CertyIQ

CertyIQ

Premium exam material

Get certification quickly with the CertyIQ Premium exam material.
Everything you need to prepare, learn & pass your certification exam easily. Lifetime free updates
First attempt guaranteed success.

https://www.CertyIQ.com

About CertyIQ

We here at CertyIQ eventually got enough of the industry's greedy exam paid for. Our team of IT professionals comes with years of experience in the IT industry Prior to training CertIQ we worked in test areas where we observed the horrors of the paywall exam preparation system.

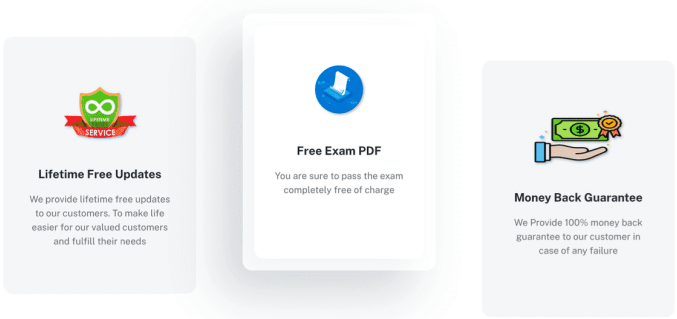
The misuse of the preparation system has left our team disillusioned. And for that reason, we decided it was time to make a difference. We had to make In this way, CertyIQ was created to provide quality materials without stealing from everyday people who are trying to make a living.

Doubt Support

We have developed a very scalable solution using which we are able to solve 400+ doubts every single day with an average rating of 4.8 out of 5.

https://www.certyiq.com

Mail us on - certyiqofficial@gmail.com



John

October 19, 2022

★★★★★

Thanks you so much for your help. I scored 972 in my exam today. More than 90% were from your PDFs!

Dana

September 04, 2022

★★★★★

Thanks a lot for this updated AZ-900 Q&A. I just passed my exam and got 974, I followed both of your Az-900 videos and the 6 PDF, the PDFs are very much valid, all answers are correct. Could you please create a similar video/PDF for DP900, your content/PDF's is really awesome. The team did a really good job. Thank You 😊.

Ahamed Shibly

2 months ago

★★★★★

Customer support is realy fast and helpful, I just finished my exam and this video along with the 6 PDF helped me pass! Definitely recommend getting the PDFs. Thank you!

October 22, 2022

★★★★★

Passed my exam today with 891 marks. Out of 52 questions, 51 were from certyiq PDFs including Contoso case study.
Thank You certyiq team!

Henry Rome

2 months ago

★★★★★

These questions are real and 100 % valid. Thank you so much for your efforts, also your 4 PDFs are awesome, I passed the DP900 exam on 1 Sept. With 968 marks. Thanks a lot, buddy!

Esmaria

2 months ago

★★★★★

Simple easy to understand explanations. To anyone out there wanting to write AZ900, I highly recommend 6 PDF's.Thank you so much, appreciate all your hard work in having such great content. Passed my exam Today - 3 September with 942 score.

Google

(Professional Cloud Security Engineer)

Professional Cloud Security Engineer

Total: **249 Questions**

Link: https://certyiq.com/papers?provider=google&exam=professional-cloud-security-engineer

Question: 1 CertyIQ

Your team needs to make sure that a Compute Engine instance does not have access to the internet or to any Google APIs or services.
Which two settings must remain disabled to meet these requirements? (Choose two.)

A. Public IP
B. IP Forwarding
C. Private Google Access
D. Static routes
E. IAM Network User Role

Answer: AC

Explanation:

Public IP

Private Google Access

Reference:

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

Question: 2 CertyIQ

Which two implied firewall rules are defined on a VPC network? (Choose two.)

A. A rule that allows all outbound connections
B. A rule that denies all inbound connections
C. A rule that blocks all inbound port 25 connections
D. A rule that blocks all outbound connections
E. A rule that allows all inbound port 80 connections

Answer: AB

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.

Reference:

https://cloud.google.com/vpc/docs/firewalls

Question: 3 CertyIQ

A customer needs an alternative to storing their plain text secrets in their source-code management (SCM) system.
How should the customer achieve this using Google Cloud Platform?

A. Use Cloud Source Repositories, and store secrets in Cloud SQL.

B. Encrypt the secrets with a Customer-Managed Encryption Key (CMEK), and store them in Cloud Storage.

C. Run the Cloud Data Loss Prevention API to scan the secrets, and store them in Cloud SQL.

D. Deploy the SCM to a Compute Engine VM with local SSDs, and enable preemptible VMs.

Answer: B

Explanation:

B. Encrypt the secrets with a Customer-Managed Encryption Key (CMEK), and store them in Cloud Storage.

Question: 4 CertyIQ

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

Explanation:

The question clearly states that, centrally manage. So, Cloud Sync is correct one.

