Exam Session - Cert Prep: Google Cloud Digital Leader

cloudacademy.com/quiz/exam/3761930/results

#1

You are a Chief Technology Officer helping your organization to modernize its IT infrastructure by adopting Google's public cloud services. Which of the following is an advantage of the Infrastructure-as-a-Service model that you should consider when choosing a solution?

✗

Web application security is managed by Google.

✗

IT costs change from operational to capital expenditures.

✓

Google assumes responsibility for server maintenance.

✗

Data storage and encryption become the responsibility of the organization.

Explanation

In the IaaS model, the cloud service provider managed and updates the data centers, servers, and other hardware, allowing subscribers to focus on core business activities rather than maintenance tasks associated with data centers.

In the IaaS model, web application security is the responsibility of the subscriber.

In the IaaS model, expenditures shift from capital to operational. Capital expenditures are business expenses incurred in order to create long-term benefits in the future, such as purchasing fixed assets like a building or equipment. Operational expenses are the daily operational costs of running a business, such as printer cartridges, electricity for powering office buildings, or services like website hosting. By using Google's IaaS solution, the organization greatly reduces the initial costs of getting the infrastructure up and running, thus eliminating the potentially large capital expenditures on traditional in-house IT infrastructure.

In the IaaS model, data storage and encryption are the responsibility of Google, not the organization. The IaaS model shifts the responsibility of data storage and encryption to the cloud provider.

🔗 https://cloud.google.com/learn/what-is-iaas

#2

A fitness application company is collecting the health data of its users is adding approximately 50 TBs of data every month. The data is expected to grow to 200+ TB every year.It has been observed that the users are primarily concerned with the last 30 days of data and are ready to wait for data retrieval if data is older than 30 Days.The company has decided that they will now store the infrequently accesses data older than 30 days to minimize the cost, as this data is typically accessed at max once per quarter or less.Which storage option would be best suited to store infrequently accesses data?

✗

Standard

✗

Nearline

✓

Coldline

✗

Archive

Explanation

Coldline storage is best suited to store infrequently accessed data that is planned to be read or modified at most once per quarter.

Standard storage is best suited to frequently accessed data also known as "Hot Data."

Nearline storage is best suited to store data that will be read or modified once a month or less.

Archive storage is best suited to store archive data that is required for legal, regulatory, or disaster recovery reasons.

🔗 https://cloud.google.com/storage/docs/storage-classes

#3

Your organization has planned to implement Site Reliability Engineering (SRE) best practices. You are tasked with configuring application-level monitoring and monitoring service-level objectives (SLOs) for applications and trigger alerts when SLOs are violated. Which of the following products should you choose for these tasks?

✗

Error reporting

✗

Cloud Logging

✓

Cloud Monitoring

✗

Cloud Trace

Explanation

Cloud Monitoring helps to gain visibility into application and infrastructure performance, availability, and health by:

- Automatically collecting system metrics
- Enabling SRE best practices
- Creating custom dashboards
- Creating alerts in integration with incident management tools.

Error reporting helps in identifying and understanding application errors.

Cloud Logging helps in the real-time management of logs with storage, search, analysis, and alerting and is a fully managed and scalable Google product.

Cloud Trace helps to identify performance bottlenecks in production and is not an appropriate tool for monitoring infrastructure performance.

https://cloud.google.com/error-reporting/

#4

You work for a ridesharing company that has recently moved to Google Cloud. Jack, the senior manager of the corporate accounting group is worried about the bill and wants to track actual Google Cloud spend against planned spend. Jack also wants to receive alerts via email when certain budget expenditures are reached. Which of the following actions should Jack take to meet these requirements?

✓

Create Cloud Billing Budgets, set a budget amount, and set budget alert threshold rules

✗

Use Cloud Billing Reports with Google Data Studio

✗

Use Cloud Billing data export to BigQuery functionality with Google Data Studio

✗

Create a Cloud Billing account, set a budget amount, and set budget alert threshold rules

Explanation

Cloud Billing budgets help customers to monitor Google Cloud charges in one place. In addition, a budget enables tracking of actual Google Cloud spends vis-à-vis planned spend.

The Cloud Billing Reports page helps users view Google Cloud usage costs and enables discovering and analyzing trends, while Google Data Studio helps to visualize data.

Up-to-date Cloud Billing graphs could be made available, and labels could be used to customize Google Cloud bills by combining Cloud Billing data export to BigQuery functionality with Google Data Studio.

A Cloud Billing account is an account where the project usage is charged. Setting budget amount and budget alert threshold rules is not possible with a Cloud Billing account.

https://cloud.google.com/billing/docs/how-to/budget-api-overview

#5

You are working on an enhancement project that requires the existing application to access the Analytics report data from the Analytics Reporting API. The application is hosted on a virtual machine with an internal IP address and no external IP address. What should you do to access the Analytics Reporting API?

✗

Disable Private Google Access.

✓

Enable Private Google Access.

✕

Ensure that VM interface has an external IP address assigned.

✕

Ensure that the VM interface is connected to a subnet where Private Google Access is disabled.

Explanation

Private Google Access can be enabled on the Virtual Machine instances that only have internal IP addresses to reach the external IP addresses of Google APIs and services, with an exception to App Engine Memcache, Filestore, and Memorystore.

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

#6

You have joined a growing company that offers online costume rentals through its website and mobile application. Although the volume of rental requests varies throughout the year, it peaks during the holiday season from October through January.The Head of the AppDev team has called for suggestions on scaling the systems to meet the spikes in demand without posing a risk to uptime.Which of the following solutions would best meet these requirements?

✕

Scale the systems vertically

✕

Increase the number of servers

✓

Scale the systems horizontally

✕

Implement load-balancing

Explanation

Horizontal scaling refers to adding additional machines/nodes to cater to the increased demand. Implementing horizontal scaling prevents downtime.

Vertical Scaling increases the system's capacity by adding more resources to the existing system to cater to the demand. However, vertical scaling carries a risk of downtime.

Increasing the number of servers to cater to the request would increase cost and infrastructure management needs.

By implementing load balancing, requests are efficiently distributed across configured resources; however, the addition or reduction of the resources is not a feature of load balancing because it applies to assigning traffic to machines rather than adding or removing machines based on traffic loads.

https://cloud.google.com/compute/docs/load-balancing-and-autoscaling

#7

A global insurance and financial company is planning to adopt cloud services to bring down infrastructure costs. The cloud deployment model adopted must meet all relevant international data security regulations.To ensure regulation compliance, the customer data with Client Identifying Data (CID) should be stored on-premises. Data without Client Identifying Data (CID) will be stored on the public cloud.Which of the following Cloud deployment models would you recommend?

✗

Public Cloud

✗

Private Cloud

✗

Community Cloud

✓

Hybrid Cloud

Explanation

As the customer requires storing customer data with CID on-premises and storing other applications and data on the public cloud, the hybrid cloud deployment model would be the most appropriate. Hybrid cloud consists of both public cloud and on-premises resources.

