

Exam Session - Cert Prep: Google Associate Cloud Engineer

 cloudacademy.com/quiz/exam/3771854/results

#1

Dave has been asked to track down logging on some actions that were initiated by the GCP infrastructure. He's also been asked to review the audit logs for some write operations that were performed on a BigQuery database. Which audit log(s) should Dave be interested in?



Admin Activity audit logs only



System Event audit logs only



Data Access audit logs only



System Event audit logs and Data Access audit logs

Explanation

Admin Activity audit logs contain log entries for API calls or other administrative actions that modify the configuration or metadata of resources. For example, these logs record when users create VM instances or change Cloud Identity and Access Management permissions.

Data Access audit logs contain API calls that read the configuration or metadata of resources, as well as user-driven API calls that create, modify, or read user-provided resource data. Data Access audit logs do not record the data-access operations on resources that are publicly shared (available to **All Users** or **All Authenticated Users**) or that can be accessed without logging into Google Cloud.

System Event audit logs contain log entries for Google Cloud administrative actions that modify the configuration of resources. System Event audit logs are generated by Google systems; they are not driven by direct user action.



<https://cloud.google.com/logging/docs/audit/>

#2

To configure Stackdriver to monitor a web server and notify you if it goes down, what steps do you need to take? (Choose 2 answers)



Install the Stackdriver Monitoring Agent on the web server



Create an uptime check



Create an alerting policy



Install the Stackdriver Logging Agent on the web server

Explanation

Uptime checks verify that your web server is always accessible. The **alerting policy** controls who is notified if the uptime checks should fail.

You don't need to install the Stackdriver Monitoring Agent to get downtime alerts. The agent provides additional information, but it's not required. The Stackdriver Logging Agent is for additional logging, not for alerts.

Using the Monitoring agent is optional. Stackdriver Monitoring can access some metrics without the Monitoring agent, including CPU utilization, some disk traffic metrics, network traffic, and uptime information. [<https://cloud.google.com/monitoring/agent/#purpose>]

 <https://cloud.google.com/monitoring/quickstart-lamp#gs-checks>

Covered in this lecture

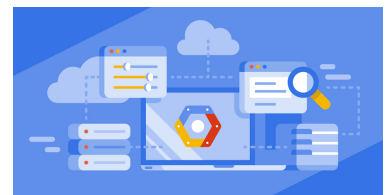
Monitoring

Course: Managing Your Google Cloud Infrastructure

9m



#3



Steven has been tasked with ensuring that only those people who actually need access to certain GCP resources have access. Which service should Steven be relying on to secure access to his organization's GCP resources?



Cloud IAM



Cloud AD



Directory Services



RBAC

Explanation

Cloud IAM lets you grant granular access to specific Google Cloud resources and helps prevent access to other resources. Cloud IAM lets you adopt the security principle of least privilege, where you grant only necessary permissions to access specific resources.

 <https://cloud.google.com/iam/docs/overview>

#4

Which of the following Kubernetes controllers should be used for maintenance operations that must run with exactly one pod running on each node?



DaemonSet



ReplicaSet



StatefulSet



Deployment

Explanation

DaemonSets attempt to adhere to a one-Pod-per-node model, either across the entire cluster or a subset of nodes. As you add nodes to a node pool, DaemonSets automatically add Pods to the new nodes as needed.

 <https://cloud.google.com/kubernetes-engine/docs/concepts/daemonset>

Covered in this lecture

Summary

Course:Administering Kubernetes Clusters



4m



#5

Cloud Dataproc charges you only for what you really use with _____ billing.



daily



hour-by-hour



minute-by-minute



second-by-second

Explanation

One of the advantages of Cloud Dataproc is its low cost. Dataproc charges for what you really use with second-by-second billing and a one-minute-minimum billing period.



<https://cloud.google.com/dataproc/docs/concepts/overview>

#6

After an incident at Blue Widget Corp, where a user accidentally deleted a project, corporate leaders are now demanding that projects be protected from accidental deletion. What tool (or service) will allow Steve, as the administrator, to enforce this standard?



GCP Cloud Identity and Access Management



Role-Based Access Control



Assigning Liens



GCP Trust and Security

Explanation

You can place a lien upon a project to block the project's deletion until you remove the lien. This can be useful to protect projects of particular importance.

 <https://cloud.google.com/resource-manager/docs/project-liens>

#7

Steven has been asked to deploy a custom, home-grown application on a VM on GCP. This application collects data and stores it for review on a hard-coded S: drive, which must be local to the VM. Which storage option should Steven use to store the application's data?



VM-attachable persistent disk storage



Cloud Storage Nearline



Cloud Storage Coldline



None of the Above

Explanation

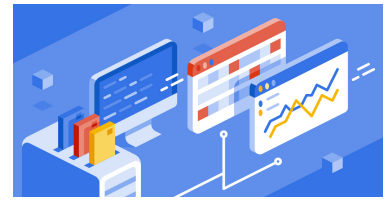
Google Cloud has five distinct offerings for simple storage without any concern for structure or database software.

