cloud.google.com/dlp/docs/pseudonymization
FPE provides fewer security guarantees compared to other deterministic encryption methods such as AES-SIV. For these reasons, Google strongly recommends using deterministic encryption with AES-SIV instead of FPE for all security sensitive use cases. Other methods like deterministic encryption using AES-SIV provide these stronger security guarantees and are recommended for tokenization use cases unless length and character set preservation are strict requirements-for example, for backward compatibility with a legacy data system.

NEW QUESTION: 165
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: B (LEAVE A REPLY)
https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains

NEW QUESTION: 166
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 (PII) from files that are older than 12 months. Also you must archive the anonymized files for retention purposes.
What should you do?
A. Configure the Autoclass feature of the Cloud Storage bucket to de-identify PII Archive the files that are older than 12 months Delete the original files.
B. Schedule a Cloud Key Management Service (KMS) rotation period of 12 months for the encryption keys of the Cloud Storage files containing PII to de-identify them Delete the original keys.
C. Create a Cloud Data Loss Prevention (DLP) inspection job that de-identifies PII in files created more than 12 months ago and archives them to another Cloud Storage bucket. Delete the original files.
D. 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.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 167
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 (LEAVE A REPLY)
https://cloud.google.com/vpc-service-controls/docs/dry-run-mode
When using VPC Service Controls, it can be difficult to determine the impact to your environment when a service perimeter is created or modified. With dry run mode, you can better understand the impact of enabling VPC Service Controls and changes to perimeters in existing environments.

NEW QUESTION: 168
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 (LEAVE A REPLY)
De-identifying sensitive data Cloud Data Loss Prevention (DLP) can de-identify sensitive data in text content, including text stored in container structures such as tables. De-identification is the process of removing identifying information from data. The API detects sensitive data such as personally identifiable information (PII), and then uses a de-identification transformation to mask, delete, or otherwise obscure the data. For example,

de-identification techniques can include any of the following: Masking sensitive data by partially or fully replacing characters with a symbol, such as an asterisk (*) or hash (#). Replacing each instance of sensitive data with a token, or surrogate, string. Encrypting and replacing sensitive data using a randomly generated or pre-determined key. When you de-identify data using the CryptoReplaceFfxFpeConfig or CryptoDeterministicConfig infoType transformations, you can re-identify that data, as long as you have the CryptoKey used to originally de-identify the data. https://cloud.google.com/dlp/docs/deidentify-sensitive-data

NEW QUESTION: 169
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: (SHOW ANSWER)
Explanation
B: you need KMS to store the CryptoKeyhttps://cloud.google.com/dlp/docs/reference/rest/v2/projects.deidentifyTemplates#crypt E: for the de-identity you need to use CryptoReplaceFfxFpeConfig or CryptoDeterministicConfighttps://cloud.google.com/dlp/docs/reference/rest/v2/projects.deidentifyTemplates#cry https://cloud.google.com/dlp/docs/deidentify-sensitive-data

NEW QUESTION: 170
You are in charge of migrating a legacy application from your company datacenters to GCP before the current maintenance contract expires. You do not know what ports the application is using and no documentation is available for you to check. You want to complete the migration without putting your environment at risk.
What should you do?
A. Migrate the application into an isolated project using a "Lift & Shift" approach. Enable all internal TCP traffic using VPC Firewall rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.
B. Migrate the application into an isolated project using a "Lift & Shift" approach in a custom network. Disable all traffic within the VPC and look at the Firewall logs to determine what traffic should be allowed for the application to work properly.
C. Refactor the application into a micro-services architecture in a GKE cluster. Disable all traffic from outside the cluster using Firewall Rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.

D. Refactor the application into a micro-services architecture hosted in Cloud Functions in an isolated project.Disable all traffic from outside your project using Firewall Rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.

Answer: A (LEAVE A REPLY)

Migrate the application into an isolated project using a "Lift & Shift" approach. Enable all internal TCP traffic using VPC Firewall rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.

NEW QUESTION: 171

You have numerous private virtual machines on Google Cloud. You occasionally need to manage the servers through Secure Socket Shell (SSH) from a remote location. You want to configure remote access to the servers in a manner that optimizes security and cost efficiency.