As the scenario requires that the customer data with CID be stored on-premises, the public cloud deployment model is incorrect.

A private cloud deployment model would not be cost-efficient because the private cloud is operated solely for a single organization.

A community cloud deployment model would not allow the organization to comply with the regulations to store customer data with CID because several organizations from the specific community share the infrastructure.

🔗 https://cloud.google.com/learn/what-is-cloud-computing

#8

Which of the following cloud computing concepts refers to increasing or decreasing compute resources based on demand?

✓

Elasticity

✕

Fault tolerance

✕

Load balancing

✕

High availability

Explanation

Elasticity is the degree to which a system is able to adapt to workload changes by provisioning and de-provisioning resources in an automated manner, such that at each point in time the available resources match the current demand as closely as possible.

Fault tolerance refers to the ability of an application to keep running even if some of its components fail.

Load balancing is a core networking solution used to distribute traffic across multiple servers in a server farm. Load balancers improve application availability and responsiveness and prevent server overload.

High availability is similar to fault tolerance. It refers to the ability of an application to keep running for an agreed-upon percentage of time, such as 99.99% of the time.

🔗 https://cloud.google.com/architecture/scalable-and-resilient-apps

#9

A news media giant with over 200 publications plans to build a scalable, secure, and serverless document database with a powerful query engine that can be added with mobile and web apps. Which Google Cloud product or service should the organization use?

✗

Memorystore

✗

Cloud BigTable

✗

Cloud SQL

✓

Firestore

Explanation

Firestore is a scalable, secured, and serverless NoSQL document database with a powerful query engine that can be added to mobile and web apps.

Memorystore is an in-memory data store best used to build application caches.

Cloud Bigtable is Google's fully managed product and is a NoSQL Big Data database service. It is a Cloud-native NoSQL wide-column store for large-scale, low-latency workloads including personalization, Adtech, and recommendation engines. It is not the most ideal database for a search engine that can be added with mobile and web apps.

Cloud SQL is a relational database service and is not suitable for this use case. It is most commonly used in Lift and shift of on-premises SQL databases to the cloud, Large-scale SQL data analytics, supporting content management system (CMS) data storage and scalability, and managing databases using Infrastructure as Code (IaC) https://cloud.google.com/memorystore/

#10

A wearable startup collecting the health data of its users is adding approximately 50 TBs of data every month. The data is expected to grow to 200+ TB every year.It is observed that the users are primarily concerned with the last 30 days of data and are ready to wait for data retrieval if data is older than 30 Days.The company has decided that they will now store infrequently accessed data that is older than 30 days to minimize the cost, as this data is typically accessed no more than once per quarter.To minimize manual intervention when moving data older than 30 days to Coldline storage from Standard storage, what should the company do?

✓

Configure object lifecycle management.

✗

Write a code and schedule it using Cloud Scheduler.

✗

Configure Cloud Scheduler to move data move based on required conditions.

✗

Configure an Object Lifecycle Management job using Cloud Scheduler.

Explanation

The movement of data from one storage class to another storage class could be automated by configuring Object Lifecycle Management.

Writing code requires manual effort and therefore does not fit the project's requirements.

Cloud Scheduler is a fully managed cron job service that does not have the capability of moving data between storage types.

Object Lifecycle Management is not a job and cannot be scheduled using Cloud Scheduler. Object Lifecycle Management is a set of rules.

https://cloud.google.com/storage/docs/lifecycle

#11

Your company uses Google Cloud Platform to house secure customer data. You are a data security manager and want to control which permissions are granted to the users who handle the data. Which of the following should you do to control permissions?

✓

Assign roles

✗

Use access lists

✗

Use authentications

✗

Assign resources

Explanation

In order to assign permissions, you should assign roles. Cloud Identity allows you to manage and authorize your user accounts across multiple applications and projects. It also supports SAML 2.0 (Security Assertion Markup Language) for single sign-on (SSO), as well as two-factor authentication (2FA). Whichever option you choose, you have full control over which permissions are granted to your users.

User access lists are for customizing access to specific objects within a bucket rather than managing permissions. Authentications are not appropriate in this scenario because roles include authentication measures such as SAML 2.0 (Security Assertion Markup Language) for single sign-on (SSO), as well as two-factor authentication (2FA). Resources refer to folders and projects, not users' permission to access them.

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

#12

An organization wants to use a Google Cloud service for a time-restricted project with the following guidelines:The developers should be free from infrastructure management activities.The chosen service should be able to integrate, clean, prepare, blend, transfer, and transform data.Which of the following Google Cloud services should the organization use?

✓

Cloud Data Fusion

✗

Cloud Composer

✗

Data Catalog

✗

Dataproc

Explanation

Cloud Data Fusion is best suited for the given scenario because it is a fully managed service that helps quickly build and manage data pipelines by integrating, cleaning, preparing, blending, transferring, and transforming data.

Cloud Composer facilitates creating, scheduling, monitoring, and managing workflows. It is not the optimal service for a project that requires the integration of data.

Data Catalog is a fully managed and scalable metadata management service that allows organizations to understand all their Google Cloud data by enabling quick discovery and management. Because Data Catalog focuses on metadata management rather than data integration, cleaning, preparation, blending, transferral, and transformation, it is not the best solution in this scenario.

Dataproc is a service that facilitates batch processing, querying, and streaming. It is not the best solution for this situation because it is primarily used for batch processing rather than managing data pipelines.

https://cloud.google.com/data-fusion/

#13

You are a manager with an e-retail website. The company has opted for the Standard Support customer care plan. The number of users has surged recently, and the company has realized the need for responses to its Priority 1 (P1) cases in 1 hour while also maintaining control of cost.Which of the following support plans would you suggest?

✗

Basic

✗

Standard

✓

Enhanced

✕

Premium

Explanation

The Enhanced Support customer is the appropriate choice in this scenario because it includes one-hour response times but is less costly than the Premium Support care plan. The Enhanced Support includes:

1. One-hour response time for P1 cases
2. 24/7 for P1 and P2 cases
3. Multi-channel support
4. Technical experts with advanced product knowledge
5. Third-Party Technology Support

The Basic Support plan is cost-effective because it is free, but it is not appropriate in this scenario because it does not include one-hour response times for P1 cases. With Basic Support, you have access to our documentation, community support, and support for Cloud Billing issues.

Standard Support is more cost-effective than Enhanced Support; however, it does not offer one-hour response times for P1 cases. Standard Support offers unlimited 1:1 technical support for outages and defects, unexpected product behavior, product usage questions, billing issues, and feature requests. The Standard Support offering is designed for small to medium organizations with workloads under development. With Standard Support, you have access to Active Assist recommendations and receive 4-hour response times for Priority 2 (P2) cases.

The premium support plan offers a response time of 15 minutes for P1 cases but is costlier than the Enhanced Support customer care plan. Premium Support is a paid support offering designed for enterprises that run mission-critical workloads and require fast response times, platform stability, and increased operational efficiencies. It is best suited for large enterprises rather than a smaller business seeking to optimize costs.