As mentioned the first is VM-attachable persistent disk storage. This is analogous to Amazon EBS volumes. You can attach blocks of HDD or SSD storage to individual Compute Engine instances. This is a great solution if you're doing a monolithic app on a single server and need all of your data and possibly a database engine running on that instance. Two really nice features of persistent disk storage are zero-downtime scalability and automatic encryption. You get the piece of mind of knowing that your data is secure at rest and you can easily add more storage if needed without interrupting anything.

 <https://cloud.google.com/compute/docs/disks/>

Covered in this lecture

Introduction to Google Cloud Compute Options
Course: Planning and Configuring a Google Cloud Platform
Solution



9m



#8

What is the primary function of Google BigQuery?



Storing and querying massive datasets



Providing machine learning services



Implementing real-time messaging



Monitoring GCP resources

Explanation

Google BigQuery is an enterprise data warehouse tool that allows its customers to store and query massive datasets, a potentially time-consuming and expensive task.



<https://cloud.google.com/bigquery/what-is-bigquery>

#9

Jennifer is the cloud admin for the Blue Widget Corp. She has been asked to deploy a Kubernetes cluster so that the organization can perform some testing of a containerized app. After creating the cluster, her team begins testing. Thirty days later, Jennifer's team informs her the cluster appears to have been deleted. Nobody on the team has deleted the cluster. What is likely the cause of this?



Jennifer deployed a private cluster with a 30-day window



Jennifer deployed a zonal cluster



Jennifer deployed a dev cluster



Jennifer deployed an alpha cluster

Explanation

Alpha clusters expire after thirty days and do not receive security updates. You must migrate your data from alpha clusters before they expire. GKE does not automatically save data stored on alpha clusters.

 <https://cloud.google.com/kubernetes-engine/docs/concepts/alpha-clusters>

#10

Dana, the junior cloud admin, has been asked to deploy a virtual machine on the GCP platform. Which images below can Dana use to deploy her VM?



Public image



Custom image



Container image



None of these

Explanation

Dana can deploy a VM from a public, custom, or container image. There is no hybrid image option for Google. Hybrid refers to the multi-cloud infrastructure to deploy a single application system across multiple sites. These different sites could be different public clouds (multi-cloud) or a combination of public and on-premises data centers (hybrid cloud).

 <https://cloud.google.com/compute/docs/images>

Covered in this lecture

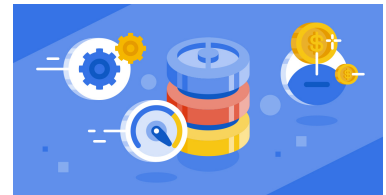
DEMO: Create and Assign an Instance Template

Course:Managing Networking and Compute Resources on Google Cloud Platform

3m



#11



Steve is a cloud admin at the Blue Widget Company. He's been asked to deploy a public-facing web application. Jen, who is Steve's manager, doesn't want to deploy any more hardware, infrastructure, or services than are absolutely necessary. Which service should Steve use to host the web application?



Compute Engine



App Engine



Kubernetes Engine



None of the Above

Explanation

tbd



<https://cloud.google.com/appengine>

#12

When you set the project using the "gcloud config" command, which of the following ways of referring to a project do you use?



Project Name



Project ID



Project Number



None of the choices are correct.

Explanation

To set the project property, run:

```
gcloud config set project PROJECT_ID
```

 <https://cloud.google.com/sdk/gcloud/reference/config/set>

#13

You've asked your junior admin to setup billing for a project you are planning in your Google Cloud Organization. However, your junior admin reports back that GCP will not allow her to setup the billing. Which primitive role definition below is the minimum necessary to setup billing for a project?

✗

roles/viewer

✗

roles/editor

✓

roles/owner

✗

roles/manager

Explanation

The roles/owner definition provides all editor permissions and permissions to manage roles and permissions for a project and all resources within the project, and to set up billing for a project.

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

#14

David is the cloud admin for Blue Widget Corp. He needs to stop the APP01 virtual machine instance to test his load balancer. Which command below should David use?

✗

```
gcloud compute stop APP01 --zone us --central1-a
```



`gcloud instances stop APP01 --zone us-central1-a`



`gcloud compute instances stop APP01 --zone us-central1-a`



`gcloud stop APP01 --zone us-central1-a`

Explanation

gcloud compute instances stop APP01 --zone us-central1-a allows you to stop the APP01 virtual machine.



<https://cloud.google.com/compute/docs/instances/stop-start-instance>

#15

The Blue Widget Corp website is visited by hundreds of thousands of users every month - from all over the world. The website is currently hosted on a single server. Steve has been asked to improve the response times for the website users while also reducing the load on the server hosting the website. Which solution below should Steve take advantage of?



