Exam Session - Knowledge Check: Designing a Google Cloud Infrastructure

cloudacademy.com/quiz/exam/3761971/results

#1

Which Google Cloud Platform service requires the least management because it takes care of the underlying infrastructure for you?

✓

App Engine

✗

Cloud Engine

✗

Container Engine

✗

Docker containers running on Cloud Engine

Explanation

App Engine is great for running web-based apps, line of business apps, and mobile backends. Compute Engine is great for when you need more control of the underlying infrastructure.

Container Engine is in between because it gives you control of the containers running on top of Compute Engine.

🔗

https://cloud.google.com/compute/docs/faq#how_do_google_app_engine_and_product_name_relate_to_each_other

#2

To set up a virtual private network between your office network and Google Cloud Platform and have the routes automatically updated when the network topology changes, what is the minimal number of each type of component you need to implement?

✓

1 Cloud VPN Gateway, 1 Peer Gateway, and 1 Cloud Router

✗

2 Cloud VPN Gateways and 1 Peer Gateway

✗

2 Peer Gateways and 1 Cloud Router

✗

2 Cloud VPN Gateways and 1 Cloud Router

Explanation

VPC networks allow you to regionally segment the network IP space into prefixes (subnets) and control which prefix a VM instance's internal IP address is allocated from. If you want to avoid statically managing these subnets, including the burden of adding and removing related static routes for your VPN, you can do so by enabling dynamic routing for your VPNs using Cloud Router.

The diagram at https://cloud.google.com/compute/images/cloudrouter/cr-w-subnets.svg shows a VPN Gateway, a Peer Gateway, and a Cloud Router.

https://cloud.google.com/compute/docs/cloudrouter#cloud_router_for_vpns_with_vpc_networks
Covered in this lecture
Networks
Course:Designing a Google Cloud Infrastructure

11m

#3

Which of these is not a recommended method of authenticating an application with a Google Cloud service?

✗

Use one of the Google Cloud Client Libraries.

✗

Request an OAuth2 access token and use it directly.

✓

Embed the service account's credentials in the application's source code.

✕

Use the gcloud and/or gsutil commands.

Explanation

Do not embed secrets related to authentication in source code, such as API keys, OAuth tokens, and service account credentials.

Authenticating applications using service account credentials

Client libraries can use Application Default Credentials to authenticate with Google APIs and send requests to those APIs.

For some applications, you might need to request an OAuth2 access token and use it directly without going through a client library or using the `gcloud` or `gsutil` tools.

Some applications might use commands from the `gcloud` and `gsutil` tools, which are included by default in most Compute Engine images. These tools automatically recognize an instance's service account and relevant permissions granted to the service account.

🔗https://cloud.google.com/docs/authentication#token_lifecycle_management

#4

Which of the following statements about encryption on GCP is not true?

✕

Google Cloud Platform encrypts customer data stored at rest by default.

✕

Data in Google Cloud Platform is broken into subfile chunks for storage, and each chunk is encrypted at the storage level with an individual encryption key.

✓

If you want to manage your own encryption keys for data on Google Cloud Storage, the only option is Customer-Managed Encryption Keys (CMEK) using Cloud KMS.

✕

Each encryption key is itself encrypted with a set of master keys.

Explanation

There are 3 ways to manage your own encryption keys when using Google :

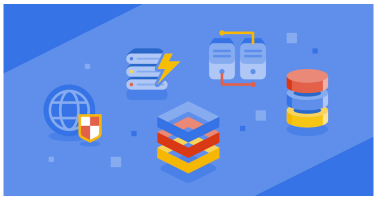
- Customer-managed encryption keys (CMEK) using Cloud KMS allow you to manage your own keys that are hosted on GCP.
- Customer-supplied encryption keys (CSEK) allow you to manage your own keys on premise, but still use them on GCP.
- With client-side encryption, you encrypt the data before you send it to GCP.

Google Cloud Platform encrypts customer data stored at rest by default, with no additional action required from you.

Data in Google Cloud Platform is broken into subfile chunks for storage, and each chunk is encrypted at the storage level with an individual encryption key. The key used to encrypt the data in a chunk is called a data encryption key (DEK). Because of the high volume of keys at Google, and the need for low latency and high availability, these keys are stored near the data that they encrypt. The DEKs are encrypted with (or “wrapped” by) a key encryption key (KEK). Customers can choose which key management solution they prefer for managing the KEKs that protect the DEKs that protect their data.