🔗 https://cloud.google.com/support

#14

Your organization is developing a global multi-player game and requires a database that can consistently capture player statistics. The most critical requirement of the database is that it can serve information for game leaderboards and return consistent rankings at any given time across game players all over the world. The game is rapidly developing a following with almost unlimited growth in the number of players. Which Google Cloud product should the organization choose?

✕

Firestore

✓

Cloud Spanner

✕

Cloud SQL

✕

Bare Metal

Explanation

Cloud Spanner is a fully managed relational database with unlimited horizontal scalability, strong consistency, and up to 99.999% availability. Because it is both global and unlimited in scale, it is the most appropriate choice in this scenario. It is highly available with zero scheduled downtime and online schema changes. It allows developers to focus on innovating gaming functions because it eliminates manual tasks with capabilities like automatic sharding that are a feature of Cloud SQL. Spanner provides a globally consistent database that can keep inventory or match history, such as the player information provided in gaming leaderboards, for massive player populations anywhere in the world.

Cloud Firestore is a fully managed, serverless, cloud-native NoSQL document database that simplifies storing, syncing, and querying data for your mobile, web, and IoT apps at a global scale. It could be used in the gaming scenario as part of the front end of the gaming platform, but it would not provide the inventory or match data for a game's global player population. The game's frontend services could use Firestore to store billions of documents with hierarchical world state data. Firestore could also hold user data like user configuration, party memberships, guilds, friends lists, and presence data. This use case incorporates other Google Cloud products as follows:

- Spanner provides a globally consistent database that can keep inventory or match history for massive player populations anywhere in the world.
- A regional in-memory cache is deployed on Memorystore for Redis to speed access to frequently used data.
- Events are logged to Bigtable, where developers or support staff can access them for troubleshooting.

- Data from frontend and backend databases is regularly imported to BigQuery to run data analytics pipelines. These pipelines help discover exploits or uncover gameplay mechanics that need an update before they affect the game's community and drive players away.

Cloud SQL is a relational database like Cloud Spanner, but it is not the ideal database to use in this scenario because it does not have the global availability of Cloud Spanner and does not scale well for massive data volume. It requires manual sharding of data, while Cloud Spanner does not, and it is primarily used for smaller amounts of data scaled vertically.

Bare Metal Solution is a data migration solution that provides hardware to run specialized workloads with low latency on Google Cloud. While it is a relational database like Cloud Spanner, it is most useful if there is an Oracle database that you want to lift and shift into Google Cloud. This enables data center retirements and paves a path to modernize legacy applications. It is not an appropriate solution in this scenario because it is specific to data migration and modernization of on-premises applications.

🔗 https://cloud.google.com/products

#15

Which of the following are benefits of Apigee? (Choose 3 answers)

✓

The ability to predict API traffic patterns

✗

The ability to make backend services visible

✓

The ability to modernize legacy services via RESTful interfaces

✓

The ability to record and analyze business metrics

Explanation

Apigee allows the user to predict API traffic patterns through metrics that can be used to understand potential traffic fluctuations and other information, modernize legacy services via RESTful interfaces by packaging legacy applications, and as An API abstraction and modernization layer to insulate client-facing applications from shifting backend services.

Apigee is an abstraction layer between backend services and the user. It does not make the backend service layer visible.

🔗 https://cloud.google.com/solutions/unlocking-legacy-applications#section-2

#16

Your client is a global packaging and printing company. They want to migrate to a fully managed Google Cloud storage solution with the following capabilities:Web content managementFile sharingMedia processing and renderingData analysisWhich solution should the company use?

✕

Archive Storage

✓

Filestore

✕

Persistent Disk

✕

Local SSD

Explanation

Filestore enables application migration to the cloud without requiring you to rewrite or rearchitect, thus accelerating and simplifying your migration. Filestore is a fully managed service suitable for Web content management, file sharing, rendering and processing media, and performing data analytics.

Archive Storage is object storage appropriate for data that can be stored for at least 365 days, such as regulatory archives. It is not the most appropriate solution for for dynamic content that must be accessed frequently.

Persistent Disk storage is Google's local durable storage service, fully integrated with Google Cloud products, Compute Engine, and Google Kubernetes Engine. While it could be used to store the company's files, it is not the most appropriate solution in this case because it would not allow media processing and rendering. If you attach a persistent disk to multiple instances, all instances must attach the persistent disk in read-only mode.

A Local SSD is not appropriate to the cloud storage requirement of the organization because they require a fully managed solution.

🔗 https://cloud.google.com/products/storage

#17

Which of the following operations in BigQuery reduce the total cost of ownership (TCO) for customers? (Choose 3 answers)

✓

Queries retrieving results from the cache

✓

Batch loading data into BigQuery from local files

✓

Running a query on an external data source from BigQuery

✕

Deleting a table, view, individual table partitions, and user-defined functions

Explanation

Certain operations in Google BigQuery are free and can result in reductions in the total cost of ownership (TCO) of a business using the service. Customers are not charged for queries that retrieve results from a cache, batch loading data into BigQuery from local files, or deleting a table, view, individual table partitions, or user-defined functions.

Customers using Google BigQuery are charged for the amount of Data processed in the selected columns and for running a query on an external data source from BigQuery, so those functions performed in BigQuery do not result in TCO reduction.

🔗 https://cloud.google.com/bigquery/pricing#bigquery-pricing

#18

Your client has multiple ongoing projects and to remove conflicts has asked you to devise a way to segregate service-level resources, such as the compute, storage, and networking resources being used by various projects.Which of the following should you use?

✕

Folders

✓

Projects

✗

Labels

✗

Tags

Explanation

Projects constitute service-level resources such as compute, storage, and networking resources.

Folders are used for projects rather than service-level resources.

Labels are used to annotate resources constituting projects and are the best choice for granular level cost tracking.

A tag is a string of characters added to a resource tags field. Tags cannot be created separately and are not separate resources.

🔗 https://cloud.google.com/resource-manager/docs/tags/tags-overview

#19

You are managing the development of a new application. You need a solution that will meet the following requirements:The developers should focus on writing code.Deployments should be zero-configuration.The developers should not manage infrastructure.The service should be scalable and accommodate surges in traffic without provisioning, patching, or monitoring.Applications should be safe from security threats.Which Google Cloud solution should you use?

✓

App Engine

✗

Cloud Functions

✗

Confidential VMs

✗

Eventarc

Explanation

App Engine is a fully managed serverless platform that helps to build highly scalable and secure applications. App Engine is suited to applications that have multiple functionalities behaving in various inter-related (or even unrelated) ways.

Cloud Functions is a serverless, lightweight compute solution for developers that helps create single-purpose, stand-alone functions that are triggered to Cloud events. Cloud Functions is suited to more single-purpose functions that respond to a specific event and perform a specific action.