What should you do?

A. Create a firewall rule to allow access from the Identity-Aware Proxy (IAP) IP range Grant the role of an IAP-secured Tunnel User to the administrators.

B. Create a jump host instance with public IP Manage the instances by connecting through the jump host.

C. Configure server instances with public IP addresses Create a firewall rule to only allow traffic from your corporate IPs.

D. Create a site-to-site VPN from your corporate network to Google Cloud.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 172

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

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

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

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

Answer: (SHOW ANSWER)

NEW QUESTION: 173

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: C (LEAVE A REPLY)

Explanation

https://cloud.google.com/resource-manager/docs/organization-policy/defining-locations

NEW QUESTION: 174

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 (LEAVE A REPLY)

Secret Manager is a secure and convenient storage system for API keys, passwords, certificates, and other sensitive data. Secret Manager provides a central place and single source of truth to manage, access, and audit secrets across Google Cloud. https://cloud.google.com/secret-manager

NEW QUESTION: 175

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. Enable VPC Flow Logs in your VPC. Use Logs Explorer to analyze whether the rules are working correctly.

C. Connect to a bastion host in your VPC. Use a network traffic analyzer to determine at which point your requests are being blocked.

D. In a pre-production environment, disable all firewall rules individually to determine which one is blocking user traffic.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 176

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 (LEAVE A REPLY)
Explanation
https://cloud.google.com/iam/docs/best-practices-for-managing-service-account-keys
"To prevent unnecessary usage of service account keys, use organization policy constraints: At the root of your organization's resource hierarchy, apply the Disable service account key creation and Disable service account key upload constraints to establish a default where service account keys are disallowed. When needed, override one of the constraints for selected projects to re-enable service account key creation or upload."

NEW QUESTION: 177
Your Security team believes that a former employee of your company gained unauthorized access to Google Cloud resources some time in the past 2 months by using a service account key. You need to confirm the unauthorized access and determine the user activity. What should you do?
A. Use Security Health Analytics to determine user activity.
B. Use the Logs Explorer to search for user activity.
C. Use the Cloud Data Loss Prevention API to query logs in Cloud Storage.
D. Use the Cloud Monitoring console to filter audit logs by user.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 178
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 (LEAVE A REPLY)
https://cloud.google.com/network-intelligence-center/docs/firewall-insights/concepts/overview#shadowed-firewall-rules Firewall Insights analyzes your firewall rules to detect firewall rules that are shadowed by other rules. A shadowed rule is a firewall rule that has all of its relevant attributes, such as its IP address and port ranges, overlapped by attributes from one or more rules with higher or equal priority, called shadowing rules.

NEW QUESTION: 179
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. Create a perimeter bridge between the service project where the Compute Engine instances reside and the perimeter that contains the protected BigQuery datasets.
C. Add the service project where the Compute Engine instances reside to the service perimeter.
D. Create a service perimeter between the service project where the Compute Engine instances reside and the host project that contains the Shared VPC.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 180
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. Private Google Access
B. IP Forwarding
C. Static routes
D. Public IP
E. IAM Network User Role
Answer: (SHOW ANSWER)

NEW QUESTION: 181
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 Cloud Storage bucket, and configure the bucket's Object Lifecycle Management feature.
D. Store the data in a BigQuery table, and set the table's expiration time.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 182

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 (LEAVE A REPLY)
https://cloud.google.com/solutions/best-practices-vpc-design
"Setting up your payment-processing environment" section in https://cloud.google.com/solutions/pci-dss-compliance-in-gcp.

NEW QUESTION: 183
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 (LEAVE A REPLY)
https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains#setting_the_organization_policy The domain restriction constraint is a type of list constraint. Google Workspace customer IDs can be added and removed from the allowed_values list of a domain restriction constraint. The domain restriction constraint does not support denying values, and an organization policy can't be saved with IDs in the denied_values list. All domains associated with a Google Workspace account listed in the allowed_values will be allowed by the organization policy. All other domains will be denied by the organization policy.

