

 Custom View Settings

## Topic 1 - Single Topic

Question #1

Topic 1

You want to upload files from an on-premises virtual machine to Google Cloud Storage as part of a data migration. These files will be consumed by Cloud

DataProc Hadoop cluster in a GCP environment.

Which command should you use?

- A. gsutil cp [LOCAL\_OBJECT] gs://[DESTINATION\_BUCKET\_NAME]/
- B. gcloud cp [LOCAL\_OBJECT] gs://[DESTINATION\_BUCKET\_NAME]/
- C. hadoop fs cp [LOCAL\_OBJECT] gs://[DESTINATION\_BUCKET\_NAME]/
- D. gcloud dataproc cp [LOCAL\_OBJECT] gs://[DESTINATION\_BUCKET\_NAME]/

### Correct Answer: A

The gsutil cp command allows you to copy data between your local file storage. boto files generated by running "gsutil config"

*Community vote distribution*

A (83%)

B (17%)

  Jamessmith112  5 months ago

I received my certificate on 19th NOV 2023 passed with 88%. Most of the questions are directly from here and pass4surehub.com. Thank you ExamTopics and pass4surehub!!

upvoted 8 times

  appu121  2 years, 8 months ago

i took up the exam yesterday. not a single question from here. i failed the exam. please do not waste your time here. Moderator does not appear this real review also.

upvoted 7 times

  rapila  3 months, 1 week ago

A is correct answer

<https://shorturl.at/ryMUW>

upvoted 5 times

  blackshuai 5 months, 2 weeks ago

A is correct answer

upvoted 1 times

  wanrltw 5 months, 3 weeks ago

 Selected Answer: A

Answer: A

Cloud Storage => gsutil. Doesn't matter how the files are going to be consumed, the task is to upload them.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: A**

I would go with A.

upvoted 1 times

 **Abhi00754** 3 months, 1 week ago

Did you pass the exam with question from here?

upvoted 1 times

 **didek1986** 8 months ago

**Selected Answer: A**

for sure A

upvoted 1 times

 **Jigglypuff09** 11 months, 1 week ago

**Selected Answer: B**

Anyone took exam recently, what percent of questions came from examtopics?

upvoted 1 times

 **Bossam** 1 year, 1 month ago

Anyone took exam recently, what percent of questions came from examtopics?

upvoted 1 times

 **atoledo** 1 year, 2 months ago

**Selected Answer: A**

gsutil cp [LOCAL\_OBJECT] gs://[DESTINATION\_BUCKET\_NAME]/

upvoted 1 times

 **melisargh** 1 year, 4 months ago

from question 100 and forward they are related to the current exam, i cleared last week and they were useful. from question 1 to 99 they are outdated.

upvoted 2 times

 **Nandak217** 1 year, 4 months ago

A is correct

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: A**

A is correct

upvoted 1 times

 **akssha74** 2 years, 3 months ago

Anyone took the exam recently?

upvoted 1 times

 **GCPSam0** 2 years, 4 months ago

Any one took the exam recently? Any questions from here?

upvoted 3 times

 **Trueeye** 2 years, 3 months ago

Yes, None of them from here

upvoted 1 times

 **SuperDevops** 2 years, 5 months ago

When will questions be update?

upvoted 4 times

 **hfudjn** 2 years, 5 months ago

When will questions be update? Not one question from here on exam

upvoted 1 times

You migrated your applications to Google Cloud Platform and kept your existing monitoring platform. You now find that your notification system is too slow for time critical problems.

What should you do?

- A. Replace your entire monitoring platform with Stackdriver.
- B. Install the Stackdriver agents on your Compute Engine instances.
- C. Use Stackdriver to capture and alert on logs, then ship them to your existing platform.
- D. Migrate some traffic back to your old platform and perform AB testing on the two platforms concurrently.

**Correct Answer: B**

Reference:

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

*Community vote distribution*

C (48%)	B (33%)	A (19%)
---------	---------	---------

✉  **gcper** Highly Voted 3 years, 6 months ago  
C

The task does not indicate that we should get rid of the old software. The pain point is slowness for time critical problems only. Thus we would use Stackdriver for the time critical alerts and still utilize the old platform for further analysis/storing of logs or whatever its business case is.  
upvoted 18 times

✉  **stevesmith112** Highly Voted 5 months ago  
Just took the exam and i passed with 88% , and surprisingly, about like a 50-60% came from here. and other questions are from pass4surehub  
A lot of kubernetes + microservices in GKE questions were asked. Thnaks to Examtopics and Pass4surehub.com  
upvoted 6 times

✉  **santoshchauhan** Most Recent 1 month, 3 weeks ago  
**Selected Answer: C**  
the most balanced and least disruptive approach would likely be option C, "Use Stackdriver to capture and alert on logs, then ship them to your existing platform". This method allows for a seamless integration of Stackdriver's real-time alerting capabilities into your existing monitoring workflow without the need for a complete overhaul of your system.  
upvoted 1 times

✉  **rapila** 3 months, 1 week ago

**Selected Answer: B**

B is correct answer

<https://shorturl.at/ryMUW>  
upvoted 5 times

✉  **blackshuai** 5 months, 2 weeks ago  
**Selected Answer: B**  
B is correct answer  
upvoted 1 times

 **wanrltw** 5 months, 3 weeks ago

Option C.

Notifications from on-prem monitoring system are too slow & applications are in GCP now => Stackdriver alerts on logs.

There's no mentioning whether the apps have been migrated to GCE, GKE, App Engine or Cloud Run, so "Compute Engine instances" come from an assumption.

upvoted 3 times

 **\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: C**

I would go with C.

upvoted 1 times

 **SARAVANA25** 8 months, 1 week ago

Option B , Install stack driver agents on the compute instances is the correct answer .  
using stackdriver and shipping it to existing platform will have some delay

upvoted 1 times

 **closer89** 12 months ago

**Selected Answer: C**

C

you have problems with notifications.

C option allows you to use stackdriver to send alerts immediately and straight away after sends all this data to your on-prem monitoring platform

upvoted 3 times

 **Foxal** 1 year, 2 months ago

**Selected Answer: B**

B is the correct answer.

<https://cloud.google.com/monitoring/agent/monitoring/installation>

upvoted 1 times

 **lxs** 1 year, 3 months ago

**Selected Answer: C**

Think twice. You have working an expensive monitoring system i.e Splunk and you have the problem with unacceptable delay time between incident and notification. You need to fix this problem, not doing a revolution (changing monitoring system). You can leverage GCP Monitoring with alerting system which is out-of-the-box with no huge effort, because if you want or not logs are in cloud logging. Simply implement alerts and push logs to Splunk. Simples.

upvoted 3 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: A**

A is correct

upvoted 2 times

 **ruben82** 1 year, 11 months ago

It's the rightest answer. C cannot work without Agent and there's not sense to send log to old monitoring

upvoted 1 times

 **ruben82** 1 year, 11 months ago

It's A 'cos you cannot use Stackdriver if you don't install Stackdriver agent on your compute engine.

upvoted 2 times

**mjdubal** 1 year, 10 months ago

Hi

Did you find any questions from here?

upvoted 1 times

 **morenocasado** 2 years ago

**Selected Answer: C**

Community choice is C

upvoted 2 times

✉️  **GCPCloudArchitectUser** 2 years, 2 months ago

**Selected Answer: A**

I think it should be A than C

Apps have been migrated and why would you invest on C to send data back to existing system instead fix old system using direct connect or something

upvoted 2 times

✉️  **GCPCloudArchitectUser** 2 years, 2 months ago

Nvm I think it should be C

upvoted 1 times

✉️  **chelovalpo** 2 years, 5 months ago

The answer is C. The point is notification problem with low performance, not monitoring.

Question #3

Topic 1

You are planning to migrate a MySQL database to the managed Cloud SQL database for Google Cloud. You have Compute Engine virtual machine instances that will connect with this Cloud SQL instance. You do not want to whitelist IPs for the Compute Engine instances to be able to access Cloud SQL.

What should you do?

- A. Enable private IP for the Cloud SQL instance.
- B. Whitelist a project to access Cloud SQL, and add Compute Engine instances in the whitelisted project.
- C. Create a role in Cloud SQL that allows access to the database from external instances, and assign the Compute Engine instances to that role.
- D. Create a CloudSQL instance on one project. Create Compute engine instances in a different project. Create a VPN between these two projects to allow internal access to CloudSQL.

**Correct Answer: C**

Reference:

<https://cloud.google.com/sql/docs/mysql/connect-external-app>

*Community vote distribution*

A (100%)

✉️  **emmet**  3 years, 11 months ago

The proposed answer seems incorrect, as according to the question application running access to Cloud SQL is run on the Compute Engine; there are no roles in Cloud SQL itself to manage Instance-level access control. According to <https://cloud.google.com/sql/docs/mysql/connect-compute-engine> there are 3 possible ways to connect from Compute Engine: 'Private IP', 'Public IP', 'Cloud SQL Proxy'.

There is no 'Cloud SQL Proxy' option in answers, 'Public IP' requires IP whitelisting which is unacceptable according to the question, so the only valid answer is 'Private IP'

upvoted 26 times

✉️  **peetzthanatip**  3 years, 5 months ago

the answer is A.

upvoted 9 times

✉️  **santoshchauhan**  1 month, 3 weeks ago

**Selected Answer: A**

Selecting Answer A, "Enable private IP for the Cloud SQL instance," is the most efficient and secure method to allow your Google Compute Engine virtual machine instances to connect with a managed Cloud SQL database without the need to whitelist IP addresses. This approach involves configuring the Cloud SQL instance to use a private IP address that is accessible within your Google Cloud Platform (GCP) network. This setup ensures that your Compute Engine instances can securely connect to the Cloud SQL database over Google's private network, providing a high level of security as the database isn't exposed to the public internet. It simplifies the network configuration and avoids the management overhead and security risks associated with maintaining an IP whitelist.

upvoted 1 times

✉️  **rapila** 3 months, 1 week ago

**Selected Answer: A**

the answer is A.

<https://shorturl.at/ryMUW>

upvoted 5 times

✉️  **stevesmith112** 5 months ago

Just took the exam and i passed with 88% , and surprisingly, about like a 50-60% came from here. and other questions are from pass4surehub.com  
A lot of kubernetes + microservices in GKE questions were asked. Thnaks to Examtopics and Pass4surehub.com

upvoted 4 times

✉️  **\_rajan\_** 7 months, 1 week ago

**Selected Answer: A**

Enabling private IP allows the Compute Engine instances and the Cloud SQL instance to communicate over a private, internal network within Google Cloud Platform (GCP), rather than relying on external IP whitelisting.

upvoted 1 times

✉️  **omermahgoub** 1 year, 3 months ago

These are the options you can use to connect a Cloud SQL instance to a Compute Engine instance:

1. Private IP: You can use the private IP of the Cloud SQL instance to connect to it from the Compute Engine instance. This requires that the Cloud SQL instance and the Compute Engine instance are in the same VPC network.

2. Public IP: You can use the public IP of the Cloud SQL instance to connect to it from the Compute Engine instance. This requires that the Cloud SQL instance is configured to allow connections from the public IP of the Compute Engine instance.

upvoted 3 times

✉️  **omermahgoub** 1 year, 3 months ago

3. Cloud SQL Auth proxy: The Cloud SQL Auth proxy is a tool that allows you to connect to Cloud SQL instances from external applications. To use the Cloud SQL Auth proxy, you need to install it on the Compute Engine instance and use it to establish a connection to the Cloud SQL instance.

4. Cloud SQL Auth proxy Docker image: The Cloud SQL Auth proxy Docker image is a Docker image that contains the Cloud SQL Auth proxy. You can use this Docker image to run the Cloud SQL Auth proxy in a Docker container on the Compute Engine instance. This allows you to easily deploy and manage the Cloud SQL Auth proxy on the Compute Engine instance.

upvoted 3 times

✉️  **omermahgoub** 1 year, 3 months ago

And off course, you can enable private IP on a Cloud SQL instance on Google Cloud Platform (GCP). Private IP allows you to access a Cloud SQL instance from within the same VPC network, without the need to use a public IP or whitelist IP addresses.

To enable private IP on a Cloud SQL instance, you need to do the following:

Create a VPC network: First, you need to create a VPC network in which the Cloud SQL instance and the Compute Engine instance will be placed.

Create a Cloud SQL instance: Next, you need to create a Cloud SQL instance and specify the VPC network that you created in step 1 as the network for the Cloud SQL instance.

Enable private IP: Finally, you can enable private IP on the Cloud SQL instance by going to the "Networking" tab in the Cloud SQL instance's configuration page and selecting the "Private IP" option.

Once you have enabled private IP on the Cloud SQL instance, you can access it from the Compute Engine instance using the private IP of the Cloud SQL instance.

Answer is A

upvoted 1 times

✉️  **tomato123** 1 year, 8 months ago

**Selected Answer: A**

A is correct

upvoted 2 times

 **ruben82** 1 year, 11 months ago

**Selected Answer: A**

The question is about "connection". Role assignment gives a set of permission to compute engine but doesn't allow connection.  
upvoted 2 times

 **GoReplyGCPExam** 1 year, 11 months ago

The best way would be to connect the compute engine instance to cloud sql with Cloud SQL Auth Proxy (<https://cloud.google.com/sql/docs/mysql/roles-and-permissions#proxy-roles-permissions>). But the way that C is phrased makes me think th is correct

"...you can use the default Compute Engine service account associated with the Compute Engine instance. As with all accounts connecting to Cloud SQL instance, the service account must have the Cloud SQL > Client role."

upvoted 1 times

 **jcataluna** 2 years, 2 months ago

**Selected Answer: A**

Right answer is A. Agree with emmet.

upvoted 1 times

 **ParagSanyashiv** 2 years, 3 months ago

Answer should be A

upvoted 1 times

 **chelovalpo** 2 years, 5 months ago

The answer is A, private ip allows the connection between gce and cloudsq, for other hand isn't possible access to from gce to cloudsq tho roles without public ip with firewall rules, private ip o cloudproxy

upvoted 2 times

 **SuperNest** 2 years, 7 months ago

Personally agree the option C, using a private IP will allow all compute engine instances to access the database. What if not all of the comput instances within the same VPC are allowed?

upvoted 1 times

 **ruben82** 1 year, 11 months ago

But the question is about connection. If you assign a role to compute engine, it'll have the permission to use Cloud SQL but couldn't allow connect to it.

upvoted 1 times

 **wilwong** 2 years, 9 months ago

agree C

upvoted 1 times

 **wilwong** 2 years, 9 months ago

sorry the answer is A

upvoted 1 times

 **yuchun** 2 years, 10 months ago

the answer is A.

upvoted 1 times

 **syu31svc** 2 years, 10 months ago

<https://cloud.google.com/sql/docs/mysql/connect-compute-engine#connect-gce-private-ip>

Answer is A given the options presented

upvoted 2 times

#### Question #4

#### Topic 1

You have deployed an HTTP(s) Load Balancer with the gcloud commands shown below.

```
export NAME=load-balancer

# create network
gcloud compute networks create ${NAME}

# add instance
gcloud compute instances create ${NAME}-backend-instance-1 --subnet ${NAME} --no address

# create the instance group
gcloud compute instance-groups unmanaged create ${NAME}-i
gcloud compute instance-groups unmanaged set-named-ports ${NAME}-i --named-ports http:80
gcloud compute instance-groups unmanaged add-instances ${NAME}-i --instances ${NAME}-instance-1

# configure health checks
gcloud compute health-checks create http ${NAME}-http-hc --port 80

# create backend service
gcloud compute backend-services create ${NAME}-http-bes --health-checks ${NAME}-http-hc --protocol HTTP --port-name http
--global
gcloud compute backend-services add-backend ${NAME}-http-bes --instance-group ${NAME}-i --balancing-mode RATE --max-rate
100000 --capacity-scaler 1.0 --global --instance-group-zone us-east1-d

# create url maps and forwarding rule
gcloud compute url-maps create ${NAME}-http-urlmap --default-service ${NAME}-http-bes
gcloud compute target-http-proxies create ${NAME}-http-proxy --url-map ${NAME}-http-urlmap
gcloud compute forwarding-rules create ${NAME}-http-fw --global --ip-protocol ICP --target-http-proxy ${NAME}-http-proxy
--ports 80
```

Health checks to port 80 on the Compute Engine virtual machine instance are failing and no traffic is sent to your instances. You want to resolve the problem.

Which commands should you run?

- A. gcloud compute instances add-access-config \${NAME}-backend-instance-1
- B. gcloud compute instances add-tags \${NAME}-backend-instance-1 --tags http-server
- C. gcloud compute firewall-rules create allow-lb --network load-balancer --allow tcp --source-ranges 130.211.0.0/22,35.191.0.0/16 --direction INGRESS
- D. gcloud compute firewall-rules create allow-lb --network load-balancer --allow tcp --destination-ranges 130.211.0.0/22,35.191.0.0/16 --direction EGRESS

#### Correct Answer: C

Reference:

<https://cloud.google.com/vpc/docs/special-configurations>

*Community vote distribution*

C (100%)

C

the source IP ranges for health checks (including legacy health checks if used for HTTP(S) Load Balancing) are:

35.191.0.0/16  
130.211.0.0/22

Furthermore it should be direction INGRESS since the health-check (ping) is coming into the load balancer/instance.

source: <https://cloud.google.com/load-balancing/docs/health-checks>  
upvoted 10 times

 **syu31svc** 2 years, 10 months ago  
Yup I would go for C based on this  
upvoted 1 times

 **santoshchauhan** Most Recent 1 month, 3 weeks ago

**Selected Answer: C**

Option C is the correct choice because it addresses the issue of health check failures for the Compute Engine instances behind the HTTP(s) Load Balancer. By creating an ingress firewall rule, this command allows traffic from the load balancer's source IP ranges to reach the instances on specified network. These source IP ranges (130.211.0.0/22 and 35.191.0.0/16) are used by Google Cloud load balancers for health checking. Without this rule, the health checks would fail because the load balancer could not communicate with the backend instances to verify their status, resulting in no traffic being routed to those instances. By implementing this firewall rule, you ensure that the health check traffic is permitted, which should resolve the traffic routing issue and allow the load balancer to function correctly.

upvoted 1 times

 **stevesmith112** 5 months ago

Just took the exam and i passed with 88% , and surprisingly, about like a 50-60% came from here. and other questions are from pass4surehub A lot of kubernetes + microservices in GKE questions were asked. Thnaks to Examtopics and Pass4surehub.com  
upvoted 4 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: C**

I would go with C.  
upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

To resolve the problem, you should run the following command:

Copy code  
`gcloud compute firewall-rules create allow-lb --network load-balancer --allow tcp --source-ranges 130.211.0.0/22,35.191.0.0/16 --direction INGRESS`  
This will create a firewall rule that allows incoming TCP traffic from the specified IP ranges to the Load Balancer network. This should allow traffic to reach the instance group and the instances it contains.