Confidential VMs are a type of Compute Engine virtual machine (VM) best suited for enhanced performance and security for high-memory workloads, not application development.

Eventarc asynchronously delivers events from Google services SaaS and helps build event-driven solutions. It is most useful in situations such as Cloud Storage events (via Cloud Audit Logs) and to trigger a data processing pipeline. It is not the best service for applications that have multiple functionalities behaving in various inter-related (or even unrelated) ways.

https://cloud.google.com/appengine

#20

A global insurance company that uses Google Cloud Platform plans for its employees to work from home. It has requested a scalable, cost-effective solution that can enable encrypted desktop streaming so that employees can access corporate resources. Which of the following would you recommend?

✗

Google workspace

✓

Google Cloud Virtual Desktop

✗

Create an encrypted connection to the office network

✗

Enable Remote Desktop Protocol (RDP) to connect to remote desktops

Explanation

Google's Virtual Desktop cloud enables access to corporate resources that is secure and scalable and for these reasons is the most appropriate solution in this scenario. Virtual Desktop includes User authentication and authorization with Google Workspace, IAP, or Active Directory.

Google Workspace is a collection of cloud computing, productivity, and collaboration tools, software, and products developed and marketed by Google. It is not a desktop streaming application but a suite of cloud solutions.

Creating an encrypted connection to the office network is appropriate in this scenario, but Google's Virtual Desktop includes encrypted connections as well as user authentication and authorization with Google Workspace, IAP, or Active Directory.

Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft which provides a user with a graphical interface to connect to another computer over a network connection. The user employs RDP client software for this purpose, while the other computer must run RDP server software. Enabling RDP to connect to the office desktop is not a secure, scalable, and cost-efficient solution in this scenario because the company uses Google and Virtual Desktop includes the security features offered by RDP.

🔗 https://cloud.google.com/solutions/virtual-desktops

#21

Which of the following is a use of Big Table?

✗

SQL support for an online transaction processing system

✗

Interactive querying in an online analytical processing system

✗

Real-time data sync between users

✓

NoSQL database operations for large analytical and operational workloads

Explanation

BigTable is most suitable for NoSQL database operations for large analytical and operational workloads.

Cloud Spanner or Cloud SQL provides support for an online transaction processing system.

BigQuery is most apt for Interactive querying in an online analytical processing system.

Firebase Realtime Database is suitable for syncing data between users in real-time.

🔗 https://cloud.google.com/bigtable

#22

Which of the following are always the responsibility of customers using the public cloud? (Choose 2 answers)

✓

Web Client protection

✓

Data protection

✗

Network Controls

✗

Patch Management

Explanation

The security of the client that is being used by the customers (on Mobile devices, PC, etc.) to access the web content is the customer's responsibility.

Management, classification, and compliance obligation adherence are the customer's responsibility.

Configuring, managing, and securing Network controls are shared responsibilities in IaaS and PaaS models; however, the cloud provider is responsible primarily for network controls in the SaaS model.

Patch Management is a shared responsibility in IaaS and PaaS. The cloud provider manages patches in the SaaS model.

🔗 https://services.google.com/fh/files/misc/gcp_pci_srm__apr_2019.pdf

#23

Which of the following is a major cost-benefit of adopting cloud-native architecture?

✓

Managed services with high operational savings

✗

Managed open source or open source-compatible services

✗

Continuous Integration/Continuous Delivery

✗

Monitoring and automated recovery

Explanation

A key cost-benefit of cloud-native architecture is that it is includes managed services that result in high operational savings because the customer is no longer responsible for them. Such managed services could include IaaS, in which the cloud provider manages such things as hardware, storage, and encryption, PaaS, in which the service provider is responsible for identity and access management features, and SaaS, in which operations is to some extent managed.

Managed open source or open source-compatible services is a feature of cloud-native architecture but it is not the most relevant to cost savings.

Continuous Integration/Continuous Delivery is a feature of cloud-native architecture but it is not the most relevant to cost savings

Monitoring and automated recovery is a feature of cloud-native architecture but it does not directly involve cost savings.

🔗 https://cloud.google.com/blog/products/application-development/5-principles-for-cloud-native-architecture-what-it-is-and-how-to-master-it

#24

You are a manager for an energy company that is collecting non-structured key/value data in the form of usage reports from energy meters and home appliance sensors. Your IT department needs to securely connect and manage its IoT devices. Which of the following solutions would help you to connect and manage the IoT devices securely?

✓

IoT Core

✗

Traffic Director

✗

IoT Hub

✗

IoT Portal

Explanation

Internet of Things (IoT) Core is a fully managed service that allows you to connect to and manages IoT devices securely.

Traffic Director helps to deploy global load balancing across clusters and virtual machine (VM) instances.

IoT Hub is not a Google Cloud product.

IoT Portal is not a Google Cloud product.

🔗 https://cloud.google.com/solutions/iot

#25

Which of the following scenarios is not suitable for a Content Delivery Network (CDN)? (Choose 2 answers)

✓

A website for a small construction company located in the United States

✗

A global retail company with customers in Europe and the Americas

✓

A family history website with only a few visitors annually

✗

A global media website that provides news in multiple languages

Explanation

A website with users located in a specific geographic area would not benefit from a Content Delivery Network. CDNs are especially useful for large, complex websites with users spread across the globe, and websites or mobile apps with lots of dynamic content. A small company will most likely not need a CDN because its customers are geographically closer to the server.

A low-traffic website may experience slower traffic when using a CDN because its files will fall out of the CDN's cache, slowing down retrieval times when they are requested. Additionally, there is some small cost incurred, which may not be worthwhile in this case.

Content Delivery Networks are especially useful to large, complex websites with users spread across the globe, and websites or mobile apps with lots of dynamic content.

🔗 https://cloud.google.com/cdn/docs/overview

#26

You are a project manager for a global company that offers high-resolution documentary film editing services. Your team of content editors in New York and London needs to collaborate on editing projects that are located in Cloud Storage buckets.The maximum time to wait for a video's availability must be within a target time of 15 minutes, with minimal loss exposure. Which of the following storage configurations should you choose?

✗

Single region

✗

Dual-region

✗

Multi-region with default replication

✓

Dual-region with turbo replication

Explanation

Dual-region storage with turbo replication enabled would be the appropriate storage configuration in this scenario because turbo replication allows you to asynchronously replicate newly written Cloud Storage objects to a separate region within a target of 15 minutes. Because turbo replication is applicable only for dual-region buckets, it can be implemented in this scenario because the project teams are in London and New York.

Single region storage would not be an ideal configuration in this scenario because the project teams are in two regions, New York and London.

A dual-region is a specific pair of regions, such as New York and London. However, in this scenario, the specification is that videos be replicated within a target time of 15 minutes, which is not a guarantee of dual-region storage redundancy. While most objects are geo-redundant within minutes, some objects can take much longer to replicate.