Partner Interconnect



Traffic Director



Dedicated Interconnect



Cloud CDN

Explanation

When a user requests content from an HTTP(S) load balancer, the request arrives at a Google Front End (GFE), which is located at the edge of Google's network as close as possible to the user. If the load balancer's URL map routes traffic to a backend that has Cloud CDN configured, the GFE uses Cloud CDN in the following way:

- The GFE first looks in the Cloud CDN cache for a response to the user's request. If the GFE finds a cached response, the GFE sends the cached response to the user. This is called a *cache hit*.
- Otherwise, if the GFE can't find a cached response for the request, the GFE makes a request to the appropriate backend (the origin server). If the response to this request is cacheable, the GFE stores the response in the Cloud CDN cache so that the cache can be used for subsequent requests.

 <https://cloud.google.com/cdn/docs/overview>

#16

The Blue Widget Corporation needs to run a VM-based, mission-critical application continuously on Google Cloud Platform for one year. What is the most cost-effective way to accomplish this?



Deploy preemptible instances or spot VMs



Deploy custom virtual machines



Purchase committed use instances



Purchase sustained use instances

Explanation

Compute Engine offers the ability to purchase committed use contracts in return for deeply discounted prices for VM usage. These discounts are referred to as **committed use discounts**. These discounts reduce your costs by up to 70%.

Sustained use discounts are automatic discounts for running specific Compute Engine resources a significant portion of the billing month. These discounts reduce your costs by 20 - 30%.

Preemptible instances and spot VMs offer deep discounts, but Google can remove them with only 30 seconds' notice, so they're not suitable for mission-critical applications.

Custom virtual machines do not offer discounts.

 <https://cloud.google.com/compute/docs/instances/signing-up-committed-use-discounts>

#17

You are a member of your organization's Google Cloud Organization and you use the Organization node to manage resources. You've been asked to create a new billing account. To perform this task, you must also be a _____?



Billing Account Creator



Billing Account Operator



Billing Manager




Billing Account Manager

Explanation

Per Google:

"If you manage your Google Cloud resources using an Organization node, and you are a member of that Google Cloud Organization, then you must be a Billing Account Creator to create a new Cloud Billing Account."

 <https://cloud.google.com/billing/docs/how-to/manage-billing-account>

#18

Infrequently, the Blue Widget Corporation runs a number of very short-lived data processing jobs in Google Cloud Platform. These workloads take anywhere from a few minutes to an hour or so to run, and there is no concern about downtime if a job fails to complete due to VM failure. What type of Compute Engine instance would be the most cost-effective to recommend to the team for this work?



Preemptible Instance



Custom Machine



Committed Use Instance



Flexible App Engine Environment

Explanation

A preemptible VM is an instance that you can create and run at a much lower price than normal instances. However, Compute Engine might terminate (preempt) these instances if it requires access to those resources for other tasks. Preemptible instances are excess Compute Engine capacity, so their availability varies with usage.



<https://cloud.google.com/compute/docs/instances/preemptible>

#19

Regarding Cloud IAM, what type of role(s) are available?



Basic, predefined, and custom roles



User, service, and domain roles



Basic and curated roles



User, service, and custom roles

Explanation

Prior to Cloud IAM, you could only grant Owner, Editor, or Viewer roles to users. A wide range of services and resources now surface additional IAM roles out of the box. For example, the Cloud Pub/Sub service exposes Publisher and Subscriber roles in addition to the Owner, Editor, and Viewer roles.

There are several kinds of roles in IAM:

Basic roles: Roles historically available in the Google Cloud console. These roles are Owner, Editor, and Viewer.

Predefined roles: Roles that give finer-grained access control than the basic roles. For example, the predefined role Pub/Sub Publisher (roles/pubsub.publisher) provides access to only publish messages to a Pub/Sub topic.

Custom roles: Roles that you create to tailor permissions to the needs of your organization when predefined roles don't meet your needs.

 <https://cloud.google.com/iam/docs/overview>

#20

Which type of account would you use in code when you want to interact with Google Cloud services?



Service account



Google account



Google group



Code account

Explanation

A service account is an account that belongs to your application instead of to an individual end user. When you run code that is hosted on Cloud Platform, you specify the account that the code should run as. You can create as many service accounts as needed to represent the different logical components of your application.

 <https://cloud.google.com/iam/docs/overview>

Covered in this lecture

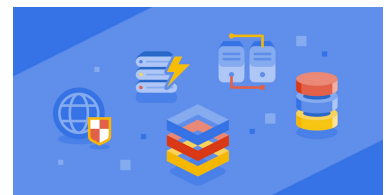
Service Accounts

Course: Designing a Google Cloud Infrastructure

4m



#21



Which of the following statements about traffic splitting in App Engine is TRUE?



Distributes a percentage of traffic to versions of your application



You can split traffic to move 100% of traffic to a single version or to route percentages of traffic to multiple versions



All of the Above



None of the Above

Explanation

Traffic splitting distributes a percentage of traffic to versions of your application. You can split traffic to move 100% of traffic to a single version or to route percentages of traffic to multiple versions. Splitting traffic to two or more versions allows you to conduct A/B testing between your versions and provides control over the pace when rolling out features.