NEW QUESTION: 184
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. Create a Cloud Storage sink with a publicly shared Cloud Storage bucket in each project.2. Process Cloud Storage objects in SIEM.
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 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.
D. 1. Export logs in each dev project to a Cloud Pub/Sub topic in a dedicated SIEM project.2. Subscribe SIEM to the topic.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 185
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 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 (LEAVE A REPLY)
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.

NEW QUESTION: 186
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 an external HTTP(S) load balancer in the host (VPC) project with the MIG as a backend.
B. Deploy an external HTTP(S) load balancer in the service project with the MIG as a backend.
C. Deploy a Cloud NAT Gateway in the host (VPC) project for the MIG.
D. Deploy a Cloud NAT Gateway in the service project for the MIG.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 187
An application log's data, including customer identifiers such as email addresses, needs to be redacted. However, these logs also include the email addresses of internal developers from company.com, and these should NOT be redacted. Which solution should you use to meet these requirements?
A. Create a regular custom dictionary detector that lists a subset of the developers' email addresses.
B. Create a regular expression (regex) custom infoType detector to match on @company.com.
C. Create a regular custom dictionary detector to match all email addresses listed in Cloud Identity.
D. Create a custom infoType called COMPANY_EMAIL to match @company.com.
Answer: B (LEAVE A REPLY)
A is not correct because as all company.com email addresses are sensitive and should be filtered, a static list is hard to maintain and can easily miss sensitive data.
B is correct because the regex will detect all company.com email addresses that need to be protected and written to the log file.
C is not correct because as the user base in Cloud Identity might only be a subset of all emails that need to be protected.
D is not correct because you need to specify a detector within the custom infoType and the detector should be a regular expression to match all @company.com email addresses.
https://cloud.google.com/dlp/docs/infotypes-reference
https://cloud.google.com/dlp/docs/creating-custom-infotypes

NEW QUESTION: 188
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: (SHOW ANSWER)
Reference:
https://cloud.google.com/solutions/pci-dss-compliance-in-gcp

NEW QUESTION: 189
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: (SHOW ANSWER)
Explanation
https://codelabs.developers.google.com/codelabs/cloud-storage-dlp-functions#0https://www.youtube.com/watch

NEW QUESTION: 190
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: (SHOW ANSWER)

NEW QUESTION: 191
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 (LEAVE A REPLY)

Provide granular access to secrets: 2.Enforce access control to secrets using project-level identity and Access Management (IAM) bindings. Give you control over the rotation schedules for the encryption keys that wrap your secrets: 3. Use customer-managed encryption keys to encrypt secrets. Maintain environment separation: 1. Use separate Google Cloud projects to store Production and Non-Production secrets.

NEW QUESTION: 192

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 (LEAVE A REPLY)

Explanation
https://cloud.google.com/logging/docs/access-control#considerations roles/logging.privateLogViewer (Private Logs Viewer) includes all the permissions contained by roles/logging.viewer, plus the ability to read Data Access audit logs in the _Default bucket.

NEW QUESTION: 193

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: C,D (LEAVE A REPLY)

Reference:
https://cloud.google.com/vpc/docs/configure-private-google-access

NEW 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 (LEAVE A REPLY)

Explanation

If you want to manage the key encryption keys used for your data at rest, instead of having Google manage the keys, use Cloud Key Management Service to manage your keys. This scenario is known as customer-managed encryption keys (CMEK). https://cloud.google.com/bigquery/docs/encryption-at-rest

NEW QUESTION: 195

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 (LEAVE A REPLY)

Explanation

nodeSelector is the simplest recommended form of node selection constraint. You can add the nodeSelector field to your Pod specification and specify the node labels you wantthe target node to have. Kubernetes only schedules the Pod onto nodes that have each of the labels you specify. => https://kubernetes.io/docs/concepts/scheduling-eviction/assign-pod-node/#nodeselector Tolerations are applied to pods. Tolerations allow the scheduler to schedule pods with matching taints. Tolerations allow scheduling but don't guarantee scheduling: the scheduler also evaluates other parameters as part of its function. =>https://kubernetes.io/docs/concepts/scheduling-eviction/taint-and-toleration/

NEW QUESTION: 196

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: (SHOW ANSWER)

Explanation
https://cloud.google.com/logging/docs/export/troubleshoot#errors_exporting_to_cloud_storage
https://cloud.google.com/logging/docs/export/troubleshoot
Unable to grant correct permissions to the destination: Even if the sink was successfully created with the correct service account permissions, this error message displays if the access control model for the Cloud Storage bucket was set to uniform access when the bucket was created. For existing Cloud Storage buckets, you can change the access control model for the first 90 days after bucket creation by using the Permissions tab. For new buckets, select the Fine-grained access control model during bucket creation. For details, see Creating Cloud Storage buckets.