Multi-region with default replication is not the optimal storage configuration in this scenario. While default replication asynchronously replicates newly written Cloud Storage objects to a separate region within minutes, some larger objects can take longer. Additionally, the regional requirements do not include multiple regions.

🔗 https://cloud.google.com/storage/docs/locations

#27

A credit card company has moved its applications to Google Cloud. Its customer data is stored across Cloud Storage, Datastore, and BigQuery and is used by applications and employees across the firm.Which Google Cloud solution should you use for the detection and classification of the stored sensitive data?

✕

Cloud Armor

✓

Cloud Data Loss Prevention

✕

Risk Manager

✕

Security Command Center

Explanation

The Cloud Data Loss Prevention service enables the discovery, detection, and classification of stored sensitive data. With Cloud Data Loss Prevention, you can create dashboards and audit reports, and automate tagging, remediation, or policy based on findings. Connect DLP results into Security Command Center, Data Catalog, or export to your own SIEM or governance tool for further analysis.

Cloud Armor helps to protect infrastructure and applications from DDoS and web attacks. It is not a solution for enabling the discovery, detection, and classification of stored data.

Risk Manager facilitates quick evaluation of the organization's security posture and connects with insurance partners for specialized cyber cover for GCP. The service does not focus on stored data.

Security Command Center strengthens the security posture of Google Cloud with a thorough evaluation that can mitigate threats. It is a tool for understanding an organization's overall security status rather than a solution for discovering, detecting, and classifying stored data.

🔗 https://cloud.google.com/dlp

#28

Your organization has decided to adopt a work-from-home policy. As part of the transition to remote work, the organization has made the decision to implement single sign-on (SSO) and multi-factor authentication (MFA) for all employees accessing resources in Google Cloud.Which of the following benefits of the cloud is applicable to this decision?

✓

Security

✕

Scalability

✕

Unlimited storage

✕

Reduced latency

Explanation

The primary benefit of the cloud in this use case is security. Because the company has adopted single sign-on (SSO) and multi-factor authentication (MFA) as part of its remote employees' login process, it has considered security as a beneficial feature of working in the cloud. Google Cloud helps protect your user accounts and company data with a wide variety of MFA verification methods such as push notifications, Google Authenticator, phishingresistant Titan Security Keys, and using your Android or iOS device as a security key. Employees can work from virtually anywhere, on any device, with single sign-on to thousands of pre-integrated apps, in the cloud.

Although scalability, unlimited storage, and reduced latency are all benefits of the cloud, they are not the most relevant benefits in this case.

🔗 https://cloud.google.com/identity

#29

In the shared responsibility model, which areas are the sole responsibility of public cloud customers for SaaS, PaaS, and IaaS services? (Choose 2 answers)

✓

Client device security

✓

Data protection

✕

Network hardware

✕

Physical security of public cloud infrastructure

Explanation

The security of the client device that is being used by customers (mobile device, PC, etc.) to access cloud applications is the customer's responsibility.

Data protection is the responsibility of the customer, although the customer can use some cloud services to help protect its data.

Network security is a shared responsibility. The cloud vendor provides a fundamental level of network security, while the customer is responsible for configuring certain types of network security in IaaS and PaaS models.

Maintenance of the server operating system is handled by the customer in the IaaS model and is handled by the cloud vendor in PaaS and SaaS models.

🔗 https://services.google.com/fh/files/misc/gcp_pci_srm__apr_2019.pdf

#30

To optimize the company’s Google Cloud spend, the management committee team wants an at-a-glance waterfall overview of their monthly costs and savings.Which of the following should you use to provide this information to the management team?

✓

Cost Breakdown reports

✗

Budget notifications

✗

Cost Table reports

✗

Pricing table reports

Explanation

The Cost Breakdown report helps with an at-a-glance waterfall overview of monthly costs and savings.

Budget notifications facilitate a real-time status of the Cloud Billing budget and are not a method for gaining an overview of monthly costs.

Cost Table reports help access and analyze invoice and statements details but are not an optimal method for providing an overview of costs.

The pricing table report helps access SKU prices for Google's cloud services and is not an efficient method for providing a high-level picture of costs.

🔗 https://cloud.google.com/billing/docs/how-to/cost-breakdown

#31

You are leading a team of developers on a project whose goal is to improve customer experience on a credit card company's website.The solution requires custom code without the overhead of managing operating systems or infrastructure.Which of the following cloud offerings would you suggest to your client?

✗

Infrastructure as a Service (IaaS)

✓

Platform as a Service (PaaS)

✕

On-premises infrastructure

✕

Software as a Service (SaaS)

Explanation

Platform as a Service (PaaS) allows the development, testing, and hosting of apps in the same environment but provides no user control over the infrastructure. It is the best choice for creating customized apps.

Infrastructure as a Service (IaaS):

- Provides complete control over the data, apps, middleware, operating system
- Automated hardware deployment
- Virtualized management workload

Function as a Service (FaaS)

- Helps the developers in running and managing the microservices
- Facilitates event-based-triggered code execution
- Software as a Service (SaaS)

Provides subscription-based model

- No control over the infrastructure to users
- An apt choice for short-term projects requiring collaboration

🔗 https://cloud.google.com/learn/what-is-iaas

#32

How does Google Cloud suggest that organizations use third-party identity providers to enable users access to Google Cloud with their corporate credentials?

✕

By delegating responsibility to service accounts and groups

✗

By implementing the principle of least privilege

✓

By federating third-party identity providers with Google Cloud

✗

By migrating unmanaged accounts to personal accounts

Explanation

If the organization uses a third-party identity provider, the organizations’ user directory should be synchronized with Cloud Identity to let users access Google Cloud with their corporate credentials.

Delegating responsibility with service accounts and groups is associated with assigning IAM roles, not with enabling a user's access to Google Cloud with their corporate credentials.

The principle of least privilege is not related to enabling users access to Google Cloud with their corporate credentials but with access to resources within Google Cloud.

Migration of unmanaged accounts is required to be implemented when members of the organizational domain have used their corporate email ID to create a personal Google Account.

🔗 https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations#groups-and-service-accounts

#33

An organization is developing a business-critical application using Google App Engine. Which of the following should the organization expect to do? (Choose 2 answers)

✓

Establish Role-based access policies

✗

Encrypt data at rest

✓

Monitor application security

✗

Maintain network security

Explanation

Google App Engine is a fully managed Platform as a Service (PaaS) that lets users focus on code while App Engine manages infrastructure concerns. Within Google's shared responsibility matrix, the PaaS customer is responsible for establishing Role-based access policies (RBAC) and monitoring application security. Google is responsible for maintaining network security and encrypting data at rest.

🔗 https://cloud.google.com/privacy

#34

A financial organization wants to stream logs and events from Google Cloud resources into Splunk. The solution requires that services communicate asynchronously.Which of the following services will best create a system of event producers and consumers so that the event producers can communicate asynchronously with event consumers by broadcasting events?