Question: 5 CertyIQ

When creating a secure container image, which two items should you incorporate into the build if possible? (Choose two.)

A. Ensure that the app does not run as PID 1.

B. Package a single app as a container.

C. Remove any unnecessary tools not needed by the app.

D. Use public container images as a base image for the app.

E. Use many container image layers to hide sensitive information.

Answer: BC

Explanation:

Reference:
https://cloud.google.com/solutions/best-practices-for-building-containers

Question: 6 CertyIQ

A customer needs to launch a 3-tier internal web application on Google Cloud Platform (GCP). The customer's

internal compliance requirements dictate that end- user access may only be allowed if the traffic seems to originate from a specific known good CIDR. The customer accepts the risk that their application will only have SYN flood DDoS protection. They want to use GCP's native SYN flood protection.
Which product should be used to meet these requirements?

A. Cloud Armor
B. VPC Firewall Rules
C. Cloud Identity and Access Management
D. Cloud CDN

Answer: A

Explanation:

If there were at least a L4 load balancer in the picture, I'd vote for B, since then the LB would take care of "GCP's native SYN flood protection", also considering that "The customer accepts the risk that their application will only have SYN flood DDoS protection.".

With cloud armor I guess they get more protection that required on the question, but it seems to be the only entry that fulfills the requirements

Reference:

https://cloud.google.com/blog/products/identity-security/understanding-google-cloud-armors-new-waf-capabilities

Question: 7 CertyIQ

A company is running workloads in a dedicated server room. They must only be accessed from within the private company network. You need to connect to these workloads from Compute Engine instances within a Google Cloud Platform project.
Which two approaches can you take to meet the requirements? (Choose two.)

A. Configure the project with Cloud VPN.
B. Configure the project with Shared VPC.
C. Configure the project with Cloud Interconnect.
D. Configure the project with VPC peering.
E. Configure all Compute Engine instances with Private Access.

Answer: AC

Explanation:

A) IPsec VPN tunels: https://cloud.google.com/network-connectivity/docs/vpn/concepts/overview

C) Interconnect

https://cloud.google.com/network-connectivity/docs/interconnect/concepts/dedicated-overview

Question: 8 CertyIQ

A customer implements Cloud Identity-Aware Proxy for their ERP system hosted on Compute Engine. Their security team wants to add a security layer so that the
ERP systems only accept traffic from Cloud Identity-Aware Proxy.

What should the customer do to meet these requirements?

A. Make sure that the ERP system can validate the JWT assertion in the HTTP requests.
B. Make sure that the ERP system can validate the identity headers in the HTTP requests.
C. Make sure that the ERP system can validate the x-forwarded-for headers in the HTTP requests.
D. Make sure that the ERP system can validate the user's unique identifier headers in the HTTP requests.

Answer: A

Explanation:

Use Cryptographic Verification

If there is a risk of IAP being turned off or bypassed, your app can check to make sure the identity information it receives is valid. This uses a third web request header added by IAP, called X-Goog-IAP-JWT-Assertion. The value of the header is a cryptographically signed object that also contains the user identity data. Your application can verify the digital signature and use the data provided in this object to be certain that it was provided by IAP without alteration.

So answer is A

Question: 9 CertyIQ

A company has been running their application on Compute Engine. A bug in the application allowed a malicious user to repeatedly execute a script that results in the Compute Engine instance crashing. Although the bug has been fixed, you want to get notified in case this hack re-occurs.
What should you do?

A. Create an Alerting Policy in Stackdriver using a Process Health condition, checking that the number of executions of the script remains below the desired threshold. Enable notifications.
B. Create an Alerting Policy in Stackdriver using the CPU usage metric. Set the threshold to 80% to be notified when the CPU usage goes above this 80%.
C. Log every execution of the script to Stackdriver Logging. Create a User-defined metric in Stackdriver Logging on the logs, and create a Stackdriver Dashboard displaying the metric.
D. Log every execution of the script to Stackdriver Logging. Configure BigQuery as a log sink, and create a BigQuery scheduled query to count the number of executions in a specific timeframe.

Answer: A

Explanation:

Other options won't provide any notification to the user. So, the correct answer is A.

Question: 10 CertyIQ

Your team needs to obtain a unified log view of all development cloud projects in your SIEM. The development projects are under the NONPROD organization folder with the test and pre-production projects. The development projects share the ABC-BILLING billing account with the rest of the organization.
Which logging export strategy should you use to meet the requirements?