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

Covered in this lecture
Data Protection and Encryption
Course:Designing a Google Cloud Infrastructure



7m

#5

Which of these statements about Microsoft licenses is true?

✗

You can migrate your existing Microsoft Windows and Microsoft application licenses to Compute Engine instances.

✗

You can migrate your existing Microsoft Windows licenses to Compute Engine instances, but not your Microsoft application licenses.

✓

You can migrate your existing Microsoft application licenses to Compute Engine instances, but not your Microsoft Windows licenses.

✗

You cannot migrate your existing Microsoft Windows or Microsoft application licenses to Compute Engine instances.

Explanation

You cannot migrate your existing Windows Server licenses to Compute Engine, but you can bring your existing Microsoft Application Licenses to your Windows Server instances to run specific applications.

🔗

https://cloud.google.com/compute/docs/instances/windows/#licensing_for_windows_server_images

#6

Which is the fastest instance storage option that will still be available when an instance is stopped?

✓

SSD Persistent Disk

✗

Local SSD

✗

RAM disk

✗

Standard Persistent Disk

Explanation

Local SSDs and RAM disks disappear when you stop an instance. Standard Persistent Disks and SSD Persistent Disks both survive when you stop an instance, but SSD Persistent Disks have up to 4 times the throughput and up to 40 times the I/O operations per second of a Standard Persistent Disk.

🔗https://cloud.google.com/compute/docs/disks/

#7

Which database service requires that you configure a failover replica to make it highly available?

✕

Cloud Datastore

✓

Cloud SQL

✕

Cloud Spanner

✕

BigQuery

Explanation

Cloud Datastore, Cloud Spanner, and BigQuery are all horizontally scalable and are automatically replicated to multiple zones. Since Cloud SQL is not horizontally scalable, you must configure a failover replica to make it highly available.

https://cloud.google.com/sql/docs/mysql/configure-ha

Covered in this lecture

High Availability

Course:Designing a Google Cloud Infrastructure

6m

#8

Which database service(s) support standard SQL queries?

✕

Cloud SQL

✕

Cloud SQL and Cloud Datastore

✕

Cloud Bigtable and Cloud SQL

✓

Cloud Spanner and Cloud SQL

Explanation

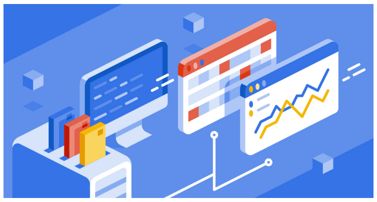
Cloud SQL is a managed service for MySQL and PostgreSQL, which both support SQL queries. Cloud Spanner supports SQL queries. Cloud Bigtable and Cloud Datastore are NoSQL databases.

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

Covered in this lecture

GCP Overview

Course:Overview of Google Cloud Platform



8m

#9

If you do not grant a user named Bob permission to access a Cloud Storage bucket, but then use an ACL to grant access to an object inside that bucket to Bob, what will happen?

✗

Bob will not be able to access the object because he does not have access to the bucket.

✗

Bob will be able to access all of the objects inside the bucket because he was granted access to at least one object in the bucket.

✗

It is not possible to grant access to an object when it is inside a bucket for which a user does not have access.

✓

Bob will be able to access the object because bucket and object ACLs are independent of each other.

Explanation

Bucket and object ACLs are independent of each other, which means that the ACLs on a bucket do not affect the ACLs on objects inside that bucket. It is possible for a user without permissions for a bucket to have permissions for an object inside the bucket. For example, you can create a bucket such that only GroupA is granted permission to list the objects in the bucket, but then upload an object into that bucket that allows GroupB `READ` access to the object. GroupB will be able to read the object, but will not be able to view the contents of the bucket or perform bucket-related tasks.

https://cloud.google.com/storage/docs/best-practices#security

#10

What are two different features that fully isolate groups of VM instances?

✗

Networks and subnetworks

✗

Subnetworks and projects

✓

Projects and networks

✗

Firewall rules and subnetworks

Explanation

Google uses software-defined networking that enables you to subject every packet to security checks, thereby enabling complete isolation of Cloud Platform projects.

Networks within projects are used to isolate groups of VM instances.

Subnetworks on Compute Engine enable you to control the address space in which VM instances are created, while maintaining the ability to route between them.