✓

Pub/Sub

✗

Dataflow

✗

Dataproc

✗

Google Data Studio

Explanation

Pub/Sub is the appropriate choice because it ingests event streams at scale between the publishers and subscribers.

Dataflow helps in developing real-time batch and streaming data processing pipelines. Because it is used in developing batch processing pipelines, it is not the ideal service to use for ingesting events communicated between publishers and subscribers.

Dataproc facilitates batch processing, querying, and streaming. Because the focus of the service is on batch processing rather than on event streams, it is not the most appropriate choice in this scenario.

The online tool Google Data Studio helps in generating reports and dashboards from data. It is not an appropriate solution for ingesting event streams at scale.

🔗 https://cloud.google.com/pubsub/

#35

An organization using Google Cloud wants to hierarchically organize and group resources, as well as manage access control and configuration settings for container resources.Which Google product or service should the organization use?

✗

Eventarc

✗

Artifact Registry

✗

Container Registry

✓

Resource Manager API

Explanation

The Resource Manager API service helps Google Cloud customers programmatically manage the container resources by creating, reading, and updating metadata for Google Cloud Platform resource containers.

Eventarc asynchronously delivers events from Google Cloud's SaaS and helps build event-driven architectures without having to implement, customize, or maintain the underlying infrastructure. Eventarc offers a standardized solution to manage the flow of state changes, called events, between decoupled microservices. When triggered, Eventarc routes these events through Pub/Sub subscriptions to Cloud Run or Cloud Run for Anthos while managing delivery, security, authorization, observability, and error handling for you.

Artifact Registry is a fully-managed service with support for both container images and non-container artifacts. Artifact Registry facilitates storing, managing, and securing docker container images, and language packages.

Container Registry facilitates storing, managing, and securing docker container images.

🔗 https://cloud.google.com/resource-manager/

#36

A team of Cloud Engineers is working on developing and deploying a containerized application that will process and serve a large amount of image data in cloud storage. The data must be invocable via requests or events.Which Google Cloud compute service should the team use so that there are no infrastructure management problems?

✗

Cloud Build

✗

Cloud Code

✓

Cloud Run

✗

Cloud Deploy

Explanation

Cloud Run is a fully managed, serverless compute platform that enables the development and deployment of a containerized application invocable via requests or events. Using Cloud Run would avoid the problem of infrastructure management because it is a fully managed service.

Cloud Build is a Google Cloud Service that helps in executing the builds on Google Cloud Platform infrastructure. It would not be the most appropriate service in this case because the use case requires processing and serving images in the cloud, not executing infrastructure builds on Google Cloud's platform.

Cloud Code is a fully integrated Google Cloud offering for Kubernetes development and debugging environment within IDE. Cloud Code helps in creating and managing clusters directly from within the IDE, it is not the appropriate service for enabling the development and deployment of a containerized application invocable via requests or events.

Cloud Deploy Google Cloud Deploy facilitates automated delivery of applications in a defined sequence to a series of target environments. It is not a service that would allow you to develop and deploy a containerized application that will process and serve a large amount of image data in cloud storage.

🔗 https://cloud.google.com/build/

#37

You are managing a project for a large healthcare provider with 100+ clinics and hospitals across the European Union. Your client plans to develop an OCR application to digitize overall clinical records, including X-Rays and patients' health records.As part of the solution, it is decided that:Image files will be uploaded.Text will be extracted from the image.The extracted text will be translated into English.The final ready text will be stored for further use.The client does not want any overhead and has asked you to use a Google Cloud product that can offer pre-trained machine learning models through REST APIs.Which Google Cloud solution would you suggest?

✕

AutoML Vision

✓

Vision API

✕

Cloud Natural Language API

✕

Vertex AI Vizier

Explanation

Vision API is the correct choice. Vision API offers pre-trained ML models through RPC and REST APIs. Because Vision API offers pre-trained ML models, it is the best solution for extracting text from image files as requested in this use case. The Google Cloud Vision API uses pre-trained Vision API models to detect emotion, understand text, and more. It allows developers to easily integrate vision detection features within applications, including image labeling, face, and landmark detection, optical character recognition (OCR), and tagging of explicit content.

In the given scenario, the client has requested to use a Google Cloud solution that can offer pre-trained ML models through REST APIs. AutoML Vision is a product that helps by automating the custom ML models' training. AutoML Vision enables you to train machine learning models to classify your images according to your own defined labels and train models from labeled images and evaluate their performance, leverage a human labeling service for datasets with unlabeled images, and register trained models for serving through the AutoML API.

Cloud Natural Language API provides capabilities to derive natural language understanding to find and label fields within a text document, including emails, chat, and social media, and then use sentiment analysis to understand customer opinions to find actionable product and UX insights. It is not an appropriate tool for extracting text from image files.

Vertex AI Vizier does not help in extracting text from images. It assists in orchestrating ML (Machine Learning) workflows.

https://cloud.google.com/vision

#38

A company that stores some of its customers' credit card data on-premises is migrating the data to Google Cloud. Prior to the migration, the organization wants to understand how Google will store and process the customer data. Which of the following aspects of the Google Cloud platform should the organization learn more about?

✗

Availability

✗

Compliance

✓

Privacy

✗

Security

Explanation

Privacy in the context of the cloud refers to the data organizations or individuals have access to and share. When the organization moves its data to the cloud, the organization retains control of the data. As a Google Cloud customer, the organization should learn that when it migrates to the cloud, it continues to own its customers' data and can control who has access to it and who the data can be shared with. Google stores and processes data, but the data remains private because access to it is controlled by the organization. Google provides the organization with tools and features to control that access, thus helping the organization maintain the privacy of the customers' data in the cloud.

Availability refers to the duration of Google's services' availability and the response time to user requests for services, not specifically to access to and control of customer data.

Compliance refers to third-party or other regulatory standards for handling data. While it would be an area of concern for an organization migrating customers' credit data to the cloud, it does not specifically reference how Google will store and process the customer data. Data compliance is a part of a total approach to data privacy in the cloud, but it does not specifically reference how access to customers' data is handled when it is migrated to the cloud.

Security in the cloud refers to the policies, procedures, and controls that keep data safe. When the organization migrates to Google Cloud, Google implements stringent security measures to safeguard an organization's customer data and provides the organization with tools and features to control it. Security is part of the concept of privacy as it applies to customer data, which includes rules about who can access data and with whom it can be shared.

🔗 https://cloud.google.com/privacy

#39

A multinational retail corporation plans to migrate its on-premises inventory management system to Google Cloud. The current inventory management system has experienced performance issues that are the result of very high IOPS.How can the organization increase performance and decrease latency by moving to Google Cloud?

✓

Use Local SSDs

✕

Use SSD disks

✕

Use Standard persistent disks

✕

Use Balanced persistent disks

Explanation

Compute Engine offers always-encrypted local solid-state drive (SSD) block storage for virtual machine (VM) instances. Each local SSD is 375 GB in size, but you can attach a maximum of 24 local SSD partitions for 9 TB per instance. Optionally, you can format and mount multiple local SSD partitions into a single logical volume.