A. 1. Export logs to a Cloud Pub/Sub topic with folders/NONPROD parent and includeChildren property set to True in a dedicated SIEM project. 2. Subscribe SIEM to the topic.
B. 1. Create a Cloud Storage sink with billingAccounts/ABC-BILLING parent and includeChildren property set to False in a dedicated SIEM project. 2. Process Cloud Storage objects in SIEM.

C. 1. Export logs in each dev project to a Cloud Pub/Sub topic in a dedicated SIEM project. 2. Subscribe SIEM to the topic.

D. 1. Create a Cloud Storage sink with a publicly shared Cloud Storage bucket in each project. 2. Process Cloud Storage objects in SIEM.

Answer: C

Explanation:

"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.

The only option that filters the log is C - so the answer must be C.

Question: 11 CertyIQ

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

Explanation:

Correct Answer is (C):

DNSSEC — use a DNS registrar that supports DNSSEC, and enable it. DNSSEC digitally signs DNS communication, making it more difficult (but not impossible) for hackers to intercept and spoof.

Domain Name System Security Extensions (DNSSEC) adds security to the Domain Name System (DNS) protocol by enabling DNS responses to be validated. Having a trustworthy Domain Name System (DNS) that translates a domain name like www.example.com into its associated IP address is an increasingly important building block of today's web-based applications. Attackers can hijack this process of domain/IP lookup and redirect users to a malicious site through DNS hijacking and man-in-the-middle attacks. DNSSEC helps mitigate the risk of such attacks by cryptographically signing DNS records. As a result, it prevents attackers from issuing fake DNS responses that may misdirect browsers to nefarious websites.

Reference:

https://cloud.google.com/blog/products/gcp/dnssec-now-available-in-cloud-dns

Question: 12 CertyIQ

A customer deploys an application to App Engine and needs to check for Open Web Application Security Project (OWASP) vulnerabilities.
Which service should be used to accomplish this?

A. Cloud Armor

B. Google Cloud Audit Logs

C. Web Security Scanner

D. Anomaly Detection

Answer: C

Explanation:

Answer is (C).

Web Security Scanner supports categories in the OWASP Top Ten, a document that ranks and provides remediation guidance for the top 10 most critical web application security risks, as determined by the Open Web Application Security Project (OWASP).

Reference:

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

Question: 13 CertyIQ

A customer's data science group wants to use Google Cloud Platform (GCP) for their analytics workloads. Company policy dictates that all data must be company-owned and all user authentications must go through their own Security Assertion Markup Language (SAML) 2.0 Identity Provider (IdP). The
Infrastructure Operations Systems Engineer was trying to set up Cloud Identity for the customer and realized that their domain was already being used by G Suite.
How should you best advise the Systems Engineer to proceed with the least disruption?

A. Contact Google Support and initiate the Domain Contestation Process to use the domain name in your new Cloud Identity domain.

B. Register a new domain name, and use that for the new Cloud Identity domain.

C. Ask Google to provision the data science manager's account as a Super Administrator in the existing domain.

D. Ask customer's management to discover any other uses of Google managed services, and work with the existing Super Administrator.

Answer: D

Explanation:

Answer is D - there is no evidence that the account is lost, or similar. In a large corp it is very possible that someone (the IT org) has registered with google, and the Data science Department simply haven't been given access to it yet.

Question: 14 CertyIQ

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: A

Explanation:

Answer A > Its the only one that allow you to manage permissions on the projects

answer B > dont have any iam set permission so is not correct

C > organizationRoleAdmin let you only create custom roles, you cant assign it to anyone (so with thisone you cant manage permissions just create roles)

D> org policyes are for manage the ORG policies constrains , that is not about project permissions,

for me the correct is A

Question: 15 CertyIQ

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

Explanation:

The Answer is C

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

Question: 16 CertyIQ

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

Explanation:

Its B.

They are asking for advise for Developers. (IaC is the suitable as they don't have to worry about managing infrastructure manually).

Moreover "An organization's typical network and security review consists of analyzing application transit routes, request handling, and firewall rules." statement is defining the process, they are not asking about the option to review the rules. Using Forseti is not reducing the overhead for Developers.

Question: 17 CertyIQ

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

Explanation:

D is the only option that is reversible.

D. CryptoReplaceFfxFpeConfig is the correct answer for sure, it allows you to recover the original data.

Question: 18 CertyIQ

An organization adopts Google Cloud Platform (GCP) for application hosting services and needs guidance on setting up password requirements for their Cloud
Identity account. The organization has a password policy requirement that corporate employee passwords must have a minimum number of characters.
Which Cloud Identity password guidelines can the organization use to inform their new requirements?