Option A will not help because it is used to add an external IP address to an instance, which is not necessary for the Load Balancer to work. Option B is not necessary because it is used to apply metadata to an instance, which is not related to the Load Balancer. Option D is not correct because it allows outgoing traffic from the Load Balancer network, which is not necessary for the Load Balancer to work.

I hope this helps! Let me know if you have any other questions.

upvoted 2 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: C**  
C is correct  
upvoted 1 times

 **wilwong** 2 years, 9 months ago

C  
ingress not egress  
upvoted 1 times

- ✉  **maleksah** 3 years, 3 months ago  
I would say B with predefined http-server tag on instance.  
upvoted 2 times
- ✉  **yuchun** 2 years, 10 months ago  
even if you set tag, but if you don't set firewall rule based on tag, it still can't create connection from health check probe to backend service  
upvoted 2 times
- ✉  **jcataluna** 1 year, 5 months ago  
If you check Http Server on vm creation, a FW rules with network tag "http-server" is created, but it didn't work the other way around  
upvoted 1 times
- ✉  **donchick** 3 years, 4 months ago  
I choose C.  
upvoted 3 times
- ✉  **donchick** 3 years, 4 months ago  
[https://www.qwiklabs.com/focuses/1232?catalog\\_rank=%7B%22rank%22%3A1%2C%22num\\_filters%22%3A1%2C%22has\\_search%22%3Atrue%7D&parent=catalog&search\\_id=31039](https://www.qwiklabs.com/focuses/1232?catalog_rank=%7B%22rank%22%3A1%2C%22num_filters%22%3A1%2C%22has_search%22%3Atrue%7D&parent=catalog&search_id=31039)  
upvoted 3 times

Question #5

Topic 1

Your website is deployed on Compute Engine. Your marketing team wants to test conversion rates between 3 different website designs. Which approach should you use?

- A. Deploy the website on App Engine and use traffic splitting.
- B. Deploy the website on App Engine as three separate services.
- C. Deploy the website on Cloud Functions and use traffic splitting.
- D. Deploy the website on Cloud Functions as three separate functions.

**Correct Answer: A**

Reference:

<https://cloud.google.com/appengine/docs/standard/python/splitting-traffic>

*Community vote distribution*

A (83%)

B (17%)

- ✉  **mlyu**  3 years, 9 months ago

Ans:A

<https://cloud.google.com/appengine/docs/standard/python/splitting-traffic>

upvoted 11 times

- ✉  **santoshchauhan**  1 month, 3 weeks ago

**Selected Answer: A**

option A is the best approach because it allows you to use App Engine's built-in traffic splitting feature to distribute traffic across different versions of your site. This feature is designed for scenarios exactly like A/B testing, making it possible to seamlessly and efficiently test conversion rates across multiple website designs.

upvoted 1 times

- ✉  **stevesmith112** 5 months ago

Just took the exam and I passed with 88%, and surprisingly, about like a 50-60% came from here. And other questions are from pass4surehub. A lot of Kubernetes + microservices in GKE questions were asked. Thanks to Examtopics and Pass4surehub.com

upvoted 3 times

 **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: A**

A is Correct.

upvoted 1 times

 **coco10k** 1 year, 7 months ago

**Selected Answer: A**

you have a URL for each version deployed in the same service.

upvoted 2 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: A**

A is correct

upvoted 2 times

 **kinoko1330** 1 year, 8 months ago

**Selected Answer: A**

A of course

upvoted 1 times

 **riccardo990** 1 year, 10 months ago

**Selected Answer: A**

i think traffic splitting is more suitable

upvoted 2 times

 **ruben82** 1 year, 11 months ago

**Selected Answer: A**

I vote A but It could be wrong 'cos the question is not detailed. It doesn't ask to let url remain the same. So B could be a good answer: in this way you have 3 url different without any need to manage splitting

upvoted 1 times

 **yogi\_508** 2 years ago

A

A is correct because it allows routing traffic to a single domain and split traffic based on IP or Cookie.

B is not correct because the domain name will change based on the service.

source: Google Sample Questions

upvoted 2 times

 **[Removed]** 2 years ago

Answer is A

upvoted 1 times

 **GCPCloudArchitectUser** 2 years, 2 months ago

**Selected Answer: B**

If you want to test three different websites and compare how would you use traffic splitting (33%)

upvoted 2 times

 **GCPCloudArchitectUser** 2 years, 2 months ago

I can safely remove compare keyword from my comment... so it will be back to A

upvoted 2 times

 **wilwong** 2 years, 9 months ago

A is correct

upvoted 3 times

 **syu31svc** 2 years, 10 months ago

This is A for sure

upvoted 4 times

 **mastodilu** 2 years, 11 months ago

this question is also asked in the example questions.

Correct answer is A, because traffic splitting is exactly for testing purpose and you can choose to redirect 100% percent traffic to a specific version.

upvoted 4 times

✉️  **rgpalop** 3 years, 2 months ago

3 different website designs but the same service. I think is A  
upvoted 4 times

✉️  **yuchun** 2 years, 10 months ago

yes, the question is to test 'if the 3 website design is the same service?', absolutely it's.  
upvoted 2 times

✉️  **maleksah** 3 years, 3 months ago

Answer is B with 3 appengine services. (3 urls to access the version you want).  
With traffic splitting on versions, you can't choose exactly the version you want...  
upvoted 3 times

✉️  **hitmax87** 2 years ago

No, you don't need to have different urls. GCP will automatically split 33% of traffic to each version. You should have just 3 releases with different front end markup of one service. Answer A is correct  
upvoted 1 times

You need to copy directory local-scripts and all of its contents from your local workstation to a Compute Engine virtual machine instance. Which command should you use?

- A. gsutil cp --project my-gcp-project -r ~/local-scripts/ gcp-instance-name:~/server-scripts/ --zone us-east1-b
- B. gsutil cp --project my-gcp-project -R ~/local-scripts/ gcp-instance-name:~/server-scripts/ --zone us-east1-b
- C. gcloud compute scp --project my-gcp-project --recurse ~/local-scripts/ gcp-instance-name:~/server-scripts/ --zone us-east1-b
- D. gcloud compute mv --project my-gcp-project --recurse ~/local-scripts/ gcp-instance-name:~/server-scripts/ --zone us-east1-b

**Correct Answer: C**

Reference:

<https://cloud.google.com/sdk/gcloud/reference/compute/copy-files>

*Community vote distribution*

C (100%)

 **Blueocean** Highly Voted 2 years, 3 months ago

Agreed C is correct option

upvoted 5 times

 **\_rajan\_** Most Recent 7 months, 1 week ago

**Selected Answer: C**

C is correct.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: C**

C is correct

upvoted 1 times

 **kinoko1330** 1 year, 8 months ago

**Selected Answer: C**

C because of scp

upvoted 1 times

 **ruben82** 1 year, 11 months ago

**Selected Answer: C**

C is the correct answer

upvoted 1 times

You are deploying your application to a Compute Engine virtual machine instance with the Stackdriver Monitoring Agent installed. Your application is a unix process on the instance. You want to be alerted if the unix process has not run for at least 5 minutes. You are not able to change the application to generate metrics or logs.

Which alert condition should you configure?

- A. Uptime check
- B. Process health
- C. Metric absence
- D. Metric threshold

**Correct Answer: B**

Reference:

<https://cloud.google.com/monitoring/alerts/concepts-indepth>

*Community vote distribution*

B (75%)

C (25%)

 **santoshchauhan** 1 month, 3 weeks ago

**Selected Answer: C**

To be alerted if your Unix process has not run for at least 5 minutes, you should configure a \*\*metric absence\*\* alert condition. Since you can modify the application to generate metrics or logs, this approach allows you to monitor the absence of data for a specific duration. When the Unix process stops running, the metric data will be absent, triggering the alert.

Therefore, the correct answer is \*\*C. Metric absence\*\*. This type of alerting policy will help you stay informed about any unexpected interrupt in your process execution.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: B**

B is correct.

upvoted 1 times

 **studyingveryhard** 9 months, 2 weeks ago

Complete explanations for correct and incorrect answers can be seen on <https://examlab.co/google/google-cloud-professional-cloud-developer-exam-practice-test/>

upvoted 1 times

 **closer89** 12 months ago

**Selected Answer: B**

<https://cloud.google.com/monitoring/alerts/policies-in-json#json-process-health>

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: B**

B is correct

upvoted 1 times

 **wilwong** 2 years, 9 months ago

B is correct

upvoted 1 times

 **syu31svc** 2 years, 10 months ago

<https://cloud.google.com/monitoring/uptime-checks>:

"An uptime check is a request sent to a resource to see if it responds"

A is wrong

Metric absence and threshold don't make sense

Process health is correct for sure so answer is B

upvoted 1 times

 **gcper** 3 years, 2 months ago

B

Process-health policy

A process-health policy can notify you if the number of processes that match a pattern crosses a threshold. This can be used to tell you, for example, that a process has stopped running.

source: <https://cloud.google.com/monitoring/alerts/policies-in-json#json-process-health>

upvoted 4 times

 **saurabh1805** 3 years, 5 months ago

B is correct answer

<https://cloud.google.com/monitoring/alerts/types-of-conditions#metric-threshold>

upvoted 2 times

You have two tables in an ANSI-SQL compliant database with identical columns that you need to quickly combine into a single table, removing duplicate rows from the result set.

What should you do?

- A. Use the JOIN operator in SQL to combine the tables.
- B. Use nested WITH statements to combine the tables.
- C. Use the UNION operator in SQL to combine the tables.
- D. Use the UNION ALL operator in SQL to combine the tables.

**Correct Answer: C**

Reference:

[https://www.techonthenet.com/sql/union\\_all.php](https://www.techonthenet.com/sql/union_all.php)

*Community vote distribution*

C (100%)

 **saurabh1805** Highly Voted 3 years, 5 months ago

C is correct answer here.

The only difference between Union and Union All is that Union All will not removes duplicate rows or records, instead, it just selects all the row from all the tables which meets the conditions of your specifics query and combines them into the result table.

upvoted 7 times

 **\_rajan\_** Most Recent 7 months, 1 week ago

**Selected Answer: C**

C is correct.

upvoted 1 times

 **ash\_meharun** 1 year, 4 months ago

UNION removes duplicate rows.

UNION ALL does not remove duplicate rows.

upvoted 3 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: C**

C is correct

upvoted 1 times

 **wilwong** 2 years, 9 months ago

C is correct

upvoted 1 times

 **syu31svc** 2 years, 10 months ago

If you know SQL well enough, C is the answer

upvoted 2 times

You have an application deployed in production. When a new version is deployed, some issues don't arise until the application receives traffic from

users in production. You want to reduce both the impact and the number of users affected.

Which deployment strategy should you use?

- A. Blue/green deployment
- B. Canary deployment
- C. Rolling deployment
- D. Recreate deployment

**Correct Answer: A**

Reference:

<https://thenewstack.io/deployment-strategies/>

*Community vote distribution*

B (93%)

7%

 [Removed] Highly Voted 4 years ago

I tkink it is B) Canary deployment.

With Blue/green deployment there will be more users affected.

upvoted 23 times

 Alekshar 3 years, 11 months ago

More than that, blue/green deployment affects all the users as we switch the full production to the new version in one time

upvoted 1 times

 mastodilu 2 years, 11 months ago

exactly, plus with blue green strategy the new version is not gradually exposed to production, but canary is.

upvoted 1 times

 santoshchauhan Most Recent 1 month, 3 weeks ago

**Selected Answer: B**

B. Canary deployment: In this strategy, the new version of the application (the "canary") is rolled out to a small subset of users before it is made available to the entire user base. This allows you to monitor the performance and stability of the new version in the real-world production environment with actual traffic, but only affects a small group of users. If issues arise, the canary deployment can be rolled back with minimal impact.

upvoted 1 times

 theseawillclaim 2 months, 2 weeks ago

**Selected Answer: B**

That's exactly what Canary Deployment is for.

upvoted 1 times

 wanrltw 5 months, 3 weeks ago

**Selected Answer: B**

B:

[https://cloud.google.com/architecture/application-deployment-and-testing-strategies#canary\\_test\\_pattern](https://cloud.google.com/architecture/application-deployment-and-testing-strategies#canary_test_pattern)

upvoted 1 times

 \_\_rajan\_\_ 7 months, 1 week ago

**Selected Answer: B**

I would go with B as it is best suited for this senario.

upvoted 1 times

 telp 1 year, 3 months ago

**Selected Answer: B**

answer is B to reduce impact on users because it's a progressive release

upvoted 2 times

 **Mark123321** 1 year, 4 months ago

**Selected Answer: A**

I think A is correct because of the switching to green only happens after you perform all the tests on it. So you can also test traffic (to satisfy t question) This is the point of blue-green deployment as far as I understood it.

B is not correct because the real traffic is switched partially to new version immediately and so it effects some users.

reference: <https://digitalvarys.com/what-is-blue-gren-deployment/>

upvoted 1 times

 **jcataluna** 1 year, 5 months ago

**Selected Answer: B**

Blue/Green is 100% users to Green, Canary id progressive. B.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: B**

B is correct

upvoted 2 times

 **maxdanny** 1 year, 9 months ago

For me it's B, in Canary Deployment only a percentage of users receives the new version and therefore in case of error immediately rollback , immediately the new version , Green, receive all traffic and Blue marked as deprecated

upvoted 1 times

 **PetervanLeeuwen** 1 year, 9 months ago

I think the concept of google about B/G testing is that there is a shadow running next to production that receives the same traffic as producti When this shadow is not having any errors you can update the shadow to PROD. So no user is impacted, since all possible new errors will oc in the shadow and not in prod.

upvoted 1 times

 **PetervanLeeuwen** 1 year, 9 months ago

Find more info here: [https://cloud.google.com/architecture/implementing-deployment-and-testing-strategies-on-gke#perform\\_a\\_bluegreen\\_deployment](https://cloud.google.com/architecture/implementing-deployment-and-testing-strategies-on-gke#perform_a_bluegreen_deployment)

upvoted 1 times

 **ruben82** 1 year, 11 months ago

**Selected Answer: B**

For me is B. But I cannot understand why all purchased exam test with this question, put Blue/Green as correct answer. It's so clear that Can is the rightest one 'cos forward only a few of users to new deploy (not every as blue/green) and also allow the rollback action

upvoted 1 times

 **nazonazonazo** 2 years, 2 months ago

B is correct. Blue Green(B/G) affects all users.

upvoted 1 times

 **HolaBaby** 2 years, 4 months ago

**Selected Answer: B**

1. Reducing impact

2. Number of users affected

If you want meet both of the conditions, you need to choose Canary

upvoted 3 times

 **tendzen** 2 years, 5 months ago

I think it is B, but correct answer is A, hmm.....

if we think that we need to test 100% of the traffic, i.e. create a full working test, then right A, because if there is an error we can quickly go ba to the old version

upvoted 1 times

 **wilwong** 2 years, 9 months ago

Agree B

upvoted 1 times

 **syu31svc** 2 years, 10 months ago

This is canary for sure; B

upvoted 4 times

Your company wants to expand their users outside the United States for their popular application. The company wants to ensure 99.999% availability of the database for their application and also wants to minimize the read latency for their users across the globe.

Which two actions should they take? (Choose two.)

- A. Create a multi-regional Cloud Spanner instance with "nam-asia-eur1" configuration.
- B. Create a multi-regional Cloud Spanner instance with "nam3" configuration.
- C. Create a cluster with at least 3 Spanner nodes.
- D. Create a cluster with at least 1 Spanner node.
- E. Create a minimum of two Cloud Spanner instances in separate regions with at least one node.
- F. Create a Cloud Dataflow pipeline to replicate data across different databases.