Unlike Persistent Disks, Local SSDs are physically attached to the server that hosts your VM instance. This tight coupling offers superior performance, very high input/output operations per second (IOPS), and very low latency compared to persistent disks.

Persistent disks are networked storage and have higher latency in comparison to physical disks or local SSDs.

https://cloud.google.com/compute/docs/disks/local-ssd

#40

A startup is planning to adopt Google Cloud Services. As a first step, the company plans to migrate its data to Google Cloud.Which of the following should the company use to migrate over 1 TB of data from a private data center to the cloud while adhering to a strict timeline of 1-2 days and accommodating available bandwidth in order to meet the project deadline?

✓

Storage Transfer Service

✕

gsutil

✕

Transfer appliance

✕

Migrate for Anthos and GKE

Explanation

Storage Transfer Service allows you to migrate data from a private data center to Google Cloud. With Storage transfer, you can move petabytes of data from on-premises sources or other clouds over online networks with billions of files and 10s of Gbps. You can also optimize your network bandwidth and accelerate transfers with scale-out performance.

gsutil is a file transfer service that allows up to 1TB of data transfer, not more than 1TB, as is specified in this scenario.

A transfer appliance is a device for transferring and shipping data to Google for transfer to the cloud. With Transfer Appliance, you can receive the appliance and capture a petabyte of data in under 25 days. Your data can be accessed in Cloud Storage within another 25 days. In this scenario, it would not be the most expedient way to transfer data from on-premises to the cloud because of the restrictive timeline in this scenario.

Migrate for Anthos and Google Kubernetes Engine (GKE) facilitates the conversion of VM-based workloads into containers in GKE or Anthos. It would not be the most relevant migration method in this scenario because the project does not specify compatibility with GKE or Anthos.

🔗 https://cloud.google.com/architecture/migration-to-google-cloud-transferring-your-large-datasets#transfer-options
#41

You work for an e-commerce website and want to use a product that can predict users' purchasing behavior and suggest products based on that behavior. Which of the following Google Cloud AI solutions would you recommend?

✓

Vertex AI Matching Engine

✕

Vertex AI

✕

Vertex Explainable AI

✕

Vertex AI Workbench

Explanation

Vertex AI Matching Engine is the appropriate solution to use in this scenario because it uses a vector similarity search function to perform searches on a large amount of data. At a basic level, a vector similarity search involves representing pictures or bits of text as vectors or embeddings (mappings of a discrete — categorical — variable to a vector of continuous numbers) that can train machine learning models. The state-of-the-art paradigm for building such semantic matching systems is by computing vector representations of the items. These vector representations are often called 'embeddings'. Embeddings are computed by using machine learning models. The models are trained to learn an embedding space in which similar examples are close while dissimilar ones are far apart. Thus, the closer two items are in the embedding space, the more similar they are. An example of this function for e-commerce is when given a query item, such as a product previously purchased, Matching Engine finds the most semantically similar items to it from a large corpus of candidate items. The ability to search for semantically similar or semantically related items has many real-world use cases and is a vital part of applications such as recommendation engines, search engines, ad targeting systems, image classification or image search, text classification, question answering, and chatbots

Vertex AI helps train models, save models, deploy models, and make predictions from a unified MLOps platform. Vertex AI provides options of AutoML and AI Platform to choose from its users. It is best suited to scenarios in which the user wishes to deploy AI for a variety of use cases involving data, uses which extend beyond those of product recommendations on an e-commerce website as described in this scenario.

Vertex Explainable AI Vertex Explainable AI integrates feature attributions into Vertex AI. This page provides a brief conceptual overview of the feature attribution methods available with Vertex AI. For an in-depth technical discussion, refer to our AI Explanations Whitepaper.

Vertex Explainable AI helps you understand your model's outputs for classification and regression tasks. Vertex AI tells you how much each feature in the data contributed to the predicted result. You can then use this information to verify that the model is behaving as expected, recognize bias in your models, and get ideas for ways to improve your model and your training data. Vertex Explainable AI could be used to train models to discover customer preferences; however, its uses could extend beyond those of the e-commerce website, and therefore it is not the most suitable solution in this scenario.

Vertex AI Workbench helps in implementing complete data science workflow in Jupyter notebook-based development environment. It is primarily a data training tool rather than an analysis tool for recommending products based on behavior as specified in the scenario. It can natively analyze your data with a reduction in context switching between services.

🔗 https://cloud.google.com/vertex-ai/docs/matching-engine

#42

Which of the following Google infrastructure security layers provides denial-of-service (DoS) protection?

✗

Operational Security

✓

Internet Communication

✗

Storage Services

✗

User Identity

Explanation

There are 6 Google infrastructure security layers: Operational Security, Internet Communication, Storage Services, User Identity, Service Deployment, and Hardware Infrastructure.

Google Front End and denial-of-service (DoS) protection are provided at the Internet Communication layer.

The Operational Security layer addresses Intrusion detection and reducing insider risk are some of the areas addressed at

Encryption at rest and deletion of data protection are provided at the Storage Services layer.

Authentication and login abuse protection are found at the User Identity layer.

🔗 https://cloud.google.com/security/infrastructure/design

#43

A multinational food delivery startup has moved its applications to the cloud. The Head of AppDev wants to introduce a new service that analyses customer preferences based on previous orders and suggests to them what to order.Which cloud computing model would help developers create the service while freeing them of infrastructure and management tasks?

✓

Serverless computing

✗

IoT

✗

High-performance computing

✗

Edge Computing

Explanation

Serverless computing helps developers to build code without managing infrastructure. Event-driven services could be built using serverless computing offerings.

IoT stands for Internet of Things and refers to objects, generally sensors that are internet-connected and have the capability to collect and transfer data.

High-performance computing (HPC) is the computing ability that helps in processing data and performing complex calculations at very high speeds. This is not a cloud computing execution model.

Edge computing is the computing model that helps capture, process and analyze the data near the data source. In the given scenario, Edge computing does not serve the purpose of developing the service described.

🔗 https://en.wikipedia.org/wiki/Serverless_computing

#44

Which of the following Google Cloud products can be used to explore and visualize data? (Choose 2 answers)

✕

Cloud Firestore

✕

Dataproc

✓

Datalab

✓

Data Studio

Explanation

Datalab and Data Studio are tools for exploring and visualizing data. Datalab allows you to interactively explore, visualize, analyze, and transform data using familiar languages, such as Python and SQL. Pre-installed Jupyter introductory, sample, and tutorial notebooks, show you how to access, analyze, monitor, and visualize data. Data Studio is a tool that allows you to tell your data story with charts, including line, bar, and pie charts, geo maps, area and bubble graphs, paginated data tables, pivot tables, and more.

Cloud Firestore is a storage tool. It is a NoSQL document database that lets you easily store, sync, and query data for your mobile and web apps on a global scale. It is not appropriate in this scenario because it is not a data visualization tool.