A. Set the minimum length for passwords to be 8 characters.

B. Set the minimum length for passwords to be 10 characters.

C. Set the minimum length for passwords to be 12 characters.

D. Set the minimum length for passwords to be 6 characters.

Answer: A

Explanation:

Answer A

For Cloud Identity password requirements still is - Minimum 8 Maximum is 100

https://support.google.com/cloudidentity/answer/139399?hl=en#:~:text=It%20can%20be%20between%208,decide%20to%20change%20their%20password.

Question: 19 CertyIQ

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

Explanation:

A is correct

The process of encrypting data is to generate a DEK locally, encrypt data with the DEK, use a KEK to wrap the DEK, and then store the encrypted data and the wrapped DEK. The KEK never leaves Cloud KMS.

Reference:

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

Question: 20 CertyIQ

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

Explanation:

Correct answer is C

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

Question: 21 CertyIQ

In order to meet PCI DSS requirements, a customer wants to ensure that all outbound traffic is authorized.
Which two cloud offerings meet this requirement without additional compensating controls? (Choose two.)

A. App Engine
B. Cloud Functions
C. Compute Engine
D. Google Kubernetes Engine
E. Cloud Storage

Answer: CD

Explanation:

Answer is CD

because the doc mentions the following: "App Engine ingress firewall rules are available, but egress rules are not currently available:" and "Compute Engine and GKE are the preferred alternatives."

Question: 22 CertyIQ

A website design company recently migrated all customer sites to App Engine. Some sites are still in progress and should only be visible to customers and company employees from any location.
Which solution will restrict access to the in-progress sites?

A. Upload an .htaccess file containing the customer and employee user accounts to App Engine.
B. Create an App Engine firewall rule that allows access from the customer and employee networks and denies all other traffic.
C. Enable Cloud Identity-Aware Proxy (IAP), and allow access to a Google Group that contains the customer and employee user accounts.
D. Use Cloud VPN to create a VPN connection between the relevant on-premises networks and the company's GCP Virtual Private Cloud (VPC) network.

Answer: C

Explanation:

C https://cloud.google.com/iap/docs/concepts-overview#when_to_use_iap

Question: 23 CertyIQ

When working with agents in a support center via online chat, an organization's customers often share pictures of their documents with personally identifiable information (PII). The organization that owns the support center is concerned that the PII is being stored in their databases as part of the regular chat logs they retain for review by internal or external analysts for customer service trend analysis.
Which Google Cloud solution should the organization use to help resolve this concern for the customer while still maintaining data utility?

A. Use Cloud Key Management Service (KMS) to encrypt the PII data shared by customers before storing it for analysis.

B. Use Object Lifecycle Management to make sure that all chat records with PII in them are discarded and not saved for analysis.

C. Use the image inspection and redaction actions of the DLP API to redact PII from the images before storing them for analysis.

D. Use the generalization and bucketing actions of the DLP API solution to redact PII from the texts before storing them for analysis.

Answer: C

Explanation:

C. Use the image inspection and redaction actions of the DLP API to redact PII from the images before storing them for analysis.

https://cloud.google.com/dlp/docs/concepts-image-redaction

Question: 24 CertyIQ

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

Explanation:

C is correct. As explained, 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.

Reference:

https://cloud.google.com/iam/docs/understanding-service-accounts

Question: 25 CertyIQ

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

Explanation:

A Centralize network control:

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.

Reference:

https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations#centralize_network_control

Question: 26 CertyIQ

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

Explanation:

Correct Answer is C

GSuite is Saas application.

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.

Question: 27 CertyIQ

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

A. Create an organization node, and assign folders for each business unit.

B. Establish standalone projects for each business unit, using gmail.com accounts.

C. Assign GCP resources in a project, with a label identifying which business unit owns the resource.

D. Assign GCP resources in a VPC for each business unit to separate network access.

Answer: A

Explanation:

A https://cloud.google.com/resource-manager/docs/listing-all-resources

Also: https://wideops.com/mapping-your-organization-with-the-google-cloud-platform-resource-hierarchy/

Question: 28 CertyIQ

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

Explanation:

Corrrect Answer is (A):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

Question: 29 CertyIQ

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

Explanation:

The correct answer is B.https://cloud.google.com/vpc/docs/shared-vpc#svc_proj_admins

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

Question: 30 CertyIQ

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

Explanation:

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

Question: 31 CertyIQ

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

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

Answer: B

Explanation:

B confirmed :-) https://cloud.google.com/solutions/dr-scenarios-planning-guide#use-cloud-storage-as-part-of-your-daily-backup-routine

Question: 32 CertyIQ

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

A. Create a new Service account, and give all application users the role of Service Account User.

B. Create a new Service account, and add all application users to a Google Group. Give this group the role of Service Account User.

C. Use a dedicated G Suite Admin account, and authenticate the application's operations with these G Suite credentials.

D. Create a new service account, and grant it G Suite domain-wide delegation. Have the application use it to impersonate the user.