<https://cloud.google.com/appengine/docs/admin-api/migrating-splitting-traffic>

#22

When using Google BigQuery, roughly how much data would you need to process in queries per month to qualify for the flat-rate pricing?



Any amount - flat-rate pricing is flexible per account



500 terabytes per month



At least a petabyte per month



Multiple petabytes per month

Explanation

Without getting bogged down in details, you would need to query petabytes worth of data per month to qualify for flat-rate pricing. BigQuery charges a half-cent per GB of data processed (\$0.005). At the time this course was created, you needed to process over \$10,000 of data, (which equals 2 petabytes) and now the minimum amount has changed to \$40,000 (or 8 petabytes.)

The minimum rate is very likely to change over time, but the point is you need to be processing LARGE AMOUNTS of data per month to qualify.

 <https://cloud.google.com/bigquery/pricing#storage>

Covered in this lecture

Pricing

Course: Introduction to Google BigQuery

2m



#23



To use load balancing and protocol forwarding, you must create a forwarding rule that directs traffic to specific _____ that contain instances from multiple zones.



priority pools



target pools



source pools



resource groups

Explanation

In Google Compute Engine, forwarding rules work in conjunction with target pools and target instances to support load balancing and protocol forwarding features. To use load balancing and protocol forwarding, the user must create a forwarding rule that directs traffic to specific target pools (for load balancing) or target instances (for protocol forwarding). It is not possible to use either of these features without a forwarding rule.

<https://cloud.google.com/compute/docs/protocol-forwarding/>

Covered in this lecture

Load Balancer

Course:Google Cloud Platform: Systems Operations

7m



#24



As the GCP admin in your organization, you need to perform some tasks using the Google Cloud SDK, using your Windows 10 workstation. To begin using the SDK on your workstation, you've created a Google Cloud Platform project, downloaded the Google Cloud SDK installer, and completed the installation. At this point, you need to initialize the SDK. Which command do you use to complete this task?



initialize gcloud



gcloud init



gcloud start



start gcloud

Explanation

To begin using the SDK on a local Windows workstation, you must first create a Google Cloud Platform project, if you don't have one already. You then need to download the Google Cloud SDK installer and complete the installation.

After the installation completes, you must initialize the SDK, using the *gcloud init* command.

<https://cloud.google.com/sdk/docs/quickstart-windows>

#25

After an incident at Blue Widget Corp, where a user deleted some resources accidentally, corporate leaders are now demanding that users only have the exact access and management privileges that they need. What tool (or service) will allow Steve, as the administrator, enforce this doctrine of "least privilege"?



Role-Based Access Control



GCP Cloud Identity and Access Management



Assigning Liens



GCP Trust and Security

Explanation

Using Cloud Identity and Access Management (IAM), you can follow the principle of least privilege and limit the permissions granted to any particular user to the minimum necessary.

 <https://cloud.google.com/iam/docs/overview>

#26

Which statement regarding Cloud IAM primitive roles is incorrect?



Primitive roles are concentric.



There are three primitive roles: viewer, editor, and owner.



The most permissive primitive role is the owner role, which allows you to invite project members and delete projects.



Primitive roles can be assigned to Google accounts, service accounts, and Google App domains.

Explanation

Three roles existed before the introduction of Cloud IAM: Owner, Editor, and Viewer. These roles are concentric; that is, the Owner role includes the permissions in the Editor role, and the Editor role includes the permissions in the Viewer role.

Predefined roles can be assigned to Google accounts, service accounts, and Google App domains. Primitive roles are for users only.

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

#27

When setting up a domain with Cloud DNS, what steps are recommended? (Choose 2 answers)



Avoid registering parent domains that are not hosted on Cloud DNS.



Register the parent domain first, then create records for any subdomains.



If subdomains will be hosted on Cloud DNS but parent domains will not, then register the parent domains anyhow.



Register the parent domain only - subdomain records are not required.

Explanation

If you have a domain with subdomains, register the parent domain first, then create records for any subdomains. Even if you do not host the parent domain with Cloud DNS, it is better to register the parent domain anyway. If you change your mind later and want to migrate the parent domain to Cloud DNS, the process is more robust if the parent domain is already in place.

 https://cloud.google.com/dns/overview#cloud_dns_concepts

#28

Which of the following practices can help you develop more secure software? (Select 3 answers.)



Peer review of code



Integrating static code analysis tools into your CI/CD pipeline



Penetration tests



Encrypting your source code

Explanation

There are four basic techniques for analyzing the security of a software application - automated scanning, manual penetration testing, static analysis, and manual code review.

Despite the many claims that code review is too expensive or time-consuming, there is no question that it is the fastest and most accurate way to find and diagnose many security problems. There are also dozens of serious security problems that simply can't be found any other way.

Encrypting your source code might help with keeping it out of the hands of hackers, but it won't help you develop more secure software.