Dataproc is a tool for processing and analyzing data. Dataproc is a fully managed and highly scalable service for running Apache Spark, Apache Flink, Presto, and 30+ open source tools and frameworks. It is not appropriate in this scenario because it is not primarily a data visualization tool as specified in this scenario.

🔗 https://cloud.google.com/architecture/data-lifecycle-cloud-platform

#45

A DevOps team is responsible for maintaining and analyzing system and application logs for an application running across several instances on Google Cloud Platform. What steps should the team take to ensure the integrity of the logs generated on these instances? (Choose 2 answers)

✓

Implement log versioning on log buckets in Cloud Storage.

✓

Copy the logs to another project with a different owner.

✗

Set the logging level to only collect log output for critical messages.

✗

Export all log files to BigQuery.

Explanation

Here are two things you could do to protect the integrity of your log files:

- Implement log versioning on log buckets in Cloud Storage to prevent losing or overwritten data if an unauthorized person gains access. The Cloud Storage service automatically encrypts all data before it is written to the log buckets. Still, with versioning, you can increase security by forcing a new version to be saved whenever an object in a log bucket is changed.

- Copy the logs to another project with a different owner to require two people to have ownership of the logs.

The other options are incorrect for the following reasons:

- Setting the log level to only collect critical messages would not help maintain the integrity, and would make it so that you cannot see messages that may help you identify problems.
- Exporting logs to BigQuery could help you do complex log analysis, but would not protect the integrity of the logs.

/course/introduction-google-cloud-operations-suite/logging-gcs/

#46

Which of the following defines a private cloud?

✓

A collection of resources that are not shared with the general public

✗

A collection of virtual on-demand services that are offered to the public

✗

A collection of resources that are shared between private and public cloud users

✗

A collection of resources that are isolated on-premises for use by an organization

Explanation

A private cloud is a collection of resources that are not shared with the general public.

A public cloud is a virtual on-demand service that is offered to the public.

A hybrid collection of resources that are shared between the private and public.

An on-site data center is a collection of on-premise resources that are used by an organization.

https://cloud.google.com/vpc

#47

You are an IT manager who wants to reduce the cost and labor that would be required for a manual application modernization project using a Google Cloud solution. You are deciding whether to adopt Migrate for Compute Engine or Migrate for Anthos and need to explain the differences between the two solutions to management.Which of the following differences would you explain?

✗

Migrate for Compute Engine charges for transferring data to Google, but Migrate for Anthos does not.

✓

Migrate for Anthos migrates to containers, and Migrate for Compute Engine migrates to virtual machines.

✗

Migrate for Compute Engine requires complex deployment and setup, while Migrate for Anthos requires only lift and shift migration.

✗

Migrate for Anthos requires manual operating system upgrades, and Migrate for Compute Engine is fully managed.

Explanation

The key difference between the two solutions is that Migrate for Anthos migrates to containers, and Migrate for Compute Engine migrates to virtual machines.

A difference between the two solutions is not that Migrate for Compute Engine charges for transferring data to Google, but Migrate for Anthos does not. Migrate for Compute Engine does not charge for ingress traffic.

Migrate for Compute Engine is often associated with lift and shift operations, while Migrate for Anthos may involve a more complex to its containerized system depending on the needs of the organization.

Migrate for Anthos does not require manual operating system upgrades because it is a containerized system, and Migrate for Compute Engine is not a fully managed solution. Compute Engine offers two kinds of VM instance groups, managed and unmanaged: Managed instance groups (MIGs) let you operate apps on multiple identical VMs. Unmanaged instance groups let you load balance across a fleet of VMs that you manage yourself.

🔗 https://cloud.google.com/migrate/anthos/docs/anthos-migrate-benefits

#48

An organization requires a fully managed, scalable queuing service that will help manage the execution, dispatch, and delivery of multiple distributed tasks. Which Google Cloud solution should the organization use?

✗

Cloud Scheduler

✓

Cloud Tasks

✗

Service Infrastructure

✗

Workflows

Explanation

Cloud Tasks is a fully managed, scalable queuing service that could help manage the execution, dispatch, and delivery of multiple distributed tasks. Cloud Tasks lets you separate out pieces of work that can be performed independently, outside of your main application flow, and send them off to be processed, asynchronously, using handlers that you create. These independent pieces of work are called tasks. For example, you need to update a database as part of processing a user request, but updates can be time-consuming. Offloading that detail as a task allows you to return from the request more quickly.

Cloud Scheduler is a Fully managed cron job service that facilitates scheduling batch jobs, big data jobs, and cloud infrastructure operations.

Service Infrastructure is a foundational platform for creating, managing, securing, and consuming APIs and services across organizations. It is used by Google APIs, Cloud APIs, Cloud Endpoints, and API Gateway. Service Infrastructure provides a wide range of features to service consumers and service producers, including authentication, authorization, auditing, rate limiting, analytics, billing, logging, and monitoring.

Workflows are serverless workflows that help with the orchestration and automation of Google Cloud and HTTP-based API services.

🔗 https://cloud.google.com/tasks/docs/dual-overview

#49

Your company's website enables users to upload images and input text to create memes of their choice. Lately, you have observed some suspicious traffic and want to protect your website from spam, specifically from bots using the website.Which of the following Google Cloud solutions should you use to protect your website from bots and ensure that it is being accessed only by human users?

✓

reCAPTCHA Enterprise

✕

Policy Troubleshooter

✕

Web Risk

✕

Cloud Identity

Explanation

reCAPTCHA Enterprise uses an adaptive risk analysis engine to keep automated software from engaging in abusive activities on your site. With technology that has helped defend millions of websites for over a decade, reCAPTCHA Enterprise is built to help mitigate fraudulent online activity for your business.

Web Risk is an enterprise security product that lets client applications check URLs against Google's directory of unsafe web resources.

Policy Troubleshooter enables security administrators to understand why requests were denied and help them modify policies to grant the appropriate access. It is an access management and control tool, not a threat detection tool.

Cloud Identity helps easy management of user identities, devices, and applications from a single console. It is not an automated, adaptive risk analysis tool because the user must manage it.

🔗 https://cloud.google.com/recaptcha-enterprise/

#50

How can a software developer contribute to Site Reliability Engineering (SRE) within an organization?

✗

By allocating problem-solving tasks to operations teams

✗

By manually configuring production systems

✓

By focusing on implementing automation

✗

By creating static solutions in order to avoid failure

Explanation

Site Reliability Engineering teams focus on hiring software engineers to run products and create systems to accomplish the work that would otherwise be performed, often manually, by sysadmins.

In a traditional operations model, problem-solving tasks were often allocated to operations teams.

Site Reliability Engineering focuses on automating production systems rather than manually configuring them.

Site Reliability Engineering focuses on dynamic, not static solutions to problems. SRE operates with the understanding that failure is planned for and expected and that solutions to problems may change as a result.

https://sre.google/sre-book/introduction/