Answer: D

Explanation:

Correct answer is Dhttps://developers.google.com/admin-sdk/directory/v1/guides/delegation

Clearly D is the right answer

Question: 33 CertyIQ

A customer wants to move their sensitive workloads to a Compute Engine-based cluster using Managed Instance Groups (MIGs). The jobs are bursty and must be completed quickly. They have a requirement to be able to control the key lifecycle.
Which boot disk encryption solution should you use on the cluster to meet this customer's requirements?

A. Customer-supplied encryption keys (CSEK)

B. Customer-managed encryption keys (CMEK) using Cloud Key Management Service (KMS)

C. Encryption by default

D. Pre-encrypting files before transferring to Google Cloud Platform (GCP) for analysis

Answer: B

Explanation:

Customer Managed Encryption keys using KMS lets users control the key management and rotation policies and Compute Engine Disks support CMEKs

Reference -

https://cloud.google.com/kubernetes-engine/docs/how-to/dynamic-provisioning-cmek

Question: 34 CertyIQ

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

Explanation:

Answer is B,https://cloud.google.com/dataproc/docs/concepts/configuring-clusters/customer-managed-encryption

In my opinion it should be B. reference : https://cloud.google.com/kms/docs/envelope-encryptionHow to encrypt data using envelope encryptionThe process of encrypting data is to generate a DEK locally, encrypt data with the DEK, use a KEK to wrap the DEK, and then store the encrypted data and the wrapped DEK. The KEK never leaves Cloud KMS.

Question: 35 CertyIQ

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

Explanation:

The Answer is C. Check "Setting up your payment-processing environment" section in

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

In the question, it is mentioned that it is the same environment for card processing as the Web App and Data processing and that is not recommended.

Question: 36 CertyIQ

A retail customer allows users to upload comments and product reviews. The customer needs to make sure the text does not include sensitive data before the comments or reviews are published.
Which Google Cloud Service should be used to achieve this?

A. Cloud Key Management Service
B. Cloud Data Loss Prevention API
C. BigQuery
D. Web Security Scanner

Answer: B

Explanation:

The answer can not be D (I am laughing loud since I use D for the reason of security scanning) hence the correct answer is B and it is not D

DLP provides the service of redaction.

Question: 37 CertyIQ

A company allows every employee to use Google Cloud Platform. Each department has a Google Group, with all department members as group members. If a department member creates a new project, all members of that department should automatically have read-only access to all new project resources. Members of any other department should not have access to the project. You need to configure this behavior.
What should you do to meet these requirements?

A. Create a Folder per department under the Organization. For each department's Folder, assign the Project Viewer role to the Google Group related to that department.

B. Create a Folder per department under the Organization. For each department's Folder, assign the Project Browser role to the Google Group related to that department.

C. Create a Project per department under the Organization. For each department's Project, assign the Project Viewer role to the Google Group related to that department.

D. Create a Project per department under the Organization. For each department's Project, assign the Project Browser role to the Google Group related to that department.

Answer: A

Explanation:

Correct answer - Ahttps://cloud.google.com/resource-manager/docs/cloud-platform-resource-hierarchy

It's A, Project Viewer. Project Browser doesn't allow users to see resources, only find the project in the hierarchy.

Question: 38 CertyIQ

A customer's internal security team must manage its own encryption keys for encrypting data on Cloud Storage and decides to use customer-supplied encryption keys (CSEK).
How should the team complete this task?

A. Upload the encryption key to a Cloud Storage bucket, and then upload the object to the same bucket.

B. Use the gsutil command line tool to upload the object to Cloud Storage, and specify the location of the encryption key.

C. Generate an encryption key in the Google Cloud Platform Console, and upload an object to Cloud Storage using the specified key.

D. Encrypt the object, then use the gsutil command line tool or the Google Cloud Platform Console to upload the object to Cloud Storage.

Answer: B

Explanation:

https://cloud.google.com/storage/docs/encryption/customer-supplied-keysAnswer B

you can't use google cloud console to upload the

object.https://cloud.google.com/storage/docs/encryption/using-customer-supplied-keys#upload_with_your_encryption_key

Question: 39 CertyIQ

A customer has 300 engineers. The company wants to grant different levels of access and efficiently manage IAM permissions between users in the development and production environment projects.
Which two steps should the company take to meet these requirements? (Choose two.)

A. Create a project with multiple VPC networks for each environment.
B. Create a folder for each development and production environment.
C. Create a Google Group for the Engineering team, and assign permissions at the folder level.
D. Create an Organizational Policy constraint for each folder environment.
E. Create projects for each environment, and grant IAM rights to each engineering user.

Answer: BC

Explanation:

Create a folder for each env and assign IAM policies to the group.