NEW QUESTION: 197
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 (LEAVE A REPLY)
https://cloud.google.com/identity/solutions/automate-user-provisioning#cloud_identity_automated_provisioning
"Cloud Identity has a catalog of automated provisioning connectors, which act as a bridge between Cloud Identity and third-party cloud apps."

NEW QUESTION: 198
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 LDAP search attributes to exclude manually created Cloud identity users not found in LDAP.
2. Run GCDS after user and group lifecycle changes.

B. 1. Configure the LDAP search attributes to exclude manually created Cloud Identity users not found in LDAP.
2. Set up a recurring GCDS task.

C. 1. Configure the option to delete domain users not found in LDAP.
2. Run GCDS after user and group lifecycle changes.

D. 1. Configure the option to suspend domain users not found in LDAP.
2. Set up a recurring GCDS task.

Answer: (SHOW ANSWER)

NEW QUESTION: 199

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 (LEAVE A REPLY)

Explanation

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

NEW QUESTION: 200

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: (SHOW ANSWER)
https://cloud.google.com/recommender/docs/tutorial-iac

NEW QUESTION: 201
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 (LEAVE A REPLY)
Explanation

NEW QUESTION: 202
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: C (LEAVE A REPLY)
Explanation/Reference: https://cloud.google.com/logging/docs/exclusions

NEW QUESTION: 203
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, 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.
B. 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.
C. 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.
D. 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.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 204
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. Project Creator
B. Billing Account Viewer
C. Organization Administrator
D. Billing Account Costs Manager
E. Billing Account User
Answer: (SHOW ANSWER)

NEW QUESTION: 205
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 dat a. 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 (LEAVE A REPLY)
There is mention about simulating in Web Security Scanner. "Web Security Scanner cross-site scripting (XSS) injection testing *simulates* an injection attack by inserting a benign test string into user-editable fields and then performing various user actions." https://cloud.google.com/security-command-center/docs/how-to-remediate-web-security-scanner-findings#xss

NEW QUESTION: 206
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: C (LEAVE A REPLY)
Explanation/Reference: https://cloud.google.com/solutions/pci-dss-compliance-in-gcp

NEW QUESTION: 207
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. Users sign in using OpenID (OIDC) compatible IdP, receive an authentication token, then use that token to log in to the GCP Console.
B. Manually synchronize the data in Google domain with your existing Active Directory or LDAP server.
C. Use Google Cloud Directory Sync to synchronize the data in Google domain with your existing Active Directory or LDAP server.
D. Users sign in directly to the GCP Console using the credentials from your on-premises Kerberos compliant identity provider.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 208
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. Compute Engine custom metadata
B. Compute Engine guest attributes
C. Cloud Key Management Service
D. Secret Manager
Answer: C (LEAVE A REPLY)

NEW QUESTION: 209
You are deploying regulated workloads on Google Cloud. The regulation has data residency and data access requirements. It also requires that support is provided from the same geographical location as where the data resides.
What should you do?
A. Enable Access Transparency Logging.
B. Deploy resources only to regions permitted by data residency requirements

C. Use Data Access logging and Access Transparency logging to confirm that no users are accessing data from another region.
D. Deploy Assured Workloads.
Answer: (SHOW ANSWER)
Explanation
Assured Workloads for Google Cloud allows you to deploy regulated workloads with data residency, access, and support requirements. It helps you configure your environment in a manner that aligns with specific compliance frameworks and standards.

NEW QUESTION: 210
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 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.
C. 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.
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: (SHOW ANSWER)

NEW QUESTION: 211
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 (LEAVE A REPLY)
Reference:
Use Shared VPC to connect to a common VPC network. Resources in those projects can communicate with each other securely and efficiently across project boundaries using internal IPs. You can manage shared network resources, such as subnets, routes, and firewalls, from a central host project, enabling you to apply and enforce consistent network policies across the projects.