**Correct Answer: BF**

*Community vote distribution*

AC (100%)

 **saurabh1805** Highly Voted 3 years, 5 months ago

The more number of node less read latency hence i will go with option A and C  
upvoted 9 times

 **emmet** Highly Voted 3 years, 11 months ago

I think the answer should be A) + something.  
They wants 99.999% availability - only multi-regional instance fits this. To minimize read latency nam-asia-eur1 instance works best as it has replicas in North America, Europe and Asia regions.  
(<https://cloud.google.com/spanner/docs/instances#configs-multi-region>)

As for second answer - I do not have strong opinion.. As per documentation "Adding nodes gives each replica more CPU and RAM, which increases the replica's throughput" and they recommend to choose number of nodes to "keep high priority total CPU utilization under 65%". Nodes are not about SLA and read latency. From another hand spanner "Cloud Spanner automatically replicates your data between regions with strong consistency guarantees" so no DataFlow pipeline needed to replicate data, unless the app has other DBs and ETL between Spanner and those DBs.

upvoted 7 times

 **santoshchauhan** Most Recent 1 month, 3 weeks ago

**Selected Answer: AC**

To achieve 99.999% availability and minimize read latency for a globally distributed user base, the company should:

- Deploy a multi-regional Cloud Spanner instance with the "nam-asia-eur1" configuration (Option A). This setup will provide the geographical distribution of data across three continents — North America, Asia, and Europe. The multi-regional nature of this option is designed to maintain high availability and ensure users across these regions experience low latency when accessing the database.
- Ensure that the Cloud Spanner instance has a minimum of three nodes (Option C). This configuration will contribute to the high availability and fault tolerance of the database. Spanner's built-in replication across these nodes in different regions will further support the five nines (99.999%) availability target, while also providing scalability for read operations.

upvoted 1 times

 **theseawillclaim** 2 months, 3 weeks ago

**Selected Answer: AC**

Let's think about all possible answers:

- B does not make sense, as "nam3" is not the global configuration we want;
- D is not ok, 'cause 1 node is not enough
- E is not enough, as we want a global configuration;
- F is totally unrelated.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: AC**

AC are best suited here.

upvoted 1 times

 **closer89** 12 months ago

**Selected Answer: AC**

99.999% availability and reduce latency

Option A gives us 99.999% availability (think its typo in region name)

Option C is about compute capacity, more nodes -> less latency

<https://cloud.google.com/spanner/docs/instances#compute-capacity>

B - there is no such multi-region configuration nam3

D - its better to create cluster with 3 nodes, not 1

E,F - overengineering

upvoted 2 times

 **DonWang** 10 months, 1 week ago

there is `nam3`

<https://cloud.google.com/spanner/docs/instance-configurations>

upvoted 2 times

 **closer89** 1 year ago

**Selected Answer: AC**

A - global and provides 99.999% availability

C - more nodes - less latency

upvoted 1 times

 **tuanbo91** 1 year, 4 months ago

**Selected Answer: AC**

it's obvious

upvoted 1 times

 **Lunaixiaoxin** 1 year, 4 months ago

why not C and F

upvoted 1 times

 **jcatalogna** 1 year, 5 months ago

**Selected Answer: AC**

3 regions at least, and for those that says there is no region "man-asia-eur1", take a look at the console, its multiregion nomenclature!

upvoted 1 times

 **zevexWM** 1 year, 3 months ago

There is according to their documentation: [https://cloud.google.com/spanner/docs/instance-configurations#three\\_continents](https://cloud.google.com/spanner/docs/instance-configurations#three_continents)

upvoted 1 times

 **jeeet\_** 1 year, 5 months ago

There is no region called ""nam-asia-eur1""

A is wrong,

B&C is correct

upvoted 3 times

 **brunoguzzo18** 1 year, 8 months ago

**Selected Answer: AC**

We need multi-region db (spanner) to satisfy 99,999% SLA and have multi-node to ensure resource needed.

upvoted 2 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: AC**

AC are correct

upvoted 3 times

 **maxdanny** 1 year, 9 months ago

C because the number of nodes increases the computational capabilities ( queries for seconds and so minor latency), F to cover worldwide availability; A it's wrong because the configuration "nam-asia-eur1" not exist, Google suggests "nam-eur-asia1" o "nam-eur-asia3", D it's wro because the number of nodes is too few; E is too expensive a solution

upvoted 4 times

 **jdx000** 1 year, 9 months ago

**Selected Answer: AC**

A and C make sense

upvoted 1 times

 **ParagSanyashiv** 2 years, 3 months ago

This should be A and F.

upvoted 1 times

 **wilwong** 2 years, 9 months ago

Agree with A and C

upvoted 3 times

Question #11

Topic 1

You need to migrate an internal file upload API with an enforced 500-MB file size limit to App Engine.

What should you do?

- A. Use FTP to upload files.
- B. Use CPanel to upload files.
- C. Use signed URLs to upload files.
- D. Change the API to be a multipart file upload API.

**Correct Answer: C**

Reference:

[https://wiki.christophchamp.com/index.php?title=Google\\_Cloud\\_Platform](https://wiki.christophchamp.com/index.php?title=Google_Cloud_Platform)

*Community vote distribution*

D (63%)

C (38%)

 **santoshchauhan** 1 month, 3 weeks ago

**Selected Answer: C**

C. Use signed URLs to upload files: Signed URLs are a secure way to give time-limited read or write access to a specific Google Cloud Storage object, without needing Google account credentials. You can create a signed URL that allows an object to be accessed with the specified restrictions such as HTTP method (PUT for uploads) and an expiration time. This method would allow your API users to upload files directly to Google Cloud Storage, which can handle large files efficiently. Your App Engine application can then process or reference these files as needed

upvoted 1 times

 **manikanthk** 1 month, 4 weeks ago

**Selected Answer: C**

<https://stackoverflow.com/questions/45812595/google-cloud-storage-signed-urls-how-to-specify-a-maximum-file-size>

upvoted 1 times

 **theseawillclaim** 2 months, 2 weeks ago

**Selected Answer: D**

While C is a very good option if you want to people to upload files, it does not solve the problem represented by the size.  
upvoted 2 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: D**

By changing the API to support multipart file uploads, you can maintain the functionality of your existing API while adapting it to the App Engine environment.  
upvoted 1 times

 **maxdanny** 8 months, 1 week ago

The correct answer is C because signed url permits to upload a big file in multipart-mode  
upvoted 2 times

 **DonWang** 10 months ago

**Selected Answer: D**

It should use multipart to upload big size files  
upvoted 2 times

 **Ayushman\_koul23** 1 year, 1 month ago

How is C correct ? Isn't it used to give temporary access to objects in buckets ?  
upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: C**

C is correct  
upvoted 1 times

 **wilwong** 2 years, 9 months ago

C is the best choice  
upvoted 1 times

 **syu31svc** 2 years, 10 months ago

[https://cloud.google.com/appengine/docs/standard/php/googlestorage/user\\_upload](https://cloud.google.com/appengine/docs/standard/php/googlestorage/user_upload):  
"Note that you must start uploading to this URL within 10 minutes of its creation. Also, you cannot change the URL in any way - it is signed as the signature is checked before your upload begins"

C is the answer  
upvoted 2 times

 **saurabh1805** 3 years, 5 months ago

C is correct answer  
upvoted 2 times

 **mastodilu** 2 years, 11 months ago

true  
<https://stackoverflow.com/a/18882565/8681600>  
upvoted 2 times

Question #12

Topic 1

You are planning to deploy your application in a Google Kubernetes Engine (GKE) cluster. The application exposes an HTTP-based health check at /healthz. You want to use this health check endpoint to determine whether traffic should be routed to the pod by the load balancer.

Which code snippet should you include in your Pod configuration?

A.

```
livenessProbe:  
  httpGet:  
    path: /healthz  
    port: 80  
  
B.  
  
readinessProbe:  
  httpGet:  
    path: /healthz  
    port: 80  
  
C.  
  
loadbalancerHealthCheck:  
  httpGet:  
    path: /healthz  
    port: 80  
  
D.  
  
healthCheck:  
  httpGet:  
    path: /healthz  
    port: 80
```

**Correct Answer: B**

For the GKE ingress controller to use your readinessProbes as health checks, the Pods for an Ingress must exist at the time of Ingress creation. If your replicas are scaled to 0, the default health check will apply.

✉  **wanrltw** 5 months, 3 weeks ago

B:  
<https://kubernetes.io/docs/tasks/configure-pod-container/configure-liveness-readiness-startup-probes/>  
upvoted 1 times

✉  **omermahgoub** 1 year, 3 months ago

Option B is the correct code snippet to include in the Pod configuration in order to use the /healthz endpoint as a readiness probe.

The liveness probe, specified in option A, is used to determine whether the application is running and responsive. If the liveness probe fails, the application is considered to be in a failed state and will be restarted.

The readiness probe, specified in option B, is used to determine when a Pod is ready to receive traffic. If the readiness probe fails, the Pod will not receive traffic from the load balancer until it becomes healthy again.

Option C, loadbalancerHealthCheck, is not a valid field in a Pod configuration.

Option D, healthCheck, is also not a valid field in a Pod configuration.

upvoted 2 times

✉  **fanilgor** 1 year, 7 months ago

Readiness probe marks the pod as "Running" and can START accepting traffic.

However, after the pod is in a "Running" state, the Liveness probe comes in and acts as the health check for the entire lifecycle of the pod.

So think of it this way. The pod passes its initial check (readiness), accepts traffic for a while then crashes (logically, the pod can still be "Running").

The Liveness probe is responsible for detecting it. Otherwise, the LB could still pass traffic to a pod that can't serve traffic.

Therefore, I believe it's A.

upvoted 3 times

✉  **fanilgor** 1 year, 7 months ago

On 10th read, It's more likely they mean the initial phase of the lifecycle so it's B.

But the wording here is terrible. Hopefully they refined the question in the real exam.

upvoted 1 times

✉  **tomato123** 1 year, 8 months ago

B is correct

upvoted 2 times

✉  **ruben82** 1 year, 11 months ago

B is correct according with <https://kubernetes.io/docs/tasks/configure-pod-container/configure-liveness-readiness-startup-probes/>

upvoted 1 times

✉  **nazonazonazo** 2 years, 2 months ago

<https://cloud.google.com/kubernetes-engine/docs/how-to/ingress-features>

ingress backendconfig can set healthCheck, but this resource can not set httpGet

```
""  
apiVersion: cloud.google.com/v1  
kind: BackendConfig  
metadata:  
name: my-backendconfig  
spec:  
healthCheck:  
checkIntervalSec: INTERVAL  
timeoutSec: TIMEOUT  
healthyThreshold: HEALTH_THRESHOLD  
unhealthyThreshold: UNHEALTHY_THRESHOLD  
type: PROTOCOL  
requestPath: PATH  
port: PORT  
""
```

upvoted 1 times

✉  **wilwong** 2 years, 9 months ago

B is correct

upvoted 2 times

✉  **syu31svc** 2 years, 10 months ago

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

"GKE can infer some or all of the parameters for a health check if the Serving Pods use a Pod template with a container whose readiness probe has attributes that can be interpreted as health check parameters. See Parameters from a readiness probe for implementation details and Default and inferred parameters for a list of attributes that can be used to create health check parameters. Only the GKE Ingress controller supports inferring parameters from a readiness probe."

B is correct

upvoted 3 times

✉  **yuchun** 2 years, 10 months ago

yes, readiness probe is for checking if the pod can accept traffic.

upvoted 2 times

 **saurabh1805** 3 years, 5 months ago

B is correct answer

<https://cloud.google.com/blog/products/gcp/kubernetes-best-practices-setting-up-health-checks-with-readiness-and-liveness-probes>  
upvoted 2 times

 **meh\_33** 1 year, 7 months ago

B correct

upvoted 1 times

Question #13

Topic 1

Your teammate has asked you to review the code below. Its purpose is to efficiently add a large number of small rows to a BigQuery table.

```
BigQuery service = BigQueryOptions.newBuilder().build().getService();  
  
public void writeToBigQuery(Collection<Map<String, String>> rows){  
    for(Map<String, String> row : rows) {  
        InsertAllRequest insertRequest = InsertAllRequest.newBuilder(  
            "datasetId", "tableId",  
            InsertAllRequest.RowToInsert.of(row)).build();  
        service.insertAll(insertRequest);  
    }  
}
```

Which improvement should you suggest your teammate make?

- A. Include multiple rows with each request.
- B. Perform the inserts in parallel by creating multiple threads.
- C. Write each row to a Cloud Storage object, then load into BigQuery.
- D. Write each row to a Cloud Storage object in parallel, then load into BigQuery.

**Correct Answer: B**

*Community vote distribution*

A (57%)

B (43%)

 **fraloca** Highly Voted 3 years, 4 months ago

For me the correct answer is A.

Infact the loop build a single InsertRequest and send it.

But we can build all request in a list and use InsertAllRequest.newBuilder(tableId).setRows(rows).build() to send.

<https://cloud.google.com/bigquery/streaming-data-into-bigquery#streaminginsertexamples>

upvoted 23 times

 **TrueCurry** Highly Voted 2 years, 4 months ago

**Selected Answer: B**

Response should be A, because original code pushes one row at a time, which is more time consuming in contrast to batch processing.

Proposed answer C is incorrect, because we still have more overhead in sending each row in separate request than using batch processing.

upvoted 6 times

 **santoshchauhan** Most Recent 1 month, 3 weeks ago

**Selected Answer: A**

A. Include multiple rows with each request:

This would be a very efficient way to batch the insert operations. BigQuery's insertAll method supports batched inserts, so instead of inserting each row in a separate request, you could group multiple rows into a single insertAll request. This approach reduces the number of HTTP requests made to the BigQuery service, which can improve throughput and reduce the risk of hitting rate limits.

upvoted 1 times

 **gingrick** 5 months, 1 week ago

**Selected Answer: B**

B - I was between A and B. Both options require changes in the code and Option B requires changes in the way you are managing the Collection. If you insert multiples rows at a time, you would still need to move through the ROWS in the collection one by one (remember, this is a loop) to then insert in bulk. If you first break the Collection into (n) subsets and then run the function in (n) threads, you would be moving through (n) subsets at a time, making (n) insertions at a time, all in parallel. That was my way of viewing it.

Option A would actually not even make a change in performance (sort of), you would just be interacting with the database less. (if interacting less often than inserting)

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: A**

I would go with A.

upvoted 1 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: A**

i'd choose A. for me it's same as batch insert/update recommended

upvoted 1 times

 **mrvergara** 1 year, 2 months ago

**Selected Answer: A**

A. Include multiple rows with each request.

Batch inserts are more efficient than individual inserts and will increase write performance by reducing the overhead of creating and sending individual requests for each row. Parallel inserts could potentially lead to conflicting writes or cause resource exhaustion, and adding a step of writing to Cloud Storage and then loading into BigQuery can add additional overhead and complexity.

upvoted 1 times

 **Foxal** 1 year, 2 months ago

**Selected Answer: A**

A is the correct answer

upvoted 1 times

 **telp** 1 year, 3 months ago

**Selected Answer: A**

answer A, bigquery support multiple insert in one request

<https://cloud.google.com/bigquery/docs/samples/bigquery-table-insert-rows>

upvoted 1 times

✉  **omermahgoub** 1 year, 3 months ago

A. Include multiple rows with each request.

It is generally more efficient to insert multiple rows in a single request, rather than making a separate request for each row. This reduces the overhead of making multiple HTTP requests, and can also improve performance by allowing BigQuery to perform more efficient batch operations. You can use the `InsertAllRequest.RowToInsert.of(row)` method to add multiple rows to a single request.

upvoted 1 times

✉  **omermahgoub** 1 year, 3 months ago

For example, you could modify the code to collect the rows in a list and insert them in batches:

```
List<InsertAllRequest.RowToInsert> rowsToInsert = new ArrayList<>();
for (Map<String, String> row : rows) {
    rowsToInsert.add(InsertAllRequest.RowToInsert.of(row));
    if (rowsToInsert.size() == BATCH_SIZE) {
        InsertAllRequest insertRequest = InsertAllRequest.newBuilder(
            "datasetId", "tableId", rowsToInsert).build();
        service.insertAll(insertRequest);
        rowsToInsert.clear();
    }
}
if (!rowsToInsert.isEmpty()) {
    InsertAllRequest insertRequest = InsertAllRequest.newBuilder(
        "datasetId", "tableId", rowsToInsert).build();
    service.insertAll(insertRequest);
}
```

This will insert the rows in batches of `BATCH_SIZE`, which you can adjust based on the desired balance between performance and resource usage.

upvoted 1 times

✉  **omermahgoub** 1 year, 3 months ago

Options B and D, which involve using multiple threads to perform the inserts or write the rows to Cloud Storage, may not necessarily improve the efficiency of the code. These options could potentially increase the complexity of the code and introduce additional overhead without necessarily improving the performance of the inserts.

Option C, writing each row to a Cloud Storage object before loading into BigQuery, would likely be less efficient than simply inserting the rows directly into BigQuery. It would involve additional steps and potentially increase the overall time it takes to write the rows to the table.

upvoted 1 times

✉  **test010101** 1 year, 4 months ago

**Selected Answer: A**

vote A

upvoted 1 times

✉  **jcatluna** 1 year, 4 months ago

**Selected Answer: A**

Original code inserts one row at a time so no point on using parallel requests..

upvoted 1 times

✉  **thaipad** 1 year, 7 months ago

**Selected Answer: A**

Parallel saving to the database can increase the total addition time and depends on many system conditions. While batch saving is optimized at the database core level.

upvoted 1 times

✉  **tomato123** 1 year, 8 months ago

**Selected Answer: B**

B is correct

upvoted 2 times

✉  **kinoko1330** 1 year, 8 months ago

**Selected Answer: A**

<https://cloud.google.com/bigquery/docs/samples/bigquery-table-insert-rows>

upvoted 1 times

 **akshaychavan7** 1 year, 8 months ago

**Selected Answer: A**

This should be A.

upvoted 1 times

 **alex8081** 1 year, 8 months ago

Agree A. Did you take the exam?

upvoted 1 times

 **nehaxlpb** 1 year, 9 months ago

Question #14

Topic 1

You are developing a JPEG image-resizing API hosted on Google Kubernetes Engine (GKE). Callers of the service will exist within the same GKE cluster. You want clients to be able to get the IP address of the service.

What should you do?

- A. Define a GKE Service. Clients should use the name of the A record in Cloud DNS to find the service's cluster IP address.
- B. Define a GKE Service. Clients should use the service name in the URL to connect to the service.
- C. Define a GKE Endpoint. Clients should get the endpoint name from the appropriate environment variable in the client container.
- D. Define a GKE Endpoint. Clients should get the endpoint name from Cloud DNS.

**Correct Answer: C**

*Community vote distribution*

B (81%)

Other

 **accuracy23**  2 years, 11 months ago

It's B - Clients are in the cluster and therefore can use service dns names.

<https://kubernetes.io/docs/concepts/services-networking/dns-pod-service/>

"Every Service defined in the cluster (including the DNS server itself) is assigned a DNS name. By default, a client Pod's DNS search list includes the Pod's own namespace and the cluster's default domain."

upvoted 19 times

 **santoshchauhan**  1 month, 3 weeks ago

**Selected Answer: B**

B. This is the standard Kubernetes service discovery mechanism. When you define a Service in Kubernetes, it creates a DNS entry in the internal cluster DNS. Any pod in the cluster can then reach the service using the service name as a DNS name (e.g., http://service-name). This is the most straightforward and Kubernetes-native way to enable service discovery within a cluster.

upvoted 1 times

 **Raja2112** 6 months, 2 weeks ago

This is an example of Microservice Architecture, so Ans is : B

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: B**

B is correct.

upvoted 1 times

 **maxdanny** 8 months, 1 week ago

**Selected Answer: B**

<https://www.exam-answer.com/gke-service-url-image-resizing-api>

upvoted 1 times

zanhsieh 10 months, 4 weeks ago

Selected Answer: A

A.