[https://www.owasp.org/images/2/2e/OWASP Code Review Guide-V1 1.pdf](https://www.owasp.org/images/2/2e/OWASP_Code_Review_Guide-V1_1.pdf)

Covered in this lecture

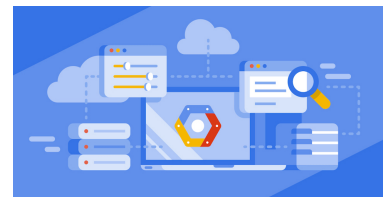
Testing

Course: Managing Your Google Cloud Infrastructure

3m



#29



Steve has been asked to deploy a virtual machine with a custom configuration. He has been asked to deploy a VM with 4 virtual CPUs and 6GB of RAM. Which gcloud command below will successfully create this custom VM?



`gcloud instances create vm01 --custom-cpu 4 --custom-memory 6`



`gcloud compute instances create vm01 --custom-cpu 4 --custom-memory 6`



`gcloud instances create vm01 -custom-cpu 4 -custom-memory 6`



gcloud compute instances create vm01 -custom-cpu 4 -custom-memory 6

Explanation

gcloud compute instances create facilitates the creation of Google Compute Engine virtual machines. The switches require "--" delimiters.

 <https://cloud.google.com/sdk/gcloud/reference/compute/instances/create>

#30

Dave has been tasked with migrating the organization's MongoDB data to a managed document database service in Google Cloud Platform. Which GCP storage product will be most relevant to Dave's needs?

✗

BigQuery

✗

CloudSpanner

✗

Memorystore

✓

Firestore

Explanation

Cloud Firestore is a flexible, scalable, realtime database. It's simple enough for rapid prototyping yet scalable and flexible enough to grow with you to any size.

Cloud Firestore is a realtime database, meaning that clients can listen to data in Cloud Firestore and be notified in real time as it changes. This feature lets you build responsive apps that work regardless of network latency or Internet connectivity.

Cloud Firestore is a cloud-hosted NoSQL database. You store data in *documents*, which contain fields mapping to values. These documents are stored in *collections*, which are simply containers that help you organize and query your documents.

 <https://cloud.google.com/firestore/docs/concepts>

#31

Google App Engine has a second hosting option, called App Engine Flexible Environment. Which of the following best describes App Engine Flexible Environment?



The Flexible Environment supports App Engine applications on configurable Compute Engine instances.



The Flexible Environment supports App Engine instances on third-party networks.



The Flexible Environment supports applications on configurable GKE containers.



The Flexible Environment supports managed functions as well as managed instances.

Explanation

Google App Engine has a second hosting option, the flexible environment, which has the following attributes:

- The flexible environment lets you run App Engine applications on configurable Compute Engine Virtual Machines (VMs)
- This VM hosting environment offers more flexibility and provides more CPU and memory options.

 <https://cloud.google.com/appengine/docs/flexible/>

#32

A 5 TB persistent disk is attached to a standard Compute Engine instance. Currently, 2 TB of the total storage is used. The user took an initial snapshot yesterday, and 250 GB of the 2 TB now stored is new or updated data since that snapshot was taken. If the user creates a second snapshot of the instance disk now, approximately how large will the snapshot be (do not take snapshot data compression into account)?



250 GB



2 TB



2.25 TB

✗

5TB

Explanation

Persistent disk snapshots are only charged for the total size of the snapshot. For example, if only 2TB of disk space is used on a 5TB persistent disk, the snapshot size will be around 2TB, rather than the full 5TB of provisioned disk space.

Additionally, snapshots are updated incrementally. If the user took a snapshot yesterday, and only 250 GB of data is new or updated since that snapshot was taken, this means the current snapshot will be roughly 250 GB.

 <https://cloud.google.com/compute/docs/disks/create-snapshots#before-you-begin>

#33

Brian is the cloud admin for the Blue Widget Company. He needs to upload a file, called "FinanceReport.xls", from his workstation to GCP. The file needs to be uploaded to a bucket, called "financereports", in Cloud Storage. Which command below will allow Brian to upload the file?

✓

`gsutil cp desktop/FinanceReport.xls gs://financereports/`

✗

`gsutil cp desktop/FinanceReport.xls g://financereports/`

✗

`gsupload cp desktop/FinanceReport.xls gs://financereports/`

✗

`gsutil desktop/FinanceReport.xls financereports`

Explanation

`gsutil cp desktop/FinanceReport.xls gs://financereports/` is the correct command

 <https://cloud.google.com/storage/docs/gsutil>

#34

Mike is a new cloud admin. He's been asked to stop one of two Windows VMs that are running a load balanced application in order to confirm that the load balancer is working. Which of the following will not be retained when Mike stops the VM instance?



Application State



Configured Persistent Disks



Internal IP



MAC Address

Explanation

Configured Persistent Disks will persist after terminating a VM. The internal IP and MAC address will as well. The application state, however, will not persist once the VM is powered off.