NEW QUESTION: 212
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 (LEAVE A REPLY)
Reference:
https://cloud.google.com/kubernetes-engine/docs/how-to/dynamic-provisioning-cmek

NEW QUESTION: 213
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 (LEAVE A REPLY)
Explanation
https://cloud.google.com/vpc-service-controls/docs/dry-run-mode
When using VPC Service Controls, it can be difficult to determine the impact to your environment when a service perimeter is created or modified. With dry run mode, you can better understand the impact of enabling VPC Service Controls and changes to perimeters in existing environments.

NEW QUESTION: 214
An administrative application is running on a virtual machine (VM) in a managed group at port 5601 inside a Virtual Private Cloud (VPC) instance without access to the internet currently. You want to expose the web interface at port 5601 to users and enforce authentication and authorization Google credentials What should you do?
A. Modify the VPC routing with the default route point to the default internet gateway Modify the VPC Firewall rule to allow access from the internet 0.0.0.0/0 to port 5601 on the application instance.
B. Configure the bastion host with OS Login enabled and allow connection to port 5601 at VPC firewall Log in to the bastion host from the Google Cloud console by using SSH-in-browser and then to the web application
C. Configure an HTTP Load Balancing instance that points to the managed group with Identity-Aware Proxy (IAP) protection with Google credentials Modify the VPC firewall to allow access from IAP network range
D. Configure Secure Shell Access (SSH) bastion host in a public network, and allow only the bastion host to connect to the application on port 5601. Use a bastion host as a jump host to connect to the application
Answer: C (LEAVE A REPLY)
Explanation
This approach allows you to expose the web interface securely by using Identity-Aware Proxy (IAP), which provides authentication and authorization with Google credentials. The HTTP Load Balancer can distribute traffic to the VMs in the managed group, and the VPC firewall rule ensures that access is allowed from the IAP network range.

NEW QUESTION: 215
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.disableServiceAccountKeyUpload boolean to disable the creation of new service accounts.
C. Use organization policy constraints/iam.disableServiceAccountKeyCreation 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 (LEAVE A REPLY)

NEW QUESTION: 216
Your team creates an ingress firewall rule to allow SSH access from their corporate IP range to a specific bastion host on Compute Engine. Your team wants to make sure that this firewall rule cannot be used by unauthorized engineers who may otherwise have access to manage VMs in the development environment. What should your team do to meet this requirement?
A. Create the firewall rule with a target of a network tag. Centrally manage access to the tag.
B. Create the firewall rule with a target of a service account. Centrally manage access to the service account.

C. Create the firewall rule in a Shared VPC with a target of a network tag.
D. Create the firewall rule in a Shared VPC with a target of a specific subnet.
Answer: B (LEAVE A REPLY)
A is not correct because the network tag value can be inferred by examining the Firewall Rule or VM metadata.
B is correct because access to the Service Account is required to use a firewall rule with a target of a Service Account.
C is not correct because the target network tag value can be inferred by examining the Firewall Rule or VM metadata.
D is not correct because the target subnet value can be inferred by examining the Firewall Rule or VM metadata.
https://cloud.google.com/vpc/docs/firewalls#service-accounts-vs-tags

NEW QUESTION: 217
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. Google Kubernetes Engine
C. Cloud Functions
D. Compute Engine
E. Cloud Storage
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 218
When creating a secure container image, which two items should you incorporate into the build if possible? (Choose two.)
A. Package a single app as a container.
B. Use public container images as a base image for the app.
C. Use many container image layers to hide sensitive information.
D. Remove any unnecessary tools not needed by the app.
E. Ensure that the app does not run as PID 1.
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 219
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: (SHOW ANSWER)

NEW QUESTION: 220
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 (LEAVE A REPLY)
Explanation
https://cloud.google.com/storage/docs/uniform-bucket-level-access#enabled

NEW QUESTION: 221
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 (LEAVE A REPLY)
Explanation
This is a Customer-supplied encryption keys (CSEK). We generate our own encryption key and manage it on-premises. A KEK never leaves Cloud KMS.There is no KEK or KMS on-premises. Encryption at rest by default, with various key management options https://cloud.google.com/security/encryption-at-rest

NEW QUESTION: 222
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 (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: (SHOW ANSWER)
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.