Question: 40 CertyIQ

You want to evaluate your organization's Google Cloud instance for PCI compliance. You need to identify Google's inherent controls.
Which document should you review to find the information?

A. Google Cloud Platform: Customer Responsibility Matrix
B. PCI DSS Requirements and Security Assessment Procedures
C. PCI SSC Cloud Computing Guidelines
D. Product documentation for Compute Engine

Answer: A

Explanation:

A. Google Cloud Platform: Customer Responsibility Matrix

https://services.google.com/fh/files/misc/gcp_pci_shared_responsibility_matrix_aug_2021.pdf

Question: 41 CertyIQ

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

Explanation:

Answer C is correct. The TTL is common use case of Cloud Storage life cycle management. Here is what GCP says:

"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

Question: 42 CertyIQ

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: B

Explanation:

Small containers usually have a smaller attack surface as compared to containers that use large base images.

https://cloud.google.com/blog/products/gcp/kubernetes-best-practices-how-and-why-to-build-small-container-images

Question: 43 CertyIQ

While migrating your organization's infrastructure to GCP, a large number of users will need to access GCP Console. The Identity Management team already has a well-established way to manage your users and want to keep using your existing Active Directory or LDAP server along with the existing SSO password.
What should you do?

A. Manually synchronize the data in Google domain with your existing Active Directory or LDAP server.

B. Use Google Cloud Directory Sync to synchronize the data in Google domain with your existing Active Directory or LDAP server.

C. Users sign in directly to the GCP Console using the credentials from your on-premises Kerberos compliant identity provider.

D. Users sign in using OpenID (OIDC) compatible IdP, receive an authentication token, then use that token to log in to the GCP Console.

Answer: B

Explanation:

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

Question: 44 CertyIQ

Your company is using GSuite and has developed an application meant for internal usage on Google App Engine. You need to make sure that an external user cannot gain access to the application even when an employee's password has been compromised.
What should you do?

A. Enforce 2-factor authentication in GSuite for all users.
B. Configure Cloud Identity-Aware Proxy for the App Engine Application.
C. Provision user passwords using GSuite Password Sync.
D. Configure Cloud VPN between your private network and GCP.

Answer: A

Explanation:

A. Enforce 2-factor authentication in GSuite for all users.

Question: 45 CertyIQ

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

Explanation:

Ans is C. BigQuery does not support CSEK.

https://cloud.google.com/security/encryption-at-rest.

https://cloud.google.com/security/encryption-at-rest

https://cloud.google.com/bigquery/docs/encryption-at-rest

Question: 46 CertyIQ

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

Explanation:

Correct answer is B.

BQ: https://cloud.google.com/bigquery-transfer/docs/locations#multi-regional-locations and https://cloud.google.com/bigquery-transfer/docs/locations#colocation_required

Bigtable: https://cloud.google.com/bigtable/docs/locations

PS: To people that are only commenting an answer, please provide a valid source to back your answers. This is a community driven forum and just spamming with wrong answers affects all of us.

Reference:

https://cloud.google.com/bigquery/docs/locations

Question: 47 CertyIQ

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

Explanation:

Correct Answer is (A)

he type of traffic that you need your load balancer to handle is another factor in determining which load balancer to use:

For HTTP and HTTPS traffic, use:

External HTTP(S) Load Balancing

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

Question: 48 CertyIQ

Applications often require access to `secrets` - small pieces of sensitive data at build or run time. The administrator

managing these secrets on GCP wants to keep a track of `who did what, where, and when?` within their GCP projects.
Which two log streams would provide the information that the administrator is looking for? (Choose two.)

A. Admin Activity logs
B. System Event logs
C. Data Access logs
D. VPC Flow logs
E. Agent logs

Answer: AC

Explanation:

AC is the answer.

Admin Access Logs and Data Access Logs

Reference:

https://cloud.google.com/kms/docs/secret-management

Question: 49 CertyIQ

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

Explanation:

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.

Question: 50 CertyIQ

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

Explanation:

Although both TCP Proxy LB and SSL Proxy LB support port 587 but only SSL Proxy LB support TLS. Hence 'D' is the right answer.

Reference:

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

Question: 51 CertyIQ

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

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

Answer: A

Explanation:

Answer 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.

Question: 52 CertyIQ

Your team needs to prevent users from creating projects in the organization. Only the DevOps team should be allowed to create projects on behalf of the requester.
Which two tasks should your team perform to handle this request? (Choose two.)

A. Remove all users from the Project Creator role at the organizational level.
B. Create an Organization Policy constraint, and apply it at the organizational level.
C. Grant the Project Editor role at the organizational level to a designated group of users.
D. Add a designated group of users to the Project Creator role at the organizational level.
E. Grant the billing account creator role to the designated DevOps team.