Firewall rules only restrict incoming network traffic. They cannot restrict outgoing network traffic.

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

#11

Which statement about IP address pricing in Google Cloud is correct?

✗

You are charged for static external IP addresses, but not ephemeral external IP addresses.

✗

You are charged for both internal and external IP addresses.

✓

An unused static external IP address cost more than a **used** static external IP address.

✗

External IP addresses are more expensive for **preemptible VMs** than for **Standard VMs**.

Explanation

Three of the choices above are incorrect. Let's review:

- One choice reads "You are charged for static external IP addresses, but not ephemeral external IP addresses." This is incorrect. Google Cloud charges for both static and ephemeral external IP addresses
- A second choice reads "External IP addresses are more expensive for **preemptible VMs** than for **Standard VMs**." This is incorrect. External IP addresses are more expensive for Standard VMs. They cost twice as much as external IP addresses for Preemptible VMs.
- A third choice reads " You are charged for both internal and external IP addresses." This is also incorrect. Users are charged for external IP addresses, but not internal IP addresses.

The one correct statement is "**An unused** static external IP address cost more than a **used** static external IP address." To quote GCP documentation directly, *Google Cloud considers a static external IP address as in use if it is associated with a VM instance whether the instance is running or stopped. If the instance is deleted or if the IP address is dissociated from the instance, Google Cloud considers the static IP address as not in use.*

https://cloud.google.com/vpc/network-pricing#ipaddress

#12

To ensure that your application will handle the load even if an entire zone fails, what should you do? (Choose the best answer.)

✓

Overprovision your regional managed instance group by at least 50%.

✗

Spread your managed instance group over two zones and overprovision by 100%.

✗

Don't select the "Multizone" option when creating your managed instance group.

✗

Create a regional unmanaged instance group and spread your instances across multiple zones.

Explanation

To account for the extreme case where one zone fails or an entire group of instances stops responding, Compute Engine strongly recommends overprovisioning your managed instance group by at least 50%. Spreading instances across three zones already helps you preserve at least 2/3 of your serving capacity and the other two zones in the region can continue to serve traffic without interruption. By overprovisioning to 150%, you can ensure that if 1/3 of the capacity is lost, 100% of traffic is supported by the remaining zones.

You need to select the "Multizone" option (or the --region flag if you're using the gcloud command) when creating a managed instance group.

It is only possible to create regional managed instance groups. You cannot create regional unmanaged instance groups.

https://cloud.google.com/compute/docs/instance-groups/distributing-instances-with-regional-instance-groups#provisioning_the_correct_managed_instance_group_size
#13

Which of the following would not reduce your recovery time in the event of a disaster?

✗

Replace your warm standby server with a hot standby server.

✓

Replace your active/active hybrid production environment (on-premises and GCP) with a warm standby server.

✗

Use a highly preconfigured machine image for deploying new instances.

✗

Make it as easy as possible to adjust the DNS record to cut over to your warm standby server.

Explanation

An active/active hybrid production environment (on-premises and GCP) can continue running in the event that either the on-premises environment or the GCP deployment fails, so its recovery time would be zero. A warm standby server requires a manual DNS adjustment, so it will always take some time to recover. Making it easier to do the DNS adjustment will reduce the recovery time for the warm standby model, though.

A hot standby server automatically fails over in the event that the main instance becomes unhealthy, so it has a lower recovery time than a warm standby server, which requires a manual failover.

Typically, the smaller your RTO (Recovery Time Objective) is, the more preconfigured you will want your image to be.

🔗https://cloud.google.com/solutions/disaster-recovery-cookbook

#14

Which of the following is not a best practice for mitigating Denial of Service attacks on your Google Cloud infrastructure?

✗

Reduce the attack surface for your GCE deployment

✗

Scale to absorb the attack

✗

Isolate your internal traffic from the external world

✓

Block SYN floods using Cloud Router

Explanation

These are all best practices for mitigating Denial of Service attacks:

- Reduce the attack surface for your GCE deployment
- Scale to absorb the attack
- Isolate your internal traffic from the external world

Cloud Router is used to dynamically update VPN routes. It cannot block SYN floods. On the other hand, Google's Frontend infrastructure, which terminates user traffic, automatically scales to absorb certain types of attacks (e.g., SYN floods) before they reach your compute instances.

https://cloud.google.com/files/GCPDDoSprotection-04122016.pdf