NEW QUESTION: 223
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. 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.
B. 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.
C. 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.
D. 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.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 224
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 (LEAVE A REPLY)
https://cloud.google.com/containers/security
Containers are meant to be immutable, so you deploy a new image in order to make changes. You can simplify patch management by rebuilding your images regularly, so the patch is picked up the next time a container is deployed. Get the full picture of your environment with regular image security reviews.

NEW QUESTION: 225
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 (LEAVE A REPLY)

NEW QUESTION: 226
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 (LEAVE A REPLY)
https://cloud.google.com/bigquery/docs/locations

NEW QUESTION: 227
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 (LEAVE A REPLY)
https://cloud.google.com/vpc/docs/packet-mirroring#enterprise_security
Security and network engineering teams must ensure that they are catching all anomalies and threats that might indicate security breaches and intrusions. They mirror all traffic so that they can complete a comprehensive inspection of suspicious flows.

NEW QUESTION: 228
You are working with a client that is concerned about control of their encryption keys for sensitive dat a. 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. Cloud External Key Manager

C. Google default encryption

D. Secret Manager

E. Customer-managed encryption keys

Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 229

Which encryption algorithm is used with Default Encryption in Cloud Storage?

A. AES-256

B. SHA512

C. MD5

D. 3DES

Answer: A (LEAVE A REPLY)

A is correct because Cloud Storage encrypts user data at rest using AES-256.

B is not correct because Cloud Storage encrypts user data at rest using AES-256.

C is not correct because Cloud Storage encrypts user data at rest using AES-256.

D is not correct because Cloud Storage encrypts user data at rest using AES-256.

https://cloud.google.com/storage/docs/encryption/default-keys

NEW QUESTION: 230

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: (SHOW ANSWER)

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

NEW QUESTION: 231
Your application is deployed as a highly available cross-region solution behind a global external HTTP(S) load balancer. You notice significant spikes in traffic from multiple IP addresses but it is unknown whether the IPs are malicious. You are concerned about your application's availability. You want to limit traffic from these clients over a specified time interval.
What should you do?
A. Configure a firewall rule in your VPC to throttle traffic from the identified IP addresses.
B. Configure a rate_based_ban action by using Google Cloud Armor and set the ban_duration_sec parameter to the specified time interval.
C. Configure a throttle action by using Google Cloud Armor to limit the number of requests per client over a specified time interval.
D. Configure a deny action by using Google Cloud Armor to deny the clients that issued too many requests over the specified time interval.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 232
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 (LEAVE A REPLY)
Explanation
https://cloud.google.com/load-balancing/docs/tcp
TCP Proxy Load Balancing is implemented on GFEs that are distributed globally. If you choose the Premium Tier of Network Service Tiers, a TCP proxy load balancer is global. In Premium Tier, you can deploy backends in multiple regions, and the load balancer automatically directs user traffic to the closest region that has capacity. If you choose the Standard Tier, a TCP proxy load balancer can only direct traffic among backends in a single region.https://cloud.google.com/load-balancing/docs/load-balancing-overview#tcp-proxy-load-balancing

NEW QUESTION: 233
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: (SHOW ANSWER)
https://cloud.google.com/blog/products/gcp/dnssec-now-available-in-cloud-dns

NEW QUESTION: 234
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 dat a. 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 (LEAVE A REPLY)
Reference:
https://cloud.google.com/security-scanner/docs/remediate-findings

NEW QUESTION: 235
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 a custom role with the permission compute.instances.list and grant the Service Account this role.
B. Give the Service Account the role of Compute Viewer, and use the new Service Account for all instances.
C. Give the Service Account the role of Project Viewer, and use the new Service Account for all instances.
D. Create an Instance Template, and allow the Service Account Read Only access for the Compute Engine Access Scope.
Answer: (SHOW ANSWER)