Answer: AD

Explanation:

A. Remove all users from the Project Creator role at the organizational level.D. Add a designated group of users to the Project Creator role at the organizational level.https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints

https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraintsI see no way to restrict project creation with an organizational policy. If that would have been possible I would have voted for it as restrictions can be overriden in GCP.

Question: 53 CertyIQ

A customer deployed an application on Compute Engine that takes advantage of the elastic nature of cloud computing.
How can you work with Infrastructure Operations Engineers to best ensure that Windows Compute Engine VMs are up to date with all the latest OS patches?

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

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

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

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

Answer: A

Explanation:

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

Definitely it will be A. The solution must take the advantage of elasticity of compute engine, so you create a template with patched OS base and redeploy images.

Question: 54 CertyIQ

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

Explanation:

A. Create an ingress firewall rule to allow access only from the application to the database using firewall tags.

Question: 55 CertyIQ

An organization receives an increasing number of phishing emails.
Which method should be used to protect employee credentials in this situation?

A. Multifactor Authentication
B. A strict password policy
C. Captcha on login pages
D. Encrypted emails

Answer: A

Explanation:

A. Multifactor Authentication

https://cloud.google.com/blog/products/g-suite/protecting-you-against-phishing

Question: 56 CertyIQ

A customer is collaborating with another company to build an application on Compute Engine. The customer is building the application tier in their GCP
Organization, and the other company is building the storage tier in a different GCP Organization. This is a 3-tier web application. Communication between portions of the application must not traverse the public internet by any means.
Which connectivity option should be implemented?

A. VPC peering
B. Cloud VPN
C. Cloud Interconnect
D. Shared VPC

Answer: A

Explanation:

A – 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.Dedicated Interconnect connections enable you to connect your on-premises network ... in another project, as long as they are both in the same organization. hence A

Question: 57 CertyIQ

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

Explanation:

Reference:
https://cloud.google.com/compute/docs/ip-addresses/reserve-static-external-ip-address

Question: 58 CertyIQ

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

A. Central management of routes, firewalls, and VPNs for peered networks

B. Non-transitive peered networks; where only directly peered networks can communicate

C. Ability to peer networks that belong to different Google Cloud organizations

D. Firewall rules that can be created with a tag from one peered network to another peered network

E. Ability to share specific subnets across peered networks

Answer: BC

Explanation:

B. Non-transitive peered networks; where only directly peered networks can communicate

C. Ability to peer networks that belong to different Google Cloud Platform organizations

Question: 59 CertyIQ

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

Explanation:

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.

C is better

Reference:

https://cloud.google.com/kubernetes-engine/docs/security-bulletins

Question: 60 CertyIQ

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

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

Answer: B

Explanation:

B. Use the Cloud Data Loss Prevention API to redact related infoTypes before data is ingested into BigQuery.

Question: 61 CertyIQ

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

Explanation:

B. Run each tier with a different Service Account (SA), and use SA-based firewall rules.

https://cloud.google.com/vpc/docs/firewalls#service-accounts-vs-tags

Question: 62 CertyIQ

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

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

Answer: B

Explanation:

GCS would be the chipest option

B. Cloud Storage buckets

Question: 63 CertyIQ

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

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/

Question: 64 CertyIQ

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

Explanation:

A. Encrypt all cache storage and VM-to-VM communication using the BoringCrypto module.

FIPS140 module is supported

Question: 65 CertyIQ

A customer has an analytics workload running on Compute Engine that should have limited internet access.
Your team created an egress firewall rule to deny (priority 1000) all traffic to the internet.
The Compute Engine instances now need to reach out to the public repository to get security updates.
What should your team do?

A. Create an egress firewall rule to allow traffic to the CIDR range of the repository with a priority greater than 1000.

B. Create an egress firewall rule to allow traffic to the CIDR range of the repository with a priority less than 1000.

C. Create an egress firewall rule to allow traffic to the hostname of the repository with a priority greater than 1000.

D. Create an egress firewall rule to allow traffic to the hostname of the repository with a priority less than 1000.

Answer: B

Explanation:

Answer is B. Lower number is higher priority and dest is only IP ranges in firewall rules

Question: 66 CertyIQ

You want data on Compute Engine disks to be encrypted at rest with keys managed by Cloud Key Management Service (KMS). Cloud Identity and Access
Management (IAM) permissions to these keys must be managed in a grouped way because the permissions should be the same for all keys.
What should you do?

A. Create a single KeyRing for all persistent disks and all Keys in this KeyRing. Manage the IAM permissions at the Key level.

B. Create a single KeyRing for all persistent disks and all Keys in this KeyRing. Manage the IAM permissions at the KeyRing level.