GKE endpoint is external facing, Opt C and D are out. Also exposing to endpoint won't expose all containers in the GKE cluster - if one service exposes to 4000 nodes with containers then does this mean the GKE would need to update 4000 times? This just doesn't make sense. Opt E use service name, in other words, CNAME, so it still has to go through Cloud DNS. Hence the opt A shall be correct.

upvoted 1 times

gc\_exam2022 11 months, 1 week ago

Selected Answer: C

It's B

upvoted 1 times

closer89 11 months, 4 weeks ago

Selected Answer: B

both A and B are valid

Option A, DNS A record maps service FQDN to IP address, fqdn like service-name.default.svc.cluster.local  
B is more easier, just use http://service-name

upvoted 1 times

telp 1 year, 3 months ago

Selected Answer: B

answer is B because client are in the same cluster so service name can be used.

upvoted 1 times

Mark123321 1 year, 4 months ago

Selected Answer: C

Question reads "IP address" and I don't think that using B the IP can be obtained.

upvoted 1 times

Mark123321 1 year, 4 months ago

C answer is suggesting to define endpoint in the service and others can use that endpoint (reading its name from a variable) to ask the service what IP it has, that why I think C is correct.

upvoted 1 times

ajipeggy 1 year, 5 months ago

Selected Answer: B

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

"In Kubernetes, service discovery is implemented with automatically generated service names that map to the Service's IP address. Service names follow a standard specification: as follows: my-svc.my-namespace.svc.cluster-domain.example. Pods can also access external services through their names, such as example.com. "

upvoted 3 times

tomato123 1 year, 8 months ago

Selected Answer: B

B is correct

upvoted 3 times

kinoko1330 1 year, 8 months ago

Selected Answer: B

B is correct

upvoted 1 times

alex8081 1 year, 8 months ago

But qn states: ".to get the IP address of the service". Or not?

upvoted 1 times

jdx000 1 year, 9 months ago

Selected Answer: B

Should be B

upvoted 1 times

 **nazonazonazo** 2 years, 2 months ago

B is collect.

If client and server are in same namespace, C is collect. But in this case, no condition of namespace. So client pod must be use server service name.

upvoted 1 times

 **zaxxon** 2 years, 2 months ago

D: see <https://cloud.google.com/endpoints/docs/openapi/get-started-kubernetes-engine#configuring-endpoints-dns>

upvoted 1 times

 **ralf\_cc** 2 years, 10 months ago

A - use SVC to expose your pod, and get the cluster DNS service to get the IP

upvoted 1 times

Question #15

Topic 1

You are using Cloud Build to build and test application source code stored in Cloud Source Repositories. The build process requires a build tool not available in the Cloud Build environment.

What should you do?

- A. Download the binary from the internet during the build process.
- B. Build a custom cloud builder image and reference the image in your build steps.
- C. Include the binary in your Cloud Source Repositories repository and reference it in your build scripts.
- D. Ask to have the binary added to the Cloud Build environment by filing a feature request against the Cloud Build public Issue Tracker.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **fraloca** Highly Voted 3 years, 4 months ago

B is correct answer

[https://cloud.google.com/cloud-build/docs/configuring-builds/use-community-and-custom-builders#creating\\_a\\_custom\\_builder](https://cloud.google.com/cloud-build/docs/configuring-builds/use-community-and-custom-builders#creating_a_custom_builder)  
upvoted 9 times

 **syu31svc** 2 years, 10 months ago

I agree

upvoted 2 times

 **meh\_33** 1 year, 7 months ago

If the task you want to perform requires capabilities that are not provided by a public image, a supported builder, or a community-contributed builder, you can build your own image and use it in a build step.

B

upvoted 1 times

 **dscifo** Most Recent 6 months ago

**Selected Answer: B**

I think is a generic solution because I can use it in other projects.

upvoted 1 times

 **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: B**

B is correct.

upvoted 1 times

 **gc\_exam2022** 11 months, 1 week ago

**Selected Answer: B**

B is correct

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: B**

B is correct

Question #16

Topic 1

You are deploying your application to a Compute Engine virtual machine instance. Your application is configured to write its log files to disk. You want to view the logs in Stackdriver Logging without changing the application code.

What should you do?

- A. Install the Stackdriver Logging Agent and configure it to send the application logs.
- B. Use a Stackdriver Logging Library to log directly from the application to Stackdriver Logging.
- C. Provide the log file folder path in the metadata of the instance to configure it to send the application logs.
- D. Change the application to log to /var/log so that its logs are automatically sent to Stackdriver Logging.

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **santoshchauhan** 1 month, 3 weeks ago

**Selected Answer: A**

A. The Stackdriver Logging Agent is a software agent that can collect logs from various sources on your virtual machine and send them to Stackdriver Logging. By configuring the agent, you can specify custom log file paths, and the agent will forward these logs to Stackdriver Logging. This is the most direct and least intrusive method when you cannot or do not want to change the application code.

upvoted 1 times

 **\_Puru\_** 7 months ago

**Selected Answer: A**

Correct answer is A

upvoted 1 times

 **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: A**

A is correct

upvoted 1 times

 **gc\_exam2022** 11 months, 1 week ago

Correct Answer: A

upvoted 1 times

 **zevexWM** 1 year, 3 months ago

A is correct here

upvoted 1 times

 **meh\_33** 1 year, 7 months ago

A is correct -We need to install stackdriver agent in the VM

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: A**

A is correct

upvoted 3 times

 **tomato123** 1 year, 8 months ago

A is correct

upvoted 1 times

 **javibadillo** 1 year, 10 months ago

**Selected Answer: A**

<https://cloud.google.com/logging/docs/agent/logging/installation>

upvoted 2 times

 **syu31svc** 2 years, 10 months ago

<https://cloud.google.com/logging/docs/agent/logging/installation>:

"The Logging agent streams logs from your VM instances and from selected third-party software packages to Cloud Logging"

Question #17

Topic 1

Your service adds text to images that it reads from Cloud Storage. During busy times of the year, requests to Cloud Storage fail with an HTTP 429

"Too Many

Requests" status code.

How should you handle this error?

- A. Add a cache-control header to the objects.
- B. Request a quota increase from the GCP Console.
- C. Retry the request with a truncated exponential backoff strategy.
- D. Change the storage class of the Cloud Storage bucket to Multi-regional.

**Correct Answer: C**

Reference:

<https://developers.google.com/gmail/api/v1/reference/quota>*Community vote distribution*

C (100%)

**✉ santoshchauhan** 1 month, 3 weeks ago**Selected Answer: C**

C. Implementing a truncated exponential backoff strategy is a recommended practice for handling 429 errors. This approach involves waiting a short period before retrying the failed request, with the wait time increasing (up to a maximum limit) with each successive retry. This can help alleviate the load causing the rate limit to be hit and is a well-established pattern for handling such errors in distributed systems.

upvoted 1 times

**✉ \_Puru\_** 7 months ago**Selected Answer: C**

Exponential backoff formula will generate delay

upvoted 1 times

**✉ \_\_rajan\_\_** 7 months, 1 week ago**Selected Answer: C**

C is Correct

upvoted 1 times

**✉ Chuckq** 1 year ago

C is a must or your code won't do the job. But Request a quota increase will come afterwards or it will be a pain rely on exponential backoff...  
upvoted 1 times

**✉ omermahgoub** 1 year, 3 months ago

To handle HTTP 429 "Too Many Requests" errors when requesting data from Cloud Storage, you should retry the request with a truncated exponential backoff strategy (C).

An HTTP 429 "Too Many Requests" status code indicates that the server is receiving too many requests and is unable to handle them all. In this situation, it is generally best to retry the request after a period of time, using a truncated exponential backoff strategy. This involves retrying the request with increasingly longer delays between each retry, up to a maximum delay. The delays can be generated using an exponential backoff formula, which increases the delay by a power of two on each retry. The retries can be truncated at a maximum delay to prevent the retries from taking too long.

upvoted 1 times

**✉ omermahgoub** 1 year, 3 months ago

Adding a cache-control header to the objects (A) may not be sufficient to address the issue, as it only affects how the objects are cached by clients. Requesting a quota increase from the GCP Console (B) may help to alleviate the issue, but it may not be a sufficient solution on its own. Changing the storage class of the Cloud Storage bucket to Multi-regional (D) may also not be sufficient to address the issue, as it only affects the location of the data and does not directly address the issue of too many requests.

upvoted 1 times

**✉ tomato123** 1 year, 8 months ago**Selected Answer: C**

C is correct

upvoted 3 times

**✉ herocc** 2 years, 3 months ago

C is right one, choose proper backoff strategy

upvoted 1 times

✉️  **saurabh1805** 3 years, 5 months ago

C is correct option here

upvoted 3 times

✉️  **arra** 3 years, 1 month ago

[https://cloud.google.com/storage/docs/json\\_api/v1/status-codes](https://cloud.google.com/storage/docs/json_api/v1/status-codes)

upvoted 2 times

✉️  **syu31svc** 2 years, 10 months ago

"A Cloud Storage JSON API usage limit was exceeded. If your application tries to use more than its limit, additional requests will fail. Throttle your client's requests, and/or use truncated exponential backoff."

Question #18

Topic 1

You are building an API that will be used by Android and iOS apps. The API must:

- \* Support HTTPS
- \* Minimize bandwidth cost
- \* Integrate easily with mobile apps

Which API architecture should you use?

- A. RESTful APIs
- B. MQTT for APIs
- C. gRPC-based APIs
- D. SOAP-based APIs

**Correct Answer: A**

Reference:

<https://www.devteam.space/blog/how-to-build-restful-api-for-your-mobile-app/>

*Community vote distribution*

C (71%)

A (29%)

✉️  **p4**  2 years, 3 months ago

Isn't C (gRPC) better because of the lower bandwidth (binary format)?

It can be used in mobile apps and supports HTTP(s)

upvoted 9 times

✉️  **KhornesFang** 1 year, 11 months ago

Probably A is the best solution for "Integrate easily with mobile apps" requirement

upvoted 1 times

✉️  **santoshchauhan**  1 month, 3 weeks ago

**Selected Answer: C**

C. gRPC-based APIs are designed to minimize bandwidth by using Protocol Buffers, a method of serializing structured data in an efficient and extensible format. gRPC is modern, fast, and supports HTTPS by default. It also provides features like streaming and efficient connection management, which can be advantageous for mobile apps that require efficient use of bandwidth and battery life.

upvoted 1 times

✉️  **theseawillclaim** 2 months, 2 weeks ago

**Selected Answer: C**

I'm going with gRPC as it is a Google Product, and we're talking about a GCP exam, so... REST APIs would still serve the purpose though.

upvoted 1 times

 **wanrltw** 5 months, 2 weeks ago

**Selected Answer: A**

A, according to <https://www.exam-answer.com/api-architecture-for-android-ios-apps>

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: C**

C is correct as it supports IOS and Android with low latency.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: C**

Answer is C: gRPC is a high-performance, open-source universal RPC framework which supports IOS and Android as well.

upvoted 1 times

 **maxdanny** 8 months, 1 week ago

**Selected Answer: A**

<https://www.exam-answer.com/api-architecture-for-android-ios-apps#:~:text=The%20most%20suitable%20API%20architecture,used%20for%20building%20web%20APIs>.

upvoted 1 times

 **gc\_exam2022** 11 months, 1 week ago

**Selected Answer: C**

gRPC-based APIs

upvoted 1 times

 **daran** 1 year, 1 month ago

gRPC supports ios and andriod also.

upvoted 1 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: C**

<https://www.imaginarycloud.com/blog/grpc-vs-rest/>

gRPC architectural style has promising features that can (and should) be explored. It is an excellent option for working with multi-language systems, real-time streaming, and for instance, when operating an IoT system that requires light-weight message transmission such as the serialized Protobuf messages allow. Moreover, gRPC should also be considered for mobile applications since they do not need a browser and can benefit from smaller messages, preserving mobiles' processors' speed.

upvoted 2 times

 **Foxal** 1 year, 2 months ago

**Selected Answer: C**

The correct is C

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

To support HTTPS, minimize bandwidth cost, and integrate easily with mobile apps, you should use gRPC-based APIs (C).

gRPC (gRPC Remote Procedure Calls) is a modern, high-performance, open-source remote procedure call (RPC) framework that can be used to build APIs. It uses HTTP/2 as the underlying transport protocol and Protocol Buffers as the encoding format. gRPC is designed to be low-bandwidth, low-latency, and easily integrable with mobile apps. It also supports HTTPS out of the box.

RESTful APIs (A) are a popular choice for building APIs, but they may not be as efficient as gRPC in terms of bandwidth usage, especially for APIs that transfer large amounts of data. MQTT (B) is a lightweight messaging protocol that is often used in IoT applications, but it may not be well-suited for building APIs as gRPC. SOAP-based APIs (D) are an older style of API that has largely been replaced by more modern alternatives like gRPC.

upvoted 4 times

fraloca 1 year, 6 months ago

Selected Answer: C

I think that the best answer is C:

- gRPC supports HTTPS;
- minimize bandwidth because use a binary payload;
- It is easy to integrate because it generate stubs and skeletons that hide the connection details.

<https://cloud.google.com/blog/products/api-management/understanding-grpc-openapi-and-rest-and-when-to-use-them>

upvoted 2 times

ash\_meharun 1 year, 6 months ago

REST APIs are not bound to client-side technology. This allows you to access these APIs from a client-side web project, iOS app, IoT device, Windows phone.

In the problem statement, they mentioned iOS and Android.

It is not officially supported by gRPC

So that points to option A, otherwise, C is nearest.

upvoted 2 times

tomato123 1 year, 8 months ago

Selected Answer: A

A is correct

upvoted 2 times

Blueocean 2 years, 3 months ago

Agreed Option A is correct

upvoted 2 times

Question #19

Topic 1

Your application takes an input from a user and publishes it to the user's contacts. This input is stored in a table in Cloud Spanner. Your application is more sensitive to latency and less sensitive to consistency.

How should you perform reads from Cloud Spanner for this application?

- A. Perform Read-Only transactions.
- B. Perform stale reads using single-read methods.
- C. Perform strong reads using single-read methods.
- D. Perform stale reads using read-write transactions.

Correct Answer: D

Reference:

<https://cloud.google.com/solutions/best-practices-cloud-spanner-gaming-database>

Community vote distribution

B (100%)

emmet [Highly Voted] 3 years, 11 months ago

As mentioned here <https://cloud.google.com/spanner/docs/reference/rest/v1/TransactionOptions> read-write transaction type has no options, there is no way to make stale reads with this transaction type, so D is definitely wrong.

In the question, low latency is more critical than consistency, so C is not an option. Read-Only transactions can do stale reads as well as SingleRead methods, but in the documentation [https://cloud.google.com/spanner/docs/transactions#read-only\\_transactions](https://cloud.google.com/spanner/docs/transactions#read-only_transactions), they encourage to use SingleRead methods where possible.

My vote is B)

upvoted 15 times

gcper 3 years, 6 months ago

I agree with B because of this statement: "Your application is more sensitive to latency and less sensitive to consistency."

Also if your application is latency sensitive but tolerant of stale data, then stale reads can provide performance benefits.

source: <https://cloud.google.com/spanner/docs/reads>

upvoted 6 times

 **syu31svc** Highly Voted  2 years, 10 months ago

<https://cloud.google.com/spanner/docs/reads>:

"A stale read is read at a timestamp in the past. If your application is latency sensitive but tolerant of stale data, then stale reads can provide performance benefits."

B is the answer since the qn is asking about reading from Cloud Spanner; no writes involved

upvoted 6 times

 **santoshchauhan** Most Recent  1 month, 3 weeks ago

**Selected Answer: B**

B. Perform stale reads using single-read methods: Stale reads (also known as bounded staleness reads) can execute with lower latency because they can serve data from a timestamp in the recent past and do not have to wait for ongoing writes to be completed. This allows the application to trade off some consistency for lower latency, which is suitable for this scenario.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: B**

It Should be B.

Since the application is more sensitive to latency and less sensitive to consistency performing stale reads is the best choice here. It will provide low latency at the cost of potentially returning stale data.

upvoted 1 times

 **tuanbo91** 1 year, 4 months ago

**Selected Answer: B**

Should be B

upvoted 1 times

 **jcataluna** 1 year, 4 months ago

**Selected Answer: B**

B is correct

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: B**

B is correct

upvoted 3 times

 **tomato123** 1 year, 8 months ago

B is correct

upvoted 1 times

 **arobertoX** 2 years ago

in my humble opinion it's D because the application must write on user contacts table.

upvoted 2 times

 **maxdanny** 1 year, 9 months ago

the question is "How should you perform reads from Cloud Spanner for this application?", so only read transaction....

upvoted 1 times

 **herocc** 2 years, 3 months ago

B is right, data consistency is less sensitive.

upvoted 1 times

 **ParagSanyashiv** 2 years, 3 months ago

**Selected Answer: B**

B is the correct answer

upvoted 1 times

 **amber4eg** 2 years, 5 months ago

"Your application takes an input from a user and publishes it to the user's contacts"

What does "publishes" mean? If "write to database" than my vote is D

upvoted 1 times

 **saurabh1805** 3 years, 5 months ago

B is correct answer here.

upvoted 4 times

Question #20

Topic 1

Your application is deployed in a Google Kubernetes Engine (GKE) cluster. When a new version of your application is released, your CI/CD tool updates the spec.template.spec.containers[0].image value to reference the Docker image of your new application version. When the Deployment object applies the change, you want to deploy at least 1 replica of the new version and maintain the previous replicas until the new replica is healthy.

Which change should you make to the GKE Deployment object shown below?