NEW QUESTION: 236
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: A,C (LEAVE A REPLY)
Explanation
A) IPsec VPN tunels: https://cloud.google.com/network-connectivity/docs/vpn/concepts/overview Interconnect https://cloud.google.com/network-connectivity/docs/interconnect/concepts/dedicated-overview

NEW QUESTION: 237
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: (SHOW ANSWER)
https://codelabs.developers.google.com/codelabs/cloud-storage-dlp-functions#0
https://www.youtube.com/watch?v=0TmO1f-Ox40

NEW QUESTION: 238
Your organization is rolling out a new continuous integration and delivery (CI/CD) process to deploy infrastructure and applications in Google Cloud Many teams will use their own instances of the CI/CD workflow It will run on Google Kubernetes Engine (GKE) The CI/CD pipelines must be designed to securely access Google Cloud APIs What should you do?
A. *1 Create two service accounts one for the infrastructure and one for the application deployment
*2 Use workload identities to let the pods run the two pipelines and authenticate with the service accounts
*3 Run the infrastructure and application pipelines in separate namespaces
B. *1 Create a dedicated service account for the CI/CD pipelines
*2 Run the deployment pipelines in a dedicated nodes pool in the GKE cluster

*3 Use the service account that you created as identity for the nodes in the pool to authenticate to the Google Cloud APIs
C. * 1 Create individual service accounts (or each deployment pipeline
*2 Add an identifier for the pipeline in the service account naming convention
*3 Ensure each pipeline runs on dedicated pods
*4 Use workload identity to map a deployment pipeline pod with a service account
D. *1 Create service accounts for each deployment pipeline
*2 Generate private keys for the service accounts
*3 Securely store the private keys as Kubernetes secrets accessible only by the pods that run the specific deploy pipeline
Answer: (SHOW ANSWER)

NEW QUESTION: 239
An organization receives an increasing number of phishing emails.
Which method should be used to protect employee credentials in this situation?
A. Captcha on login pages
B. A strict password policy
C. Encrypted emails
D. Multifactor Authentication
Answer: C (LEAVE A REPLY)

NEW QUESTION: 240
You need to implement an encryption-at-rest strategy that protects sensitive data and reduces key management complexity for non-sensitive dat a. 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 (LEAVE A REPLY)
Google uses a common cryptographic library, Tink, which incorporates our FIPS 140-2 Level 1 validated module, BoringCrypto, to implement encryption consistently across almost all Google Cloud products. To provideflexibility of controlling the key residency and rotation schedule, use google provided key for non-sensitive and encrypt sensitive data with Cloud Key Management Service

NEW QUESTION: 241

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 (LEAVE A REPLY)
Reference:
https://cloud.google.com/compute/docs/ip-addresses/reserve-static-external-ip-address

NEW QUESTION: 242
Your organization is using Active Directory and wants to configure Security Assertion Markup Language (SAML). You must set up and enforce single sign-on (SSO) for all users.
What should you do?
A. 1. Manage SAML profile assignments.
* 2. Enable OpenID Connect (OIDC) in your Active Directory (AD) tenant.
* 3. Verify the domain.
B. 1. Create a new SAML profile.
* 2. Upload the X.509 certificate.
* 3. Enable the change password URL.
* 4. Configure Entity ID and ACS URL in your IdP.
C. 1- Create a new SAML profile.
* 2. Populate the sign-in and sign-out page URLs.
* 3. Upload the X.509 certificate.
* 4. Configure Entity ID and ACS URL in your IdP
D. 1. Configure prerequisites for OpenID Connect (OIDC) in your Active Directory (AD) tenant
* 2. Verify the AD domain.
* 3. Decide which users should use SAML.
* 4. Assign the pre-configured profile to the select organizational units (OUs) and groups.

Answer: C (LEAVE A REPLY)
When configuring SAML-based Single Sign-On (SSO) in an organization that's using Active Directory, the general steps would involve setting up a SAML profile, specifying the necessary URLs for sign-in and sign-out processes, uploading an X.509 certificate for secure communication, and setting up the Entity ID and Assertion Consumer Service (ACS) URL in the Identity Provider (which in this case would be Active Directory).