C. Create a KeyRing per persistent disk, with each KeyRing containing a single Key. Manage the IAM permissions at the Key level.

D. Create a KeyRing per persistent disk, with each KeyRing containing a single Key. Manage the IAM permissions at the KeyRing level.

Answer: B

Explanation:

all permission are the same-controled at the ring level

B. Create a single KeyRing for all persistent disks and all Keys in this KeyRing. Manage the IAM permissions at the KeyRing level.

Question: 67 CertyIQ

A company is backing up application logs to a Cloud Storage bucket shared with both analysts and the

administrator. Analysts should only have access to logs that do not contain any personally identifiable information (PII). Log files containing PII should be stored in another bucket that is only accessible by the administrator.
What should you do?

A. Use Cloud Pub/Sub and Cloud Functions to trigger a Data Loss Prevention scan every time a file is uploaded to the shared bucket. If the scan detects PII, have the function move into a Cloud Storage bucket only accessible by the administrator.

B. Upload the logs to both the shared bucket and the bucket only accessible by the administrator. Create a job trigger using the Cloud Data Loss Prevention API. Configure the trigger to delete any files from the shared bucket that contain PII.

C. On the bucket shared with both the analysts and the administrator, configure Object Lifecycle Management to delete objects that contain any PII.

D. On the bucket shared with both the analysts and the administrator, configure a Cloud Storage Trigger that is only triggered when PII data is uploaded. Use Cloud Functions to capture the trigger and delete such files.

Answer: A

Explanation:

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 theadministrator.

Question: 68 CertyIQ

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

Explanation:

"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."

Question: 69 CertyIQ

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

Explanation:

A. Google Cloud Directory Sync (GCDS)

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

Question: 70 CertyIQ

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

A. ISO 27001

B. ISO 27002

C. ISO 27017

D. ISO 27018

Answer: C

Explanation:
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.

Question: 71 CertyIQ

You will create a new Service Account that should be able to list the Compute Engine instances in the project. You want to follow Google-recommended practices.
What should you do?

A. Create an Instance Template, and allow the Service Account Read Only access for the Compute Engine Access Scope.

B. Create a custom role with the permission compute.instances.list and grant the Service Account this role.

C. Give the Service Account the role of Compute Viewer, and use the new Service Account for all instances.

D. Give the Service Account the role of Project Viewer, and use the new Service Account for all instances.

Answer: B

Explanation:

B. Create a custom role with the permission compute.instances.list and grant the Service Account this role.

Key here is "and grant the Service Account this role.". C and D are giving this role to ALL instances which is overly permissive. A is wrong. Only choice is B

Question: 72 CertyIQ

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

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

Answer: BD

Explanation:

. B. Network SecurityD. Access Policies

Chart is here https://cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate

Question: 73 CertyIQ

An organization is starting to move its infrastructure from its on-premises environment to Google Cloud Platform (GCP). The first step the organization wants to take is to migrate its ongoing data backup and disaster recovery solutions to GCP. The organization's on-premises production environment is going to be the next phase for migration to GCP. Stable networking connectivity between the on-premises environment and GCP is also being implemented.
Which GCP solution should the organization use?

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

Answer: B

Explanation:

Reference:
https://cloud.google.com/solutions/migration-to-google-cloud-building-your-foundation

Question: 74 CertyIQ

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:

Answer is (C).

The process of encrypting data is to generate a DEK locally, encrypt data with the DEK, use a KEK to wrap the DEK, and then store the encrypted data and the wrapped DEK. The KEK never leaves Cloud KMS.

Reference:

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

Question: 75 CertyIQ

A customer wants to make it convenient for their mobile workforce to access a CRM web interface that is hosted on Google Cloud Platform (GCP). The CRM can only be accessed by someone on the corporate network. The customer wants to make it available over the internet. Your team requires an authentication layer in front of the application that supports two-factor authentication
Which GCP product should the customer implement to meet these requirements?

A. Cloud Identity-Aware Proxy
B. Cloud Armor
C. Cloud Endpoints
D. Cloud VPN

Answer: A

Explanation:

A. Cloud Identity-Aware ProxyI think it's A. The question asks for an authentication layer.

Thank you

Thank you for being so interested in the premium exam material.
I'm glad to hear that you found it informative and helpful.

But Wait

I wanted to let you know that there is more content available in the full version.
The full paper contains additional sections and information that you may find helpful, and I encourage you to download it to get a more comprehensive and detailed view of all the subject matter.

Download Full Version Now

Future is Secured

100% Pass Guarantee

24/7 Customer Support

Mail us - certyiqofficial@gmail.com

Free Updates

Lifetime Free Updates!

Total: **249 Questions**

Link: https://certyiq.com/papers?provider=google&exam=professional-cloud-security-engineer