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: ecommerce-frontend-deployment
spec:
  replicas: 3
  selector:
    matchLabels:
      app: ecommerce-frontend
  template:
    metadata:
      labels:
        app: ecommerce-frontend
    spec:
      containers:
        - name: ecommerce-frontend-webapp
          image: ecommerce-frontend-webapp:1.7.9
          ports:
            - containerPort: 80
```

- A. Set the Deployment strategy to RollingUpdate with maxSurge set to 0, maxUnavailable set to 1.
- B. Set the Deployment strategy to RollingUpdate with maxSurge set to 1, maxUnavailable set to 0.
- C. Set the Deployment strategy to Recreate with maxSurge set to 0, maxUnavailable set to 1.
- D. Set the Deployment strategy to Recreate with maxSurge set to 1, maxUnavailable set to 0.

**Correct Answer: D**

*Community vote distribution*

B (100%)

 **saurabh1805** Highly Voted 3 years, 5 months ago

I will go with Option B for this.

RollingUpdate: New pods are added gradually, and old pods are terminated gradually  
Recreate: All old pods are terminated before any new pods are added

Question ask us to retain current version hence rolling update is better option here.

upvoted 18 times

 **syu31svc** Highly Voted  2 years, 10 months ago

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

"The simplest way to take advantage of surge upgrade is to configure maxSurge=1 maxUnavailable=0. This means that only 1 surge node can be added to the node pool during an upgrade so only 1 node will be upgraded at a time. This setting is superior to the existing upgrade configuration (maxSurge=0 maxUnavailable=1) because it speeds up Pod restarts during upgrades while progressing conservatively."

Answer is B

upvoted 7 times

 **santoshchauhan** Most Recent  1 month, 3 weeks ago

**Selected Answer: B**

B. Set the Deployment strategy to RollingUpdate with maxSurge set to 1, maxUnavailable set to 0:

maxSurge set to 1 allows the Deployment to exceed the desired number of Pods by one, permitting the creation of an additional new Pod before terminating the old ones, which aligns with the requirement.

maxUnavailable set to 0 ensures that all existing Pods must remain available during the update, which again meets the requirement.

upvoted 1 times

 **theseawillclaim** 2 months, 2 weeks ago

**Selected Answer: B**

"maxSurge=1" means that at least one VM has to stay up during the RU process.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: B**

Option B is the correct one.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

To deploy at least 1 replica of the new version and maintain the previous replicas until the new replica is healthy, you should set the Deployment strategy to RollingUpdate with maxSurge set to 1 and maxUnavailable set to 0 (B).

The RollingUpdate Deployment strategy allows you to specify the number of replicas that can be created or removed at a time as part of the update process. The maxSurge parameter specifies the maximum number of replicas that can be created in excess of the desired number of replicas, and the maxUnavailable parameter specifies the maximum number of replicas that can be unavailable at any given time.

By setting maxSurge to 1 and maxUnavailable to 0, you are telling the Deployment to create at least 1 new replica of the new version and to maintain all of the previous replicas until the new replica is healthy. This will ensure that at least 1 replica of the new version is always available while allowing the Deployment to gradually roll out the update to the rest of the replicas.

upvoted 2 times

 **omermahgoub** 1 year, 3 months ago

The Recreate Deployment strategy (C and D) would not be suitable for this use case, as it would involve replacing all of the replicas at once rather than rolling out the update gradually.

upvoted 1 times

 **tuanbo91** 1 year, 4 months ago

**Selected Answer: B**

B is obvious

upvoted 1 times

 **jcataluna** 1 year, 4 months ago

**Selected Answer: B**

B is correct

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: B**

B is correct

upvoted 2 times

 **herocc** 2 years, 3 months ago

Obviously it's B

upvoted 1 times

 **ParagSanyashiv** 2 years, 3 months ago

**Selected Answer: B**

Answer is B

upvoted 1 times

 **ParagSanyashiv** 2 years, 3 months ago

**Selected Answer: B**

Answer is B

upvoted 1 times

 **Flavio80** 2 years, 3 months ago

the answer is B.

upvoted 1 times

 **mishsanjay** 3 years, 2 months ago

Recreate can't be maintain previous replica. Answer must be B.

upvoted 3 times

 **donchick** 3 years, 4 months ago

B is correct answer

upvoted 2 times

 **beranm** 3 years, 4 months ago

You are not maintaining anything with Recreate strategy

upvoted 1 times

Question #21

*Topic 1*

You plan to make a simple HTML application available on the internet. This site keeps information about FAQs for your application. The application is static and contains images, HTML, CSS, and Javascript. You want to make this application available on the internet with as few steps as possible.

What should you do?

- A. Upload your application to Cloud Storage.
- B. Upload your application to an App Engine environment.
- C. Create a Compute Engine instance with Apache web server installed. Configure Apache web server to host the application.
- D. Containerize your application first. Deploy this container to Google Kubernetes Engine (GKE) and assign an external IP address to the GKE pod hosting the application.

**Correct Answer: A**

Reference:

<https://cloud.google.com/storage/docs/hosting-static-website>

*Community vote distribution*

A (100%)

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: A**

Option A: As we can host static applications on Cloud Storage.  
upvoted 1 times

 **studyingveryhard** 9 months, 1 week ago

Explanation of Correct Answer

Upload your application to Cloud Storage.

Cloud Storage is the correct answer because it is the simplest way to host a static website containing images, HTML, CSS, and JavaScript. Simply upload the static files to Cloud Storage, and they can be served on the internet with minimal configuration. Cloud Storage provides high availability and reliability, ensuring a fast and secure user experience.

Source: <https://examlab.co/google/google-cloud-professional-cloud-developer>  
upvoted 1 times

 **gc\_exam2022** 11 months, 1 week ago

**Selected Answer: A**

Correct Answer: A  
upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: A**

A is correct  
upvoted 3 times

 **kinoko1330** 1 year, 8 months ago

**Selected Answer: A**

A is correct  
upvoted 1 times

 **herocc** 2 years, 3 months ago

A is right  
upvoted 1 times

 **syu31svc** 2 years, 10 months ago

A is correct; provided link supports it  
upvoted 4 times

 **saurabh1805** 3 years, 5 months ago

A, if its static then quickest way is via cloud storage.  
upvoted 3 times

Question #22

Topic 1

Your company has deployed a new API to App Engine Standard environment. During testing, the API is not behaving as expected. You want to monitor the application over time to diagnose the problem within the application code without redeploying the application. Which tool should you use?

- A. Stackdriver Trace
- B. Stackdriver Monitoring
- C. Stackdriver Debug Snapshots
- D. Stackdriver Debug Logpoints

**Correct Answer: B**

Reference:

<https://rominirani.com/gcp-stackdriver-tutorial-debug-snapshots-traces-logging-and-logpoints-1ba49e4780e6>

Community vote distribution

D (69%)

B (25%)

6%

✉️  **saurabh1805** Highly Voted 3 years, 5 months ago

D is correct answer here.

upvoted 7 times

✉️  **theseawillclaim** Most Recent 2 months, 3 weeks ago

**Selected Answer: D**

You want to see what is the problem in the code without altering it. => Logpoints.

upvoted 1 times

✉️  **wanrltw** 5 months, 2 weeks ago

You want to MONITOR the application - > Stackdriver MONITORING

upvoted 1 times

✉️  **wanrltw** 5 months, 2 weeks ago

<https://www.exam-answer.com/which-tool-should-use-monitor-application-stackdriver-monitoring>

upvoted 1 times

✉️  **\_rajan\_** 7 months, 1 week ago

**Selected Answer: C**

Option C: Stackdriver Debug Snapshots allow you to inspect the state of an application at any code location in production, without stopping or slowing down your applications.

upvoted 1 times

✉️  **maxdanny** 8 months, 1 week ago

**Selected Answer: B**

The API required a monitoring tool, not troubleshooting

upvoted 1 times

✉️  **gc\_exam2022** 11 months, 1 week ago

**Selected Answer: D**

D. Stackdriver Debug Logpoints

upvoted 1 times

✉️  **omermahgoub** 1 year, 3 months ago

Stackdriver Debug Snapshots is a feature of Stackdriver Debugger that allows you to capture a snapshot of the state of your application at a specific point in time. This snapshot includes information about the variables and the call stack at the time the snapshot was taken, as well as any log output that was generated.

To use Stackdriver Debug Snapshots to monitor your application, you would need to take periodic snapshots of your application and then analyze the snapshot data to identify any issues or problems. However, this would not be a real-time monitoring solution, and it would not allow you to continuously monitor your application for issues. Instead, it would be a way to investigate issues after they have occurred, by examining the state of the application at the time the snapshot was taken.

upvoted 1 times

✉️  **omermahgoub** 1 year, 3 months ago

Stackdriver Debug Logpoints is a feature of Stackdriver Debugger that allows you to insert logging statements into your code without modifying or redeploying your application. This can be useful for troubleshooting issues with your application, as it allows you to output data to the log without having to modify your code and redeploy the application.

To use Stackdriver Debug Logpoints to monitor your application, you would need to insert logpoints into your code at strategic points, and then analyze the log output to identify any issues or problems. However, this would not be a real-time monitoring solution, and it would not allow you to continuously monitor your application for issues. Instead, it would be a way to investigate issues after they have occurred, by examining the log output that was generated.

upvoted 1 times

✉️  **omermahgoub** 1 year, 3 months ago

Answer is B:

To monitor the application over time to diagnose a problem within the application code without redeploying the application, you should use Stackdriver Monitoring (B). Stackdriver Monitoring provides a range of tools that allow you to view and analyze performance metrics, traces, and logs for your application. This can help you identify and troubleshoot issues with your application.

upvoted 1 times

✉  **Pime13** 1 year, 4 months ago

**Selected Answer: D**

i think this question will become obsolete since Cloud debugger will be deprecated: Cloud Debugger is deprecated and will be shutdown May 31, 2023. See the deprecations page and release notes for more information.  
Cloud Debugger is deprecated and is scheduled for shutdown on May 31 2023. For an alternative, use the open source CLI tool, Snapshot Debugger.  
<https://cloud.google.com/debugger/docs/release-notes>

In thi context i'll say D

upvoted 2 times

✉  **ajipeggy** 1 year, 5 months ago

**Selected Answer: D**

" You want to monitor the application over time to diagnose the problem within the application code"

If it's only for moniroting it's B, but it mentions "within the code" so it should be D

upvoted 1 times

✉  **wanrltw** 5 months, 2 weeks ago

But it says that you want to "monitor the application over time" first, not that you want to start debugging it already.

upvoted 1 times

✉  **tab02733** 1 year, 6 months ago

**Selected Answer: B**

D can only be monitored for 24 hours.

For long-term monitoring, Cloud Monitoring is the best choice.

<https://cloud.google.com/monitoring/docs/monitoring-overview?hl=ja#uptime-checks>

I vote for B.

upvoted 3 times

✉  **ash\_meharun** 1 year, 6 months ago

If it requires just for testing purposes then option D because log points expire after 24 hours automatically, while monitoring keeps metrics for weeks.

upvoted 2 times

✉  **brunoguzzo18** 1 year, 8 months ago

**Selected Answer: D**

<https://cloud.google.com/debugger/docs/using/logpoints>

upvoted 1 times

✉  **tomato123** 1 year, 8 months ago

**Selected Answer: D**

D is correct

upvoted 3 times

✉  **javibadillo** 1 year, 10 months ago

**Selected Answer: D**

<https://cloud.google.com/debugger/docs/using/logpoints>

upvoted 1 times

✉  **morenocasado** 2 years ago

**Selected Answer: D**

Community choice is D

upvoted 1 times

✉  **[Removed]** 2 years, 9 months ago

D) is the answer as the api is not behaving as expected we have to put some logs in order to understand what is going one. So we can analys logs on a period time. With C) is only one shot not over time.

upvoted 3 times

✉  **syu31svc** 2 years, 10 months ago

<https://cloud.google.com/debugger/docs/using/logpoints>

Answer is D

upvoted 2 times

You want to use the Stackdriver Logging Agent to send an application's log file to Stackdriver from a Compute Engine virtual machine instance. After installing the Stackdriver Logging Agent, what should you do first?

- A. Enable the Error Reporting API on the project.
- B. Grant the instance full access to all Cloud APIs.
- C. Configure the application log file as a custom source.
- D. Create a Stackdriver Logs Export Sink with a filter that matches the application's log entries.

**Correct Answer: B***Community vote distribution*

C (91%)

9%

**✉️**  **santoshchauhan** 1 month, 3 weeks ago**Selected Answer: C**

C. Configuring the application log file as a custom source is the crucial step after installing the Stackdriver Logging Agent. This involves specifying the path to the application's log file in the agent's configuration files, so the agent knows where to find and how to parse your custom log files.

upvoted 1 times

**✉️**  **nicgas** 4 months, 3 weeks ago**Selected Answer: C**

it's C

upvoted 1 times

**✉️**  **\_rajan\_** 7 months, 1 week ago**Selected Answer: C**

We need to configure the log source in StackDriver agent to read the logs.

upvoted 1 times

**✉️**  **maxdanny** 8 months, 1 week ago**Selected Answer: C**

After installing StackDriver agent, you need to configure the new source from which to read the logs to be sent

upvoted 1 times

**✉️**  **closer89** 11 months, 4 weeks ago**Selected Answer: C**

first C then D

upvoted 1 times

 **tab02733** 1 year, 6 months ago

**Selected Answer: B**

API must be allowed to output logs.

<https://cloud.google.com/logging/docs/agent/ops-agent/authorization>

First, do B, then do C.

I vote for B.

upvoted 1 times

 **GofX** 1 year, 5 months ago

Answer B tells us to authorize the instance to ALL Cloud APIs. I don't see a world where this answer can be right as it breaks the least privilege principle quite heavily.

upvoted 5 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: C**

C is correct

upvoted 3 times

 **javibadillo** 1 year, 10 months ago

**Selected Answer: C**

<https://cloud.google.com/logging/docs/agent/configuration>

upvoted 1 times

 **herocc** 2 years, 3 months ago

C is right

upvoted 2 times

 **ParagSanyashiv** 2 years, 3 months ago

**Selected Answer: C**

Answer is C

upvoted 1 times

 **syu31svc** 2 years, 10 months ago

Send to Stackdriver so answer is C then

upvoted 3 times

 **maleksah** 3 years, 3 months ago

Answer is C

upvoted 2 times

 **saurabh1805** 3 years, 5 months ago

C is my answer.

upvoted 3 times

 **fraloca** 3 years, 4 months ago

[https://cloud.google.com/logging/docs/agent/configuration#streaming\\_logs\\_from\\_additional\\_inputs](https://cloud.google.com/logging/docs/agent/configuration#streaming_logs_from_additional_inputs)

upvoted 1 times

 **mlyu** 3 years, 9 months ago

Question #24

Topic 1

Your company has a BigQuery data mart that provides analytics information to hundreds of employees. One user of wants to run jobs without interrupting important workloads. This user isn't concerned about the time it takes to run these jobs. You want to fulfill this request while minimizing cost to the company and the effort required on your part.

What should you do?

- A. Ask the user to run the jobs as batch jobs.
- B. Create a separate project for the user to run jobs.
- C. Add the user as a job.user role in the existing project.

D. Allow the user to run jobs when important workloads are not running.

**Correct Answer: B**

*Community vote distribution*

A (100%)

 **syu31svc** Highly Voted 2 years, 10 months ago

Option A makes the most sense

B is wrong since it will incur more costs which is not what the qn wants

C is definitely out as creating roles is not what the qn is asking for

D is wrong as it would not minimise effort

upvoted 10 times

 **mlyu** Highly Voted 3 years, 9 months ago

Answer is A

<https://cloud.google.com/bigquery/docs/running-queries#batch>

upvoted 5 times

 **mastodilu** 2 years, 11 months ago

this seems like the perfect scenario for batch jobs

upvoted 1 times

 **santoshchauhan** Most Recent 1 month, 3 weeks ago

**Selected Answer: A**

A. Ask the user to run the jobs as batch jobs.

Running BigQuery jobs as batch jobs is a good solution when there is no concern about how long it takes to complete these jobs. Batch jobs executed when BigQuery has available resources, which ensures that they do not interfere with high-priority workloads. This is also a cost-effective solution since it does not require additional resources or the overhead of managing a separate project. BigQuery automatically prioritizes interactive jobs over batch jobs, so important workloads are less likely to be interrupted.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: A**

Batch jobs in BigQuery are not subject to the usual quota limits and do not count towards your concurrent rate limit, which makes them suitable for running large queries and reducing costs. They are executed when system resources become available, so there might be a delay, but since the user isn't concerned about the time it takes to run these jobs, this would be a suitable solution

upvoted 1 times

 **gc\_exam2022** 11 months, 1 week ago

**Selected Answer: A**

Correct Answer: A

upvoted 1 times

 **sbonesi** 11 months, 3 weeks ago

**Selected Answer: A**

Definitely the correct answer is A

upvoted 2 times

 **omermahgoub** 1 year, 3 months ago

Option A is the correct answer. By running the jobs as batch jobs, the user can specify a priority level for their jobs, allowing them to be run when system resources are available. This minimizes the impact on important workloads and allows the user to run their jobs without interrupting other users. Additionally, batch jobs are generally less expensive to run than interactive queries, so this option would also minimize cost to the company. Option B is not a good solution because it would involve creating a separate project for the user to run their jobs, which would add unnecessary complexity and effort. Option C is not a good solution because the job.user role does not provide any additional permissions beyond those of the bigquery.user role, which the user likely already has. Option D is not a good solution because it would require manual intervention to determine when important workloads are not running, which would be difficult to manage and could lead to delays in running the user's jobs.

upvoted 1 times

 **jcataluna** 1 year, 4 months ago

**Selected Answer: A**

A is correct

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: A**

A is correct

upvoted 2 times

 **herocc** 2 years, 3 months ago

A is right

upvoted 1 times

 **ParagSanyashiv** 2 years, 3 months ago

**Selected Answer: A**

A is more suitable answer here

upvoted 4 times

 **saurabh1805** 3 years, 5 months ago

A is best answer

upvoted 3 times

Question #25

*Topic 1*

You want to notify on-call engineers about a service degradation in production while minimizing development time.

What should you do?

- A. Use Cloud Function to monitor resources and raise alerts.
- B. Use Cloud Pub/Sub to monitor resources and raise alerts.
- C. Use Stackdriver Error Reporting to capture errors and raise alerts.
- D. Use Stackdriver Monitoring to monitor resources and raise alerts.

**Correct Answer: A**

*Community vote distribution*

D (100%)

 **emmet** Highly Voted 3 years, 11 months ago

I don't think the correct answer is A) Cloud Functions are not about monitoring at all, but I have found one mention of using cloud functions for monitoring: <https://cloud.google.com/solutions/serverless-web-performance-monitoring-using-cloud-functions>. But the mentioned article is about WEB page performance and it does require a lot of efforts. The question does not have info about the kind of service to monitor, so I think the answer should be D) - "Use Stackdriver Monitoring to monitor resources and raise alerts"

upvoted 11 times

 **syu31svc** Highly Voted 2 years, 10 months ago

This is D for sure

upvoted 9 times

 **santoshchauhan** Most Recent 1 month, 3 weeks ago

Selected Answer: D

D. Use Stackdriver Monitoring to monitor resources and raise alerts.

Stackdriver Monitoring provides out-of-the-box and custom monitoring capabilities for Google Cloud resources and applications. It allows you to create alerting policies that notify you when certain system metrics violate user-defined thresholds. This is a quick and effective way to set up alerts for resource monitoring and service degradation without the need for extensive development time.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

Selected Answer: D

Stackdriver Monitoring is the best option here.

upvoted 1 times

 **closer89** 11 months, 4 weeks ago

Selected Answer: D

D

Error Reporting is not about service degradation, more, Error Reporting uses Monitoring to send alerts.

<https://cloud.google.com/error-reporting/docs/notifications>

upvoted 1 times

 **zevexWM** 1 year, 3 months ago

Selected Answer: D

D is correct for monitoring.

I'm baffled by the "correct" answers given by the site, 80% of the time they are wrong.

upvoted 1 times

 **jcataluna** 1 year, 4 months ago

Selected Answer: D

D is correct

upvoted 1 times

 **tomato123** 1 year, 8 months ago

Selected Answer: D

D is correct

upvoted 3 times

 **herocc** 2 years, 3 months ago

D is right one

upvoted 4 times

 **GoReplyGCPExam** 2 years ago

why not C?

upvoted 1 times

 **rzabcio** 1 year, 9 months ago

Because "service DEGRADATION" is in question, not errors.

upvoted 1 times

 **ParagSanyashiv** 2 years, 3 months ago

Selected Answer: D

StackDriver Monitoring should be used to monitor and raising the disputes.

upvoted 3 times

 **Flavio80** 2 years, 3 months ago

This is D for sure

upvoted 1 times

 **ralf\_cc** 2 years, 10 months ago

D - <https://cloud.google.com/blog/products/gcp/drilling-down-into-stackdriver-service-monitoring>

upvoted 2 times

 **saurabh1805** 3 years, 5 months ago

D is correct answer here.

upvoted 5 times

 **google\_learner123** 3 years, 7 months ago

Answer is D

upvoted 4 times

Question #26

Topic 1

You are writing a single-page web application with a user-interface that communicates with a third-party API for content using XMLHttpRequest. The data displayed on the UI by the API results is less critical than other data displayed on the same web page, so it is acceptable for some requests to not have the API data displayed in the UI. However, calls made to the API should not delay rendering of other parts of the user interface. You want your application to perform well when the API response is an error or a timeout.

What should you do?

- A. Set the asynchronous option for your requests to the API to false and omit the widget displaying the API results when a timeout or error is encountered.
- B. Set the asynchronous option for your request to the API to true and omit the widget displaying the API results when a timeout or error is encountered.
- C. Catch timeout or error exceptions from the API call and keep trying with exponential backoff until the API response is successful.
- D. Catch timeout or error exceptions from the API call and display the error response in the UI widget.

**Correct Answer: A**

*Community vote distribution*

B (100%)

 **[Removed]** Highly Voted 3 years, 10 months ago

Answer is B.

Api should not delay rendering: asynchronous

Application perform well when Api error or timeout: omit the widget

upvoted 11 times

 **syu31svc** Highly Voted 2 years, 9 months ago

Correct answer is B

Asynchronous handling provides the ability to call the API in the background without blocking the rendering of other elements. If the response received it can be rendered or omitted if a timeout occurs.

upvoted 6 times

 **santoshchauhan** Most Recent 1 month, 3 weeks ago

Selected Answer: B

B. Asynchronous requests allow the browser to continue processing other tasks while waiting for the API response. If the response is an error a timeout, you can handle this gracefully by not displaying the widget or showing a message indicating that the data couldn't be loaded. This way, the performance of the rest of your page remains unaffected.

upvoted 1 times

 **dscifo** 6 months ago

**Selected Answer: B**

About synchronous=true is more comfortable for user experience.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: B**

Correct Answer B.

upvoted 1 times

 **maxdanny** 8 months, 1 week ago

**Selected Answer: B**

Setting the asynchronous option to true means that the requests will not block the main thread and will be executed in the background. Furthermore, so as written in the description the widget can be omitted

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

A is not the correct answer because setting the asynchronous option for the API request to false will block rendering of the user interface until API response is received. This can cause a delay in rendering other parts of the user interface and negatively impact the performance of the application.

B is the correct answer because setting the asynchronous option for the API request to true allows the user interface to continue rendering while the API request is being processed, which improves the performance of the application. Omitting the widget displaying the API results when a timeout or error is encountered allows the application to continue functioning without waiting for a successful API response.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: B**

B is correct

upvoted 3 times

 **herocc** 2 years, 3 months ago

B is right one

upvoted 1 times

 **ParagSanyashiv** 2 years, 3 months ago

**Selected Answer: B**

Understanding the question correctly, the answer should be B

upvoted 1 times

 **nehaxlpb** 2 years, 9 months ago

In will vote C, as we can catch the error and retry api again, it is like we us amazone we select a project and we see pricing and other content the picture are loaded asyn.

upvoted 2 times

 **mishsanjay** 3 years, 2 months ago

can't achieve using synchronous requests, so answer must be B.

upvoted 1 times

 **saurabh1805** 3 years, 5 months ago

Answer is B

upvoted 2 times

 **emmet** 3 years, 11 months ago

It should be B), isn't it?

Proposed answer A) uses synchronous behaviour so will block execution, it contradicts the question

upvoted 4 times

 **Alekshar** 3 years, 11 months ago

"calls made to the API should not delay rendering" -> so A cannot be the answer as it makes Synchronous requests. B is a better option

upvoted 1 times

You are creating a web application that runs in a Compute Engine instance and writes a file to any user's Google Drive. You need to configure the application to authenticate to the Google Drive API. What should you do?

- A. Use an OAuth Client ID that uses the <https://www.googleapis.com/auth/drive.file> scope to obtain an access token for each user.
- B. Use an OAuth Client ID with delegated domain-wide authority.
- C. Use the App Engine service account and <https://www.googleapis.com/auth/drive.file> scope to generate a signed JSON Web Token (JWT).
- D. Use the App Engine service account with delegated domain-wide authority.

**Correct Answer: B**

Reference:

<https://developers.google.com/drive/api/v3/about-auth>

*Community vote distribution*

A (93%)

7%

✉️  **santoshchauhan** 1 month, 3 weeks ago

**Selected Answer: A**

A. Use an OAuth Client ID that uses the <https://www.googleapis.com/auth/drive.file> scope to obtain an access token for each user.

To write a file to a user's Google Drive from a web application, you need to obtain permission from each user to access their Google Drive account. This is typically done using OAuth 2.0, where users are redirected to a consent screen where they grant your application permission to access their Google Drive with the specified scope.

upvoted 1 times

✉️  **Aeglas** 5 months ago

**Selected Answer: C**

correct answer is C. In the link you proposed about access view is clearly stated that you can prevent access to the underlying dataset and give access only to data that is in the view after applying the query.

upvoted 1 times

✉️  **\_rajan\_** 7 months, 1 week ago

**Selected Answer: A**

A is Correct.

upvoted 1 times

✉️  **telp** 1 year, 3 months ago

**Selected Answer: A**

A Because need to allow all users so not link to a domain

upvoted 2 times

✉️  **omermahgoub** 1 year, 3 months ago

I would've chosen option B if all users are in the same domain, it allows the application to authenticate to the Google Drive API with domain-wide authority, meaning that it will be able to access all users' Google Drive accounts within the domain. This is necessary because the application needs to be able to write a file to any user's Google Drive.

upvoted 1 times

✉️  **omermahgoub** 1 year, 3 months ago

But the question said any user (could be the same domain or different domains), In that case, option B would not be the best choice because it only allows for domain-wide authority. Instead, option A would be the best choice because it allows the application to obtain an access token for each individual user, regardless of whether they are in the same domain or a different domain. This ensures that the application has the necessary permissions to write a file to each user's Google Drive.

upvoted 1 times

 **jcataluna** 1 year, 4 months ago

**Selected Answer: A**

A is correct

upvoted 2 times

 **brunoguzzo18** 1 year, 8 months ago

**Selected Answer: A**

A is correct for me.

<https://developers.google.com/drive/api/guides/about-auth>: "So, when possible, use "recommended" scopes as they narrow access to specific functionality needed by an app. In most cases, providing narrow access means using the <https://www.googleapis.com/auth/drive.file> per-file access scope" plus each user needs their token to access their own files.

upvoted 2 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: A**

A is correct

upvoted 3 times

 **Blueocean** 2 years, 3 months ago

Option A

upvoted 2 times

 **ParagSanyashiv** 2 years, 3 months ago

**Selected Answer: A**

A is correct because each user should have its own access token rather giving delegated wide domain access.

upvoted 2 times

 **anisov** 2 years, 3 months ago

A is the most suitable answer in my opinion. Auth tokens should be requested per user (So for each user, a token is requested by the application and the user needs to authorise the application).

upvoted 2 times

Question #28

Topic 1

You are creating a Google Kubernetes Engine (GKE) cluster and run this command:

```
> gcloud container clusters create large-cluster --num-nodes 200
```

The command fails with the error:

```
insufficient regional quota to satisfy request: resource "CPUS": request
requires '200.0' and is short '176.0'. project has a quota of '24.0' with
'24.0' available
```

You want to resolve the issue. What should you do?

- A. Request additional GKE quota in the GCP Console.
- B. Request additional Compute Engine quota in the GCP Console.
- C. Open a support case to request additional GKE quota.
- D. Decouple services in the cluster, and rewrite new clusters to function with fewer cores.

**Correct Answer: A**

*Community vote distribution*

B (100%)

 **santoshchauhan** 1 month, 3 weeks ago

**Selected Answer: B**

The issue with the command for creating the Google Kubernetes Engine (GKE) cluster is that it fails due to insufficient regional quota for CPU. GKE clusters utilize Compute Engine resources, so when you encounter a quota issue like this, it is related to the Compute Engine quotas, not directly to GKE.

To resolve the issue, you should: B. Request additional Compute Engine quota in the GCP Console.

Compute Engine quotas are set per region and include resources like CPUs, GPUs, and disk. When you create a GKE cluster, you're actually creating Compute Engine instances that will serve as nodes for the cluster. If your project doesn't have enough quota for the CPUs required to create the cluster, you need to request additional quota for CPUs in the relevant region.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: B**

GKE uses Compute Engine so we need to increase Compute Engine Quota.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Option A is incorrect because the error message mentions Compute Engine quota, not GKE quota. Option C is incorrect because you can request additional quota through the GCP Console, rather than opening a support case. Option D is not a solution to the issue, as it does not address the shortage of Compute Engine quota.

Correct answer B: you should request additional Compute Engine quota in the GCP Console.

upvoted 1 times

 **ExamTopiczz** 1 year, 6 months ago

**Selected Answer: B**

No such thing as a GKE quota

upvoted 1 times

 **hello\_code** 1 year, 6 months ago

**Selected Answer: B**

B is the most appropriate answer

upvoted 1 times

 **brunoguzzo18** 1 year, 8 months ago

**Selected Answer: B**

The GKE node are Compute Engine instances, so if you need more CPUs you need to ask more quota of these.

Answer is B for me.

upvoted 4 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: B**

B is correct

upvoted 3 times

 **ruben82** 1 year, 11 months ago

**Selected Answer: B**

B - According to documentation <https://cloud.google.com/kubernetes-engine/docs/how-to/node-upgrades-quota> (last chapter)

upvoted 3 times

 **herocc** 2 years, 3 months ago

B is best one

upvoted 2 times

 **ParagSanyashiv** 2 years, 3 months ago

**Selected Answer: B**

As the error is referring CPU, the correct answer is B

upvoted 1 times

 **syu31svc** 2 years, 10 months ago

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

"A cluster typically has one or more nodes, which are the worker machines that run your containerized applications and other workloads. The individual machines are Compute Engine VM instances that GKE creates on your behalf when you create a cluster."

Error message mentions "CPU" so this would refer to Compute Engine VMs

Answer is B

upvoted 4 times

 **donchick** 3 years, 4 months ago

B is correct - [https://cloud.google.com/kubernetes-engine/quotas#limits\\_per\\_cluster](https://cloud.google.com/kubernetes-engine/quotas#limits_per_cluster)

upvoted 1 times

 **saurabh1805** 3 years, 5 months ago

Correct answer would be B, as its for number of node,

Question #29

*Topic 1*

You are parsing a log file that contains three columns: a timestamp, an account number (a string), and a transaction amount (a number). You want to calculate the sum of all transaction amounts for each unique account number efficiently.

Which data structure should you use?

- A. A linked list
- B. A hash table
- C. A two-dimensional array
- D. A comma-delimited string

**Correct Answer: B**

*Community vote distribution*

B (89%)

11%

 **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: B**

Hash Table will store unique values.

upvoted 1 times

 **telp** 1 year, 3 months ago

**Selected Answer: B**

B. A hash table for the efficient to find a spzcific number.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

B. A hash table. A hash table allows for fast insertion and lookup of data, which would be useful in this case for quickly looking up the transac amount for a given account number and adding it to the total. A linked list, two-dimensional array, and comma-delimited string would not be as efficient for this purpose.

upvoted 2 times

 **Andrea\_P** 1 year, 6 months ago

**Selected Answer: C**

A and C are obviously wrong.

With hash tables, you cannot store multiple values (amounts) in single key (account number), but this is exactly what you need to do.

Two dimensional array can be used to store all the couples Account-amount (timestamp is useless).

So my selected answer is C.

upvoted 1 times

 **wanrltw** 5 months, 2 weeks ago

The value is not limited to String type, though.

What about storing unique account as a key, while keeping timestamp and transaction amount in an array as its value? ;)

upvoted 1 times

 **wanrltw** 5 months, 2 weeks ago

The details don't really matter here - the account number has to be unique, so hash table is the only way from the provided options.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: B**

B is correct

upvoted 3 times

 **morenocasado** 2 years ago

**Selected Answer: B**

Hash table with the account number as the key, the timestamp is useless for this question, so we can safely discard it.

upvoted 3 times

 **yuchun** 2 years, 10 months ago

in this case, if you use hashtable, the key must be account name+ timestamp, so I think linkedlist is better

upvoted 1 times

 **ruben82** 1 year, 11 months ago

You don't need to use timestamp for this request.

upvoted 1 times

 **ralf\_cc** 2 years, 10 months ago

Hash Table seems right - <https://open4tech.com/array-vs-linked-list-vs-hash-table/>

upvoted 2 times

 **syu31svc** 2 years, 10 months ago

I agree with you on this one

upvoted 2 times

Question #30

Topic 1

Your company has a BigQuery dataset named "Master" that keeps information about employee travel and expenses. This information is organized by employee department. That means employees should only be able to view information for their department. You want to apply a security framework to enforce this requirement with the minimum number of steps.

What should you do?

- A. Create a separate dataset for each department. Create a view with an appropriate WHERE clause to select records from a particular dataset for the specific department. Authorize this view to access records from your Master dataset. Give employees the permission to this department-specific dataset.

- B. Create a separate dataset for each department. Create a data pipeline for each department to copy appropriate information from the Master dataset to the specific dataset for the department. Give employees the permission to this department-specific dataset.
- C. Create a dataset named Master dataset. Create a separate view for each department in the Master dataset. Give employees access to the specific view for their department.
- D. Create a dataset named Master dataset. Create a separate table for each department in the Master dataset. Give employees access to the specific table for their department.

**Correct Answer: B**

*Community vote distribution*

C (85%)

A (15%)

 **cloud\_mk** Highly Voted  3 years, 1 month ago

For me option c is correct.

create view is easy on one dataset with appropriate where clause. And give permission to department.

Create different dataset(option A) for department is create more steps where question denying it.

upvoted 15 times

 **emmet** Highly Voted  3 years, 11 months ago

I think that answer A) is better than B)

Authorized views being in the department-specific dataset will be able to read data from the master dataset(<https://cloud.google.com/bigquery/docs/share-access-views>). And Cloud IAM can set access on dataset level (<https://cloud.google.com/bigquery/docs/dataset-access-controls>)

upvoted 9 times

 **Aeglas** 5 months ago

But correct answer is C. In the link you proposed about access view is clearly stated that you can prevent access to the underlying database and give access only to data that is in the view after applying the query.

upvoted 1 times

 **mennahibi** Most Recent  1 month, 1 week ago

I think that "A" is the best solution, "C" could be too but the dataset Master already exists.

upvoted 1 times

 **santoshchauhan** 1 month, 3 weeks ago

**Selected Answer: C**

C. Create a dataset named Master dataset. Create a separate view for each department in the Master dataset. Give employees access to the specific view for their department.

This option is the most straightforward and requires the fewest steps to implement row-level security in BigQuery. By creating a view for each department with an appropriate WHERE clause that filters records based on the department, you can ensure that employees only see data relevant to them. The views act as a secure interface to the underlying data. You then grant each employee access to the view of their respective department. This method minimizes the number of datasets and tables you have to manage and leverages BigQuery's built-in access control mechanisms.

upvoted 1 times

 **theseawillclaim** 2 months, 2 weeks ago

**Selected Answer: C**

Handling one, big dataset is surely easier than maintaining many smaller ones.

upvoted 1 times

 **darkblade60** 3 months, 2 weeks ago

rly, I don't understand why C says "Create a dataset name Master" wtf, I have the dataset already

upvoted 1 times

 **Aeglas** 5 months ago

**Selected Answer: C**

correct answer is C. In the link you proposed about access view is clearly stated that you can prevent access to the underlying dataset and give access only to data that is in the view after applying the query.

upvoted 1 times

 **Aeglas** 5 months ago

correct answer is C. In the link you proposed about access view is clearly stated that you can prevent access to the underlying dataset and grant access only to data that is in the view after applying the query. (<https://cloud.google.com/bigquery/docs/share-access-views>)  
upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: C**

This approach allows you to maintain a single “master” dataset, while using views to control access to data based on department. This minimizes the number of steps required, as you don’t need to create separate datasets or data pipelines for each department.

upvoted 3 times

 **Chuckq** 1 year ago

Authorized views. So A since is the only one using authorized views. It may be an extra unnecessary step to create a dataset for each department. But it is a way to grant permission to users in this department, and keeps all in order...  
upvoted 1 times

 **telp** 1 year, 3 months ago

**Selected Answer: C**

correct answer c. the view answer the need of access A is eliminated because creating dataset by department is more steps.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

The correct answer is C. By creating a separate view for each department in the Master dataset, you can enforce the requirement that employees should only be able to view information for their department. This is the minimum number of steps required to implement this security framework. Option A is incorrect because it involves creating separate datasets for each department, which is unnecessary. Option B is incorrect because it involves creating data pipelines for each department, which is unnecessary. Option D is incorrect because it involves creating separate tables for each department, which is unnecessary.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: C**

C is correct

upvoted 2 times

 **akshaychavan7** 1 year, 9 months ago

**Selected Answer: C**

It should be C.

Why create a separate dataset when you can get it done simply by creating a view in the same dataset.

upvoted 1 times

 **cloud\_enth0325** 1 year, 10 months ago

**Selected Answer: C**

I vote C. Least steps compared to A.

upvoted 1 times

 **ruben82** 1 year, 11 months ago

Why not C? Less steps. A unique dataset and a view for each department. I think this is smarter and faster as approach.

upvoted 1 times

 **herocc** 2 years, 3 months ago

A is right

upvoted 1 times

You have an application in production. It is deployed on Compute Engine virtual machine instances controlled by a managed instance group. Traffic is routed to the instances via a HTTP(s) load balancer. Your users are unable to access your application. You want to implement a monitoring technique to alert you when the application is unavailable.

Which technique should you choose?

- A. Smoke tests
- B. Stackdriver uptime checks
- C. Cloud Load Balancing - health checks
- D. Managed instance group - health checks

**Correct Answer: B**

Reference:

<https://medium.com/google-cloud/stackdriver-monitoring-automation-part-3-uptime-checks-476b8507f59c>

*Community vote distribution*

B (100%)

 **yuchun** Highly Voted 2 years, 10 months ago  
C,D can both check but not 'alert', so I think the answer is B  
upvoted 5 times

 **\_rajan\_** Most Recent 7 months, 1 week ago  
**Selected Answer: B**  
Stackdriver Uptime Check is the correct option as we can configure it to send an alert when the service is down.  
upvoted 1 times

 **Chuckq** 1 year ago  
Alert. So B.  
upvoted 1 times

## Question #32

Topic 1

You are load testing your server application. During the first 30 seconds, you observe that a previously inactive Cloud Storage bucket is now servicing 2000 write requests per second and 7500 read requests per second. Your application is now receiving intermittent 5xx and 429 HTTP responses from the Cloud Storage

JSON API as the demand escalates. You want to decrease the failed responses from the Cloud Storage API.

What should you do?

- A. Distribute the uploads across a large number of individual storage buckets.
- B. Use the XML API instead of the JSON API for interfacing with Cloud Storage.
- C. Pass the HTTP response codes back to clients that are invoking the uploads from your application.
- D. Limit the upload rate from your application clients so that the dormant bucket's peak request rate is reached more gradually.

### Correct Answer: A

Reference:

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

*Community vote distribution*

D (100%)

 **mlyu** Highly Voted 3 years, 9 months ago

Answer is D  
<https://cloud.google.com/storage/docs/request-rate#ramp-up>  
upvoted 12 times

 **syu31svc** 2 years, 10 months ago

"If you run into any issues such as increased latency or error rates, pause your ramp-up or reduce the request rate temporarily in order to give Cloud Storage more time to scale your bucket. You should use exponential backoff to retry your requests when:

Receiving errors with 5xx and 429 response codes.  
Receiving errors with 408 response codes when performing resumable uploads."  
upvoted 9 times

 **santoshchauhan** Most Recent 1 month, 3 weeks ago

**Selected Answer: D**

D. Limit the upload rate from your application clients so that the dormant bucket's peak request rate is reached more gradually.

Google Cloud Storage buckets have throughput limits that ramp up as sustained traffic increases, especially for previously inactive buckets. When you start sending traffic to an inactive bucket, it takes time for Cloud Storage to automatically scale to accommodate the sudden increase in traffic. By gradually increasing the traffic to the bucket, you give the Cloud Storage infrastructure time to scale and handle the increased load without failing requests.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: D**

Google Cloud Storage buckets have an initial limit on the request rate. If a bucket is inactive for a period of time, it will have a lower limit. As traffic increases, Google Cloud Storage dynamically increases the request rate limit. This process can take several minutes. If the traffic increases too quickly, you may see intermittent 5xx and 429 HTTP responses. By limiting the upload rate from your application clients, you allow the bucket's peak request rate to increase more gradually, reducing the chance of receiving these errors.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

To decrease the failed responses from the Cloud Storage API, you should limit the upload rate from your application clients so that the dormancy bucket's peak request rate is reached more gradually. This will help prevent the bucket from being overwhelmed by a sudden increase in requests.

A, distributing the uploads across a large number of individual storage buckets, may not necessarily decrease the failed responses and could potentially increase the complexity of the system.

B, using the XML API instead of the JSON API, may not necessarily improve performance and could require significant changes to the application.

C, passing the HTTP response codes back to clients, may not address the root cause of the issue and could lead to further errors.

upvoted 1 times

 **jcataluna** 1 year, 4 months ago

**Selected Answer: D**

D is correct

upvoted 2 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: D**

D is correct

upvoted 3 times

 **nhadi82** 1 year, 9 months ago

**Selected Answer: D**

Vote for D

upvoted 1 times

 **ruben82** 1 year, 11 months ago

**Selected Answer: D**

D is the answer according to my understanding

upvoted 1 times

 **herocc** 2 years, 3 months ago

D is right one

upvoted 1 times

 **ParagSanyashiv** 2 years, 3 months ago

**Selected Answer: D**

Answer is D

upvoted 1 times

 **kernel1973** 2 years, 10 months ago

For me the right answer is D.

upvoted 1 times

 **maleksah** 3 years, 3 months ago

Answer is D

upvoted 1 times

 **saurabh1805** 3 years, 5 months ago

D is correct answer

upvoted 1 times

Your application is controlled by a managed instance group. You want to share a large read-only data set between all the instances in the managed instance group. You want to ensure that each instance can start quickly and can access the data set via its filesystem with very low latency. You also want to minimize the total cost of the solution.

What should you do?

- A. Move the data to a Cloud Storage bucket, and mount the bucket on the filesystem using Cloud Storage FUSE.
- B. Move the data to a Cloud Storage bucket, and copy the data to the boot disk of the instance via a startup script.
- C. Move the data to a Compute Engine persistent disk, and attach the disk in read-only mode to multiple Compute Engine virtual machine instances.
- D. Move the data to a Compute Engine persistent disk, take a snapshot, create multiple disks from the snapshot, and attach each disk to its own instance.

**Correct Answer: C**

*Community vote distribution*

C (100%)

 **celia20200410** Highly Voted 2 years, 9 months ago

C:

<https://cloud.google.com/compute/docs/disks/sharing-disks-between-vms#use-multi-instances>

Share a disk in read-only mode between multiple VMs

Sharing static data between multiple VMs from one persistent disk is "less expensive" than replicating your data to unique disks for individual instances.

[https://cloud.google.com/compute/docs/disks/gcs-buckets#mount\\_bucket](https://cloud.google.com/compute/docs/disks/gcs-buckets#mount_bucket)

Mounting a bucket as a file system

You can use the Cloud Storage FUSE tool to mount a Cloud Storage bucket to your Compute Engine instance. The mounted bucket behaves similarly to a persistent disk even though Cloud Storage buckets are object storage.

<https://github.com/GoogleCloudPlatform/gcsfuse/>

Cloud Storage FUSE performance issues: Latency, Rate limit

upvoted 7 times

 **\_\_rajan\_\_** Most Recent 7 months, 1 week ago

**Selected Answer: C**

Option C is Correct.

upvoted 1 times

 **jcataluna** 1 year, 4 months ago

**Selected Answer: C**

A & C are candidates. with very low latency <- C

upvoted 1 times

 **wanrltw** 5 months, 2 weeks ago

C also minimizes the total cost

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: C**

C is correct

upvoted 2 times

 **nhadi82** 1 year, 9 months ago

**Selected Answer: C**

A & C are correct answers, however the question states for low latency hence C is the correct one..

upvoted 1 times

- ✉️ [Removed] 2 years, 9 months ago  
B) is not correct because we want each instance start quickly.  
upvoted 1 times
- ✉️ syu31svc 2 years, 10 months ago  
<https://cloud.google.com/compute/docs/disks/sharing-disks-between-vms>:  
"Maximum attached instances: 2"
- I would take B  
upvoted 1 times
- ✉️ [Removed] 2 years, 9 months ago  
Your link is for write mode not read only !. C) is the answer.  
upvoted 2 times
- ✉️ syu31svc 2 years, 9 months ago  
You're right. C it is then  
upvoted 2 times
- ✉️ yuchun 2 years, 10 months ago  
Both A and C can work, but FUSE will cause more latency  
upvoted 1 times
- ✉️ StelSen 3 years, 2 months ago  
Option: C is correct. <https://cloud.google.com/compute/docs/disks/add-persistent-disk#use-multi-instances>
- Option-A: Technically will work. But not low latency. [https://cloud.google.com/compute/docs/disks/gcs-buckets#mount\\_bucket](https://cloud.google.com/compute/docs/disks/gcs-buckets#mount_bucket)  
upvoted 4 times
- ✉️ saurabh1805 3 years, 5 months ago  
i will suggest option B keeping cost in mind.  
upvoted 1 times
- ✉️ saurabh1805 3 years, 5 months ago  
\* C is correct  
upvoted 4 times

Question #34

Topic 1

You are developing an HTTP API hosted on a Compute Engine virtual machine instance that needs to be invoked by multiple clients within the same Virtual Private Cloud (VPC). You want clients to be able to get the IP address of the service.  
What should you do?

- A. Reserve a static external IP address and assign it to an HTTP(S) load balancing service's forwarding rule. Clients should use this IP address to connect to the service.
- B. Reserve a static external IP address and assign it to an HTTP(S) load balancing service's forwarding rule. Then, define an A record in Cloud DNS. Clients should use the name of the A record to connect to the service.
- C. Ensure that clients use Compute Engine internal DNS by connecting to the instance name with the url [https://\[INSTANCE\\_NAME\].\[ZONE\].compute.internal/](https://[INSTANCE_NAME].[ZONE].compute.internal/).
- D. Ensure that clients use Compute Engine internal DNS by connecting to the instance name with the url [https://\[API\\_NAME\]/\[API\\_VERSION\]/](https://[API_NAME]/[API_VERSION]/).

**Correct Answer: D**

*Community vote distribution*

 **emmet** Highly Voted 3 years, 11 months ago

My vote is answer C)

"Virtual Private Cloud networks on Google Cloud have an internal DNS service that lets instances in the same network access each other by using internal DNS names"

This name can be used for access: [INSTANCE\_NAME].[ZONE].c.[PROJECT\_ID].internal  
[https://cloud.google.com/compute/docs/internal-dns#access\\_by\\_internal\\_DNS](https://cloud.google.com/compute/docs/internal-dns#access_by_internal_DNS)

upvoted 20 times

 **syu31svc** 2 years, 10 months ago

Good find; C is supported by this

upvoted 5 times

 **santoshchauhan** Most Recent 1 month, 3 weeks ago

**Selected Answer: C**

C. Ensure that clients use Compute Engine internal DNS by connecting to the instance name with the URL [https://\[INSTANCE\\_NAME\].\[ZONE\].\[PROJECT\\_ID\].internal/](https://[INSTANCE_NAME].[ZONE].[PROJECT_ID].internal/).

This option allows clients within the same Virtual Private Cloud (VPC) to resolve the Compute Engine instance's internal IP address using internal DNS, which is a feature provided by Compute Engine. The internal DNS name is constructed using the instance name, zone, and project ID, and this DNS entry is automatically created and managed by Google Cloud. This method ensures that traffic between clients and the API does not leave the Google Cloud network, providing lower latency and enhanced security.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: C**

This is a simple and effective way to enable communication between services within the same VPC without the need for external IP addresses or load balancing services.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

D, connecting to the instance name with the url [https://\[API\\_NAME\]/\[API\\_VERSION\]/](https://[API_NAME]/[API_VERSION]/), may not work as it is not specified how clients would know the correct API name and version.

C is the correct answer: By connecting to the instance name with the url [https://\[INSTANCE\\_NAME\].\[ZONE\].c.\[PROJECT\\_ID\].internal/](https://[INSTANCE_NAME].[ZONE].c.[PROJECT_ID].internal/), clients can use Compute Engine's internal DNS to access the API hosted on the virtual machine instance within the same VPC. This will allow clients to access the API with low latency and without the need for a static external IP address.

upvoted 1 times

 **jcataluna** 1 year, 4 months ago

**Selected Answer: C**

C is correct

upvoted 1 times

 **brunoguzzo18** 1 year, 8 months ago

**Selected Answer: C**

<https://cloud.google.com/compute/docs/internal-dns>

The answer is C.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: C**

C is correct

upvoted 3 times

 **nhadi82** 1 year, 9 months ago

**Selected Answer: C**

vote for C

upvoted 1 times

 **herocc** 2 years, 3 months ago

Vote for C

upvoted 1 times

👤 **ParagSanyashiv** 2 years, 3 months ago

**Selected Answer: C**

With no doubt, it is C

upvoted 1 times

👤 **Flavio80** 2 years, 3 months ago

right answer is C

upvoted 1 times

👤 **kernel1973** 2 years, 10 months ago

For me the right answer is C.

upvoted 2 times

👤 **AtulYadav** 3 years, 3 months ago

I vote for C.

upvoted 4 times

👤 **saurabh1805** 3 years, 5 months ago

my vote for C as well.

upvoted 3 times

Question #35

Topic 1

Your application is logging to Stackdriver. You want to get the count of all requests on all /api/alpha/\* endpoints.

What should you do?

- A. Add a Stackdriver counter metric for path:/api/alpha/.
- B. Add a Stackdriver counter metric for endpoint:/api/alpha/\*.
- C. Export the logs to Cloud Storage and count lines matching /api/alpha.
- D. Export the logs to Cloud Pub/Sub and count lines matching /api/alpha.

**Correct Answer: C**

*Community vote distribution*

B (70%)

C (20%)

10%

👤 **worheck93** Highly Voted 2 years, 7 months ago

Ans: B

B have the correct endpoint /api/alpha/\*,

A only get one endpoint counter

upvoted 17 times

👤 **siwang** 1 year, 3 months ago

Agree. counter metric with applying regression filter to httpRequest.requestUrl should be able to get the count value. refer to:  
<https://cloud.google.com/logging/docs/log4j2-vulnerability#log4j-search>

upvoted 1 times

✉  **fraloca** 1 year, 3 months ago

B is the correct answer

"Create a filter that collects only the log entries that you want to count in your metric using the logging query language. You can also use regular expressions to create your metric's filters."

<https://cloud.google.com/logging/docs/logs-based-metrics/counter-metrics#console>

upvoted 2 times

✉  **google\_learner123** Highly Voted 3 years, 7 months ago

Answer should be A

upvoted 9 times

✉  **fraloca** 3 years, 4 months ago

<https://cloud.google.com/logging/docs/logs-based-metrics/counter-metrics#console>

upvoted 3 times

✉  **hug\_c0sm0s** 3 years, 1 month ago

a bit confused about A / B, it seems they mean the same thing.

upvoted 3 times

✉  **santoshchauhan** Most Recent 1 month, 3 weeks ago

Selected Answer: A

A. Add a Stackdriver counter metric for path:/api/alpha/.

In Google Cloud's operations suite (formerly Stackdriver), you can create custom metrics to count specific events within your logs. You would set up a counter metric to capture and count log entries where the request path matches your specified pattern, such as /api/alpha/\*. This would allow you to query and visualize the count of requests to these endpoints directly within Stackdriver Monitoring without the need to export the logs elsewhere.

B. This option seems to be suggesting the correct action (creating a counter metric), but the syntax endpoint:/api/alpha/\* is not correct for Stackdriver Monitoring. Custom metrics in Stackdriver are based on log data and the filter that matches the log entries, so you would specify the filter as part of creating the metric.

upvoted 1 times

✉  **theseawillclaim** 2 months, 2 weeks ago

Selected Answer: B

If you don't export the metric, then you have nothing to count.

I choose B because "endpoint" is more specific than "path".

upvoted 1 times

✉  **\_rajan\_** 7 months, 1 week ago

Selected Answer: B

Ans: B

upvoted 1 times

✉  **maxdanny** 8 months, 1 week ago

Selected Answer: B

This option will accurately track the number of requests made to all endpoints nested under /api/alpha/\*.

upvoted 1 times

✉  **kennyloo** 8 months, 2 weeks ago

B is for counter

upvoted 1 times

✉  **Pime13** 1 year, 2 months ago

Selected Answer: B

submiting just to confirm community response.

upvoted 1 times

✉  **Foxal** 1 year, 2 months ago

Selected Answer: B

B is the only one

upvoted 1 times

✉  **ash\_meharun** 1 year, 3 months ago

**Selected Answer: B**

B is the correct answer

upvoted 1 times

✉  **telp** 1 year, 3 months ago

**Selected Answer: B**

answer is B with the correct endpoint and the goal of counter metris is to resolve the need to count calls

upvoted 1 times

✉  **omermahgoub** 1 year, 3 months ago

Option B is the correct choice because it involves creating a counter metric in Stackdriver specifically for requests to the /api/alpha/\* endpoint. This will allow you to track the number of requests to these endpoints and view the data in Stackdriver.

upvoted 3 times

✉  **omermahgoub** 1 year, 3 months ago

Option C is incorrect because it involves exporting the logs to Cloud Storage and manually counting the lines that match /api/alpha. This is more time-consuming and error-prone approach compared to using a counter metric in Stackdriver.

upvoted 1 times

✉  **omermahgoub** 1 year, 3 months ago

Option A is incorrect because the path:/api/alpha/ metric will track requests to any path that starts with /api/alpha/, not just requests to /api/alpha/\* endpoints.

upvoted 1 times

✉  **omermahgoub** 1 year, 3 months ago

Option D is also incorrect for similar reasons. Exporting the logs to Cloud Pub/Sub and counting the lines that match /api/alpha is more time-consuming and error-prone compared to using a counter metric in Stackdriver.

upvoted 1 times

✉  **tomato123** 1 year, 8 months ago

**Selected Answer: C**

C is correct

upvoted 2 times

✉  **GoReplyGCPExam** 2 years ago

Ans should be B -> (<https://cloud.google.com/blog/products/management-tools/cloud-logging-gets-regular-expression-support>)  
path=~"/api/alpha/\*"

upvoted 5 times

✉  **celia20200410** 2 years, 9 months ago

ans: a

[https://cloud.google.com/logging/docs/view/basic-queries#searching\\_specific\\_fields](https://cloud.google.com/logging/docs/view/basic-queries#searching_specific_fields)

<https://cloud.google.com/monitoring/charts/metrics-selector#filter-option>

To match any US zone that ends with "a", you could use the regular expression ^us.\*.a\$.

upvoted 3 times

✉  **ruben82** 1 year, 11 months ago

documentation says: "ends with a". This question is different.

upvoted 1 times

✉  **syu31svc** 2 years, 9 months ago

<https://cloud.google.com/logging/docs/logs-based-metrics/troubleshooting#metric-name-restrictions>

I would take C

upvoted 1 times

You want to re-architect a monolithic application so that it follows a microservices model. You want to accomplish this efficiently while minimizing the impact of this change to the business.

Which approach should you take?

- A. Deploy the application to Compute Engine and turn on autoscaling.
- B. Replace the application's features with appropriate microservices in phases.
- C. Refactor the monolithic application with appropriate microservices in a single effort and deploy it.
- D. Build a new application with the appropriate microservices separate from the monolith and replace it when it is complete.

**Correct Answer: C**

Reference:

<https://cloud.google.com/solutions/migrating-a-monolithic-app-to-microservices-gke>

*Community vote distribution*

B (100%)

  **emmet** Highly Voted 3 years, 11 months ago

The referenced article shows that the correct answer is B)

"The migration is done feature by feature, avoiding a large-scale migration event and its associated risks"

upvoted 15 times

  **santoshchauhan** Most Recent 1 month, 3 weeks ago

**Selected Answer: B**

B. Replace the application's features with appropriate microservices in phases.

When transitioning from a monolithic application to a microservices architecture, it is generally best to do it incrementally, rather than all at once. This allows you to break down the application into smaller, manageable pieces and make sure each piece is functioning correctly before moving on to the next. It minimizes risk, allows for easier troubleshooting, and reduces the impact on the business because you can gradually shift traffic to the new services as they are tested and deployed.

upvoted 1 times

  **santoshchauhan** 1 month, 3 weeks ago

Here's why the other options are less suitable:

A. Deploying the application to Compute Engine with autoscaling does not change the architecture from monolithic to microservices. It may help with some scaling issues but does not achieve the goal of re-architecting the application.

C. Refactoring the entire monolithic application into microservices in a single effort can be very risky. It can introduce complex issues that are hard to troubleshoot, and if something goes wrong, it could impact the entire business.

D. Building a new application separate from the monolith and replacing it once complete is another approach, but it can be less efficient than replacing in phases. It requires a big-bang cutover, which can be risky. Phased approaches allow for gradual cutover and testing in production with real users, which can lead to a more reliable outcome.

upvoted 1 times

 **sankboy** 2 months, 2 weeks ago

**Selected Answer: B**

Option B is most logical in this situation.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: B**

Option B is most logical in this situation.

upvoted 1 times

 **maxdanny** 8 months, 1 week ago

**Selected Answer: B**

<https://cloud.google.com/architecture/microservices-architecture-refactoring-monoliths>

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Option B is the best choice because it allows you to gradually replace the features of the monolithic application with microservices, minimizing the impact on the business. This approach also allows you to test and validate each microservice before fully integrating it into the application.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Option D is not a good choice because building a new application from scratch and replacing the monolith is likely to be a time-consuming and costly process that could disrupt the business. It is generally more efficient to gradually refactor an existing application into a microservices model rather than starting from scratch.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Option C is not a good choice because refactoring the entire application into a microservices model in a single effort is likely to be a complex and risky process that could disrupt the business.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Option A is not a good choice because it does not address the need to refactor the application into a microservices model. Autoscaling might help with resource management, but it does not address the underlying architecture of the application.

upvoted 1 times

 **[Removed]** 1 year, 7 months ago

Def B, how small is this monolith that it can be converted in 1 day! In addition to the fact that undoubtedly the app will break with this approach.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: B**

B is correct

upvoted 3 times

 **cloud\_enth0325** 1 year, 10 months ago

**Selected Answer: B**

I vote B. Migrating a monolithic service is best when done feature by feature.

upvoted 3 times

 **X627** 1 year, 10 months ago

**Selected Answer: B**

B is the correct. You don't want to replace the monolithic application in one go as C suggests which kind of defeats the purpose.

upvoted 2 times

 **TesterMctester** 2 years, 2 months ago

B strangler pattern

upvoted 4 times

 **herocc** 2 years, 3 months ago

B is right one, refactor with multiple phases to minimize impact.

upvoted 1 times

 **syu31svc** 2 years, 10 months ago

Best answer is B here

A is completely wrong

C and D can be done but the amount of risk involved can be too great

upvoted 2 times

 **navidlaji** 3 years, 2 months ago

it should be B

upvoted 1 times

 **saurabh1805** 3 years, 5 months ago

B is correct answer here.

upvoted 1 times

Question #37

*Topic 1*

Your existing application keeps user state information in a single MySQL database. This state information is very user-specific and depends heavily on how long a user has been using an application. The MySQL database is causing challenges to maintain and enhance the schema for various users.

Which storage option should you choose?

- A. Cloud SQL
- B. Cloud Storage
- C. Cloud Spanner
- D. Cloud Datastore/Firebase

**Correct Answer: A**

Reference:

<https://cloud.google.com/solutions/migrating-mysql-to-cloudsql-concept>

*Community vote distribution*

D (100%)

 **emmet** Highly Voted 3 years, 11 months ago

Question says that there are challenges to maintain and enhance schema, so schemaless DB is more preferable, moreover Google mentions that Datastore/Firebase is good for user profiles ([https://cloud.google.com/datastore/docs/concepts/overview#what\\_its\\_good\\_for](https://cloud.google.com/datastore/docs/concepts/overview#what_its_good_for))

Answer: D)

upvoted 19 times

 **syu31svc** 2 years, 10 months ago

"Datastore is ideal for applications that rely on highly available structured data at scale. You can use Datastore to store and query all of the following types of data:

Product catalogs that provide real-time inventory and product details for a retailer.

User profiles that deliver a customized experience based on the user's past activities and preferences.

Transactions based on ACID properties, for example, transferring funds from one bank account to another."

upvoted 1 times

 **santoshchauhan** [Most Recent](#) 1 month, 3 weeks ago

**Selected Answer: D**

D. Cloud Datastore/Firebase

For user-specific state information that varies significantly and requires a schema that can evolve over time, a NoSQL database like Cloud Datastore or Firestore is typically more appropriate. These databases provide a flexible schema, which allows you to easily make changes as the application evolves and user requirements become more complex.

upvoted 1 times

 **theseawillclaim** 2 months, 2 weeks ago

**Selected Answer: D**

The last sentence subtly implies a schema-enforced database is not the right solution for this use case.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: D**

Since we need a flexible schema we can use Datastore/Firebase

upvoted 1 times

 **zevexWM** 1 year, 3 months ago

**Selected Answer: D**

The question is a bit misleading. If it's asking to keep a MySQL storage option then Cloud SQL or Spanner are the only options. However, assuming that they want to move away from schema and also the need for stateful DB I would go for Datastore/Firebase.

upvoted 3 times

 **omermahgoub** 1 year, 3 months ago

Out of the options provided, Cloud Datastore or Cloud Firestore would be the best choice for storing user state information that is very user-specific and depends heavily on how long a user has been using an application. This is because both Cloud Datastore and Cloud Firestore are NoSQL document databases designed for storing, retrieving, and managing semi-structured data at scale. They are well-suited for storing complex, hierarchical data structures and can handle a high volume of read and write operations. Additionally, Cloud Datastore and Cloud Firestore offer strong consistency and automatic scaling, which can help your application handle a high volume of users without requiring significant manual effort to maintain and enhance the schema.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Cloud Storage is not suitable for storing user state information as it is an object storage service that is not designed for storing structured data.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Cloud Spanner is a highly scalable, distributed database system, but it may not be the most efficient solution for storing user state information that depends heavily on how long a user has been using the application.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Cloud SQL (MySQL) is the current storage option that is causing challenges to maintain and enhance the schema, so it is not a suitable solution.

upvoted 1 times

 **subesingh** 1 year, 7 months ago

Option D

upvoted 1 times

✉  **brunoguzzo18** 1 year, 8 months ago

**Selected Answer: D**

[https://cloud.google.com/datastore/docs/concepts/overview#what\\_its\\_good\\_for](https://cloud.google.com/datastore/docs/concepts/overview#what_its_good_for) -> "User profiles that deliver a customized experience based on the user's past activities and preferences".

Answer id D.

upvoted 2 times

✉  **tomato123** 1 year, 8 months ago

**Selected Answer: D**

D is correct

upvoted 3 times

✉  **crassio12** 2 years ago

D for sure

upvoted 1 times

✉  **herocc** 2 years, 3 months ago

D is right one.

upvoted 3 times

✉  **ParagSanyashiv** 2 years, 3 months ago

**Selected Answer: D**

D is the answer

upvoted 3 times

✉  **saurabh1805** 3 years, 5 months ago

D is correct answer

upvoted 2 times

Question #38

Topic 1

You are building a new API. You want to minimize the cost of storing and reduce the latency of serving images.

Which architecture should you use?

- A. App Engine backed by Cloud Storage
- B. Compute Engine backed by Persistent Disk
- C. Transfer Appliance backed by Cloud Filestore
- D. Cloud Content Delivery Network (CDN) backed by Cloud Storage

**Correct Answer: B**

*Community vote distribution*

D (78%)

11%

11%

✉  **emmet** Highly Voted 3 years, 11 months ago

Answer D) seems more suitable as Cloud Storage has low cost and CDN provides low serving latency

upvoted 17 times

✉  **saurabh1805** 3 years, 5 months ago

Agree this is best answer

upvoted 1 times

✉  **Flavio80** 2 years, 3 months ago

But shouldn't there be something (like Compute Engine / App Engine) between the CDN and Cloud Store?

Thanks ?

upvoted 5 times

 **santoshchauhan** Most Recent 1 month, 3 weeks ago

**Selected Answer: D**

D. Cloud Content Delivery Network (CDN) backed by Cloud Storage

Using Cloud CDN backed by Cloud Storage is a cost-effective and performance-optimized solution for storing and serving images. Cloud Storage provides a durable and highly available object storage solution, while Cloud CDN leverages Google's globally distributed edge points of presence to cache and serve content closer to users, reducing latency.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: D**

D is the best option here as CDN will reduce latency.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

D. Cloud Content Delivery Network (CDN) backed by Cloud Storage.

A Cloud CDN is a content delivery network that uses Google's globally distributed edge points of presence to accelerate content delivery for websites and applications served out of Google Cloud. Cloud CDN stores and serves content from Google Cloud Storage, which allows for efficient and low-cost storage of images, as well as low latency in serving the images. The other options do not mention low latency or cost-effective storage as their primary benefits.

upvoted 2 times

 **omermahgoub** 1 year, 3 months ago

A (App Engine backed by Cloud Storage) may not be suitable because App Engine may not be optimized for serving images, and it may not offer the lowest cost or latency for serving images. Option B (Compute Engine backed by Persistent Disk) may not be suitable because it may not offer the lowest cost for storing images, and it may not offer the lowest latency for serving images.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

C (Transfer Appliance backed by Cloud Filestore) may not be suitable because it is not designed for serving images, but rather for transferring large amounts of data.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

D (Cloud Content Delivery Network (CDN) backed by Cloud Storage) is the most suitable option because CDN is optimized for serving images and other static content, and it can reduce the latency of serving images by storing copies of the images closer to the users who are requesting them. In addition, using Cloud Storage to store the images can help minimize the cost of storing the images.

upvoted 2 times

 **tuanbo91** 1 year, 4 months ago

**Selected Answer: A**

A is correct, the rest how can you write an API?

upvoted 1 times

 **plaffoniera** 1 year, 5 months ago

I think A because CDN doesn't relate to API but to static resources

upvoted 1 times

 **[Removed]** 1 year, 7 months ago

"Cloud CDN content can be sourced from various types of backends:

...

Buckets in Cloud Storage

Answer is D

upvoted 1 times

 **subesingh** 1 year, 7 months ago

Answer is D

upvoted 1 times

 **DiogoVaz** 1 year, 7 months ago

**Selected Answer: B**

CDN is appropriate to serve static files. The right answer is B)

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: D**

D is correct

upvoted 3 times

 **brewpike** 1 year, 11 months ago

D - Cloud CDN

upvoted 2 times

 **mariorossi** 1 year, 11 months ago

For me A. With CDN i can't write API

upvoted 4 times

 **ParagSanyashiv** 2 years, 3 months ago

**Selected Answer: D**

D is more suitable answer in this case.

upvoted 2 times

 **syu31svc** 2 years, 10 months ago

Answer is D since CDN reduces latency and Cloud Storage is used for images

upvoted 3 times

 **Flavio80** 2 years, 3 months ago

But shouldn't there be something (like Compute Engine / App Engine) between the CDN and Cloud Store?

Thanks

upvoted 5 times

 **[Removed]** 1 year, 7 months ago

not neeeded see the docsthey say:

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

That the CDN can be backed by cloud storage buckets

upvoted 1 times

Question #39

Topic 1

Your company's development teams want to use Cloud Build in their projects to build and push Docker images to Container Registry. The operations team requires all Docker images to be published to a centralized, securely managed Docker registry that the operations team manages. What should you do?

- A. Use Container Registry to create a registry in each development team's project. Configure the Cloud Build build to push the Docker image to the project's registry. Grant the operations team access to each development team's registry.
- B. Create a separate project for the operations team that has Container Registry configured. Assign appropriate permissions to the Cloud Build service account in each developer team's project to allow access to the operation team's registry.
- C. Create a separate project for the operations team that has Container Registry configured. Create a Service Account for each development team and assign the appropriate permissions to allow it access to the operations team's registry. Store the service account key file in the source code repository and use it to authenticate against the operations team's registry.
- D. Create a separate project for the operations team that has the open source Docker Registry deployed on a Compute Engine virtual machine instance. Create a username and password for each development team. Store the username and password in the source code repository and use it to authenticate against the operations team's Docker registry.

**Correct Answer: A**

Reference:

<https://cloud.google.com/container-registry/>*Community vote distribution*

B (100%)

**emmet** Highly Voted 3 years, 10 months ago

I think the correct answer is B)

Container Registry is a good choice to store containers in a secure manageable way. It is possible to have Container Registry in one project and push to it from Cloud Build of another project by adding appropriate service account as a member of a Cloud Storage Bucket used to host containers with the role Cloud Build Service Account.

upvoted 15 times

**saurabh1805** 3 years, 5 months ago

Yes, B is best choice here.

upvoted 4 times

**santoshchauhan** Most Recent 1 month, 3 weeks ago**Selected Answer: B**

B. Create a separate project for the operations team that has Container Registry configured. Assign appropriate permissions to the Cloud Build service account in each developer team's project to allow access to the operation team's registry.

This approach aligns with best practices for managing access and centralizing the storage of Docker images while maintaining a high level of security and control

upvoted 1 times

**\_rajan\_** 7 months, 1 week ago**Selected Answer: B**

I would go with B.

upvoted 1 times

**maxdanny** 8 months, 1 week ago**Selected Answer: B**

The option B is the best solution because it provides a centralized, securely managed Docker registry for all development teams to use, and the Cloud Build service account can be granted the necessary permissions to push Docker images to the registry.

upvoted 1 times

**sbonessi** 11 months, 2 weeks ago**Selected Answer: B**

I think B is the correct one as well

upvoted 1 times

**omermahgoub** 1 year, 3 months ago

B is the best choice because it allows the operations team to have control over the centralized, securely managed Docker registry while also allowing the development teams to use Cloud Build in their projects. In this option, the operations team can create a separate project with Container Registry configured and grant appropriate permissions to the Cloud Build service account in each developer team's project to allow access to the operations team's registry. This allows the development teams to build and push Docker images to the centralized registry while still following the operations team's requirements.

upvoted 1 times

**omermahgoub** 1 year, 3 months ago

D is not the best choice because it requires using an open source Docker Registry and creating a username and password for each development team, which may not be secure or efficient.

upvoted 1 times

**omermahgoub** 1 year, 3 months ago

C is not the best choice because it requires storing the service account key file in the source code repository, which may not be secure.

upvoted 1 times

**omermahgoub** 1 year, 3 months ago

A is not ideal because it requires granting the operations team access to each development team's registry, which may not be secure.

upvoted 1 times

 **jcataluna** 1 year, 4 months ago

**Selected Answer: B**

B is correct. No point deploying 1 CR per project.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: B**

B is correct

upvoted 2 times

 **ParagSanyashiv** 2 years, 3 months ago

**Selected Answer: B**

B is the suitable answer in this case

upvoted 2 times

 **kernel1973** 2 years, 10 months ago

B is the best way to store and share images between different projects.

Furthermore use of SA is a choice that match with GCP recommendations

upvoted 1 times

 **syu31svc** 2 years, 10 months ago

"centralized, securely managed Docker registry"

B