NEW QUESTION: 243
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. Create a new key, and use the new key in the application. Store the old key on the system as a backup key.
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. Open Cloud Shell and run gcloud iam service-accounts enable-auto-rotate --iam-account=IAM_ACCOUNT.
Answer: (SHOW ANSWER)

NEW QUESTION: 244
A security team at an e-commerce company wants to define an automatic incident response process for fraudulent credit card usage attempts. The team targets a 10-minute or faster response time for such incidents. The fraudulent card list is updated every 60 seconds. The e- commerce servers log the transaction details in near-real time. Which option should you recommend to the security team?
A. Define a log-based metric for each fraudulent credit card, and set a Stackdriver alert for these metrics.
B. Maintain a log ingestion exclusion filter based on the fraudulent credit card lists.
C. Use AutoML to automatically build models based on the fraudulent credit card lists.
D. Create a new logging export with a filter to match the transaction and a sink pointing to a Cloud Pub/Sub topic.
Answer: D (LEAVE A REPLY)
A is not correct because creating a metric for every credit card will not scale well.
B is not correct because it will exclude the transactions that are relevant to the security team.
C is not correct because while we could use AutoML to build models, this solution is incomplete without deploying and running the model, as well as wiring them up with some consumer service.
D is correct because this will capture the important events and pass them to Pub/Sub which in turn can send the message to a consumer service like a chat notification webhook.
https://cloud.google.com/logging/docs/export/configure_export_v2

NEW QUESTION: 245
Your organization wants to be compliant with the General Data Protection Regulation (GDPR) on Google Cloud You must implement data residency and operational sovereignty in the EU.
What should you do?
Choose 2 answers

A. Limit the physical location of a new resource with the Organization Policy Service resource locations constraint."
B. Use Cloud IDS to get east-west and north-south traffic visibility in the EU to monitor intra-VPC and mter-VPC communication.
C. Limit Google personnel access based on predefined attributes such as their citizenship or geographic location by using Key Access Justifications
D. Use identity federation to limit access to Google Cloud resources from non-EU entities.
E. Use VPC Flow Logs to monitor intra-VPC and inter-VPC traffic in the EU.
Answer: A,C (LEAVE A REPLY)
Explanation
https://cloud.google.com/architecture/framework/security/data-residency-sovereignty#manage_your_operational

NEW QUESTION: 246
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 (LEAVE A REPLY)
Explanation
"To support common use cases like setting a Time to Live (TTL) for objects, retaining noncurrent versions of objects, or "downgrading" storage classes of objects to help manage costs, Cloud Storage offers the Object Lifecycle Management feature. This page describes the feature as well as the options available when using it. To learn how to enable Object Lifecycle Management, and for examples of lifecycle policies, see Managing Lifecycles." https://cloud.google.com/storage/docs/lifecycle

NEW QUESTION: 247
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 (LEAVE A REPLY)

Explanation
https://cloud.google.com/iam/docs/reference/rest/v1/projects.serviceAccounts/undelete

NEW QUESTION: 248
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 OS Login with 2-step verification for the bastion host.
B. Implement Cloud VPN for the region where the bastion host lives.
C. Implement Identity-Aware Proxy TCP forwarding for the bastion host.
D. Implement Google Cloud Armor in front of the bastion host.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 249
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 (LEAVE A REPLY)
https://cloud.google.com/kms/docs/using-other-products#cmek_integrations
https://cloud.google.com/kms/docs/using-other-products#cmek_integrations CMEK is supported for all the listed google services.

NEW QUESTION: 250
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: (SHOW ANSWER)
Explanation/Reference: https://cloud.google.com/blog/products/gcp/dnssec-now-available-in-cloud-dns

NEW QUESTION: 251

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 (LEAVE A REPLY)
Explanation
https://cloud.google.com/policy-intelligence/docs/policy-analyzer-overview Policy Analyzer lets you find out which principals (for example, users, service accounts, groups, and domains) have what access to which Google Cloud resources based on your IAM allow policies.

NEW QUESTION: 252
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: (SHOW ANSWER)
Default password length is 8 characters. https://support.google.com/cloudidentity/answer/33319?hl=en https://support.google.com/cloudidentity/answer/139399?hl=en#:~:text=It%20can%20be%20between%208,decide%20to%20change%20their%20password.