<https://cloud.google.com/compute/docs/instances/stop-start-instance>

#35

David is the cloud admin for Blue Widget Corp. He has deployed a Linux VM called Linux01, and he needs to SSH to it from the console. Which command should David use to SSH to the VM?



`gcloud ssh --project blue-widget-project --zone us-central1-a Linux01`



`gcloud compute ssh --project blue-widget-project --zone us-central1-a Linux01`



`gcloud connect ssh --project blue-widget-project --zone us-central1-a Linux01`



`gcloud compute ssh -project blue-widget-project -zone us-central1-a Linux01`

Explanation

gcloud compute ssh --project blue-widget-project --zone us-central1-a Linux01 allows you to SSH to the Linux01 server.

 <https://cloud.google.com/sdk/gcloud/reference/compute/ssh>

#36

Jennifer is the cloud admin for Blue Widget Corp. She has been asked to build out a cloud application in GCP that leverages the serverless architecture model. Which GCP service will be of most interest to her?



Compute Engine



Kubernetes Engine



App Engine



Direct Peering

Explanation

The App Engine standard environment makes it easy to build and deploy an application that runs reliably even under heavy load and with large amounts of data.

Applications run in a secure, sandboxed environment, allowing the App Engine standard environment to distribute requests across multiple servers, and scaling servers to meet traffic demands. Your application runs within its own secure, reliable environment that is independent of the hardware, operating system, or physical location of the server.

 <https://cloud.google.com/appengine>

#37

Which of the following accurately describes Google Cloud Platform's multi-region product availability?



GCP globally is divided into zones that map to continents. Each zone has multiple regions that constitute individual data centers in specific countries.



GCP globally is divided into regions that map to continents. Each region has multiple zones that constitute individual data centers in specific countries.



GCP zones are locations within a country. Individual countries can have multiple zones. Zones are then broken into regions which represent a specific set of hardware within a data center.



GCP regions are specific geographical locations. Individual countries can have multiple regions. Regions are then broken into zones that represent a specific set of hardware within a data center.

Explanation

Regions are independent geographic areas that consist of *zones*. Locations within regions tend to have round-trip network latencies of under <1ms on the 95th percentile.

A *zone* is a deployment area for Google Cloud resources within a region. Zones should be considered a single failure domain within a region. To deploy fault-tolerant applications with high availability and help protect against unexpected failures, deploy your applications across multiple zones in a region.

 <https://cloud.google.com/about/locations/>

#38

Laurie, the cloud admin at Blue Widget Corp, has been asked to build a VPC network in GCP. This VPC network will be connected to the on-prem network via the Cloud VPN service. The address space for the on-prem network spans the CIDR block of 10.128.0.0/9. After deploying the VPC network, Laurie finds that there are issues with the VPN connectivity. What could be causing the VPN connectivity issues?



Laurie deployed an Auto Mode VPC Network



Laurie deployed a Custom Mode VPC Network



The Cloud VPN service doesn't allow you to connect a VPC to an on-prem network



None of the Above

Explanation

When configuring your network, please be advised of the following note from GPC documentation:

If your VPC network is connected to an on-premises network by using Cloud VPN or Cloud Interconnect, check that subnet ranges do not conflict with on-premises IP addresses. Subnet routes are prioritized first so traffic to the destination range remains in your VPC network, even though it might have been intended for the on-premises network.



<https://cloud.google.com/vpc/docs/vpc>

#39

Which GCP service below provides a direct physical connection between your GCP environment and your on-premises network using GCP network co-locations?



Cloud VPN



Carrier Peering



Dedicated Interconnect



Partner Interconnect

Explanation

Cloud Interconnect provides low latency, highly available connections that enable you to reliably transfer data between your on-premises and Virtual Private Cloud networks. Also, Cloud Interconnect connections provide RFC 1918 communication, which means internal (private) IP addresses are directly accessible from both networks.

Cloud Interconnect offers two options for extending your on-premises network. Google Cloud Interconnect - Dedicated (Dedicated Interconnect) provides a direct physical connection between your on-premises network and Google's network. Google Cloud Interconnect - Partner (Partner Interconnect) provides connectivity between your on-premises and GCP VPC networks through a supported service provider.

Cloud Interconnect provides low latency, highly available connections that enable you to reliably transfer data between your on-premises and Virtual Private Cloud networks. Also, Cloud Interconnect connections provide RFC 1918 communication, which means internal (private) IP addresses are directly accessible from both networks.

Cloud Interconnect offers two options for extending your on-premises network. Google Cloud Interconnect - Dedicated (Dedicated Interconnect) provides a direct physical connection between your on-premises network and Google's network. Google Cloud Interconnect - Partner (Partner Interconnect) provides connectivity between your on-premises and GCP VPC networks through a supported service provider.

 <https://cloud.google.com/interconnect/docs/concepts/overview>

#40

How does Google Compute Engine match certain types of traffic and forward it to a load balancer?



By using forwarding rules



By using target pools



By performing health checks



By using routing tables

Explanation

Google Compute Engine load balancing uses forwarding rule resources. These forwarding rule resources match certain types of traffic and forward it to a load balancer. For example, a forwarding rule can match TCP traffic destined to port 80 on IP address 192.0.2.1, then forward it to a load balancer, which then directs it to healthy virtual machine instances.

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

Covered in this lecture

Course Intro

Course: Deploying Networking and Compute Resources on Google Cloud Platform

3m



#41

Google Compute Engine offers _____ to distribute incoming network traffic across multiple virtual machine instances.



Load balancing



Firewall



Route



Static IP address

Explanation

Google Compute Engine offers server-side load balancing to distribute incoming network traffic across multiple virtual machine instances. Load balancing is useful because it helps the user support heavy traffic and provides redundancy to avoid failures.

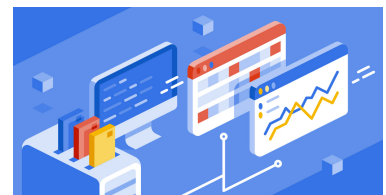
 <https://developers.google.com/compute/docs/load-balancing/>

Covered in this lecture

Planning Network Resources Demo

Course: Planning and Configuring a Google Cloud Platform

Solution



8m



#42

Which statement regarding the cost of querying with Google BigQuery is correct?



BigQuery charges for processing the data in queries and for reading it.



Querying data stored within BigQuery is less expensive than querying data stored outside of it, such as in Cloud Storage.



You are not charged for querying data that is cached within BigQuery.



The first 10 TB of data queries per month are free.

Explanation

The only correct statement below is that you are not charged for querying data that is cached within BigQuery. What qualifies as cached data in BigQuery, and how to query it specifically, is a little trickier.

Data will be cached in BigQuery if you don't specify a destination table. It puts the results in a temporary table in cache. This temporary table stays in cache for about a day. So if you run the query again within 24 hours, it'll retrieve the cached copy; and you won't be charged for the query. You will query the cached data only if you run a query again and **do not specify** a destination table. Otherwise, it will not read the data from cache, and you will be charged.

This may seem like frivolous information, but if you are querying a large amount of data, and the query should fail for some reason, you may want to know how to rerun the query without having to pay for it a second time.

 <https://cloud.google.com/bigquery/pricing#queries>

#43

Cindy is the cloud admin for Blue Widget Corp. She has been tasked with deploying a basic internal-facing IIS website that she will use to post staff updates. She also wants to load balance the website, since there are thousands of employees that will be accessing the backend on a daily basis. Which type of load balancer should Cindy deploy?



Regional Network TCP/UDP load balancer



Global TCP proxy load balancer



Internal HTTP(s) load balancer



Regional SSL proxy load balancer

Explanation

The Internal TCP/UDP and Internal HTTP(S) load balancers are comparable to their global external counterparts. They handle the same basic use cases - one is meant for TCP/UDP traffic, and the other for HTTP(S) requests - only they are situated within a private network; they cannot accept requests direct from the public internet.



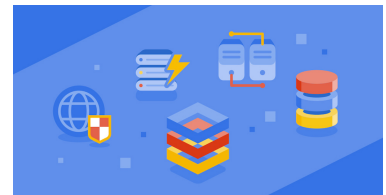
<https://cloud.google.com/load-balancing/docs/choosing-load-balancer>

Covered in this lecture

Deploying a containerized app to GKE Cluster

Course: Deploying and Implementing Google Cloud Platform

Solutions



5m



#44

Michael is the cloud administrator for the Blue Widget Company. He has been asked to protect his organization's public-facing web application from DDoS attacks. Which service should Michael take advantage of?



Traffic Manager



Traffic Director



Cloud Armor



DDoS Shield

Explanation

Use Google Cloud Armor security policies to protect your load-balanced services. Google Cloud Armor security policies are made up of rules that filter traffic based on layer 3, 4, and 7 attributes. For example, you can specify conditions that match on an incoming request's IP address, IP range, country code, or request headers.

 <https://cloud.google.com/armor/docs/security-policy-concepts>

#45

You have deployed several VMs within a Google Cloud VPC, but are considering implementing Cloud Armor for additional security. What additional security does Cloud Armor provide, in addition to your VPC's instance firewalls?

✗

Cloud Armor requires additional authentication to process requests.

✗

Cloud Armor offers additional request data packet encryption for data in transit.

✓

Cloud Armor analyzes requests at a secure perimeter outside your VPC.

✗


Cloud Armor provides a private network connection, to avoid sending packets over the public internet

Explanation

GCP HTTP(S) Load Balancing is implemented at the edge of Google's network in Google's points of presence around the world. User traffic directed to an HTTP(S) load balancer enters the POP closest to the user and is then load balanced over Google's global network to the closest backend that has sufficient capacity available.

IP deny lists/allow lists enable you to restrict or allow access to your HTTP(S) load balancer at the edge of the Google Cloud, as close as possible to the user and to malicious traffic. This prevents malicious users or traffic from consuming resources or entering your virtual private cloud (VPC) networks.

The following diagram illustrates the location of the HTTP(S) load balancers, the Google network, and Google data centers.

 https://cloud.google.com/armor/docs/security-policy-concepts#ip_address_allow_list_and_deny_list_rules_in_a_security_policy

#46

Steve is the cloud admin for Blue Widget Corp. He has been asked to configure a Kubernetes-hosted app so that it can be accessed internally by the GKE cluster. It will NOT be accessed from the public internet. Which service is suitable for exposing an internal IP address for

apps that do not need to be accessed from the public internet?



NodePort



ClusterIP



LoadBalancer



ExternalName

Explanation

ClusterIP services expose an internal IP address for apps that do not need to be accessed from the public internet. NodePort services expose the node's IP address on a specific port. LoadBalancer and ExternalName services both work closely with your cloud provider. The former works with your provider's load balancer resources to expose a set of pods while the latter returns a CNAME record based a DNS name of your choosing.

 <https://cloud.google.com/kubernetes-engine/docs/concepts/service>

Covered in this lecture

Kubernetes Concepts

Course:Managing Google Kubernetes Engine and App Engine

7m



#47



Dave is a junior cloud admin at the Blue Widget Corp. He's been asked to review the logs to identify which user created the APP01 virtual machine in GCP. Which audit log should Dave review?



data access logs



system events logs



admin activity logs



None of the Above

Explanation

Admin Activity audit logs contain log entries for API calls or other administrative actions that modify the configuration or metadata of resources. For example, these logs record when users create VM instances or change Cloud Identity and Access Management permissions.

 <https://cloud.google.com/logging/docs/audit/>

#48

Cloud Key Management Service (KMS) generates encryption keys which you can use, rotate and then destroy. There are four specific key states for KMS keys: Enabled Disabled Scheduled for destruction Destroyed. Keys in several stages can change from one state to another, but at which state(s) can a key no longer be returned to an "enabled" state?



Disabled



Scheduled for destruction



Destroyed



Both scheduled for destruction and destroyed

Explanation

The following describes how a key version can change states:

A key version can move from enabled to disabled and from disabled to enabled. A key version which is enabled or disabled can move to scheduled for destruction. A key version which is scheduled for destruction can move to disabled. However, once a key is destroyed, it cannot return to a previous key state.

 <https://cloud.google.com/kms/docs/key-states>

#49

Which of the following is not an IAM best practice?



Use primitive roles by default



Grant roles at the smallest scope needed



Restrict who has access to create and manage service accounts in your project



Treat each component of your application as a separate trust boundary

Explanation

- Treat each component of your application as a separate trust boundary. If you have multiple services that requires different permissions, create a separate service account for each of the services so that they can be permissioned differently.
- Grant primitive roles in the following cases:
 - when the Cloud Platform service does not provide a predefined role. See the predefined roles table for a list of all available predefined roles.
 - when you want to grant broader permissions for a project. This often happens when you're granting permissions in development or test environments.
 - when you need to allow a member to modify permissions for a project, you'll want to grant them the owner role because only owners have the permission to grant access to other users for for projects.
 - when you work in a small team where the team members don't need granular permissions.
- Remember that a policy set on a child resource cannot restrict access granted on its parent. Check the policy granted on every resource and make sure you understand the hierarchical inheritance.
- Grant roles at the smallest scope needed. For example, if a user only needs access to publish Pub/Sub topic, grant the Publisher role to the user for that topic.
- Restrict who can act as service accounts. Users who are granted the Service Account Actor role for a service account can access all the resources for which the service account has access. Therefore be cautious when granting the Service Account Actor role to a user.
- Restrict who has access to create and manage service accounts in your project.

- Granting owner role to a member will allow them to modify the IAM policy. Therefore grant the owner role only if the member has a legitimate purpose to manage the IAM policy. This is because as your policy contains sensitive access control data and having a minimal set of users manage it will simplify any auditing that you may have to do.

 <https://cloud.google.com/iam/docs/using-iam-securely>

Covered in this lecture

DEMO: Requesting an Increase in Quota

Course: Deploying Networking and Compute Resources on Google Cloud Platform



3m



#50

Steven has been asked to provision storage for archival purposes. The data that is archived will be accessed no more than once quarterly. Which type of storage should Steven provision?



VM-attachable persistent disk storage



Cloud Storage Nearline



Cloud Storage Coldline



None of the Above

Explanation

Coldline Storage is a very-low-cost, highly durable storage service for storing infrequently accessed data. Coldline Storage is a better choice than Standard Storage or Nearline Storage in scenarios where slightly lower availability, a 90-day minimum storage duration, and higher costs for data access are acceptable trade-offs for lowered at-rest storage costs.

Coldline Storage is ideal for data you plan to read or modify at most once a quarter. Note, however, that for data being kept entirely for backup or archiving purposes, Archive Storage is more cost-effective, as it offers the lowest storage costs.

 <https://cloud.google.com/storage/docs/storage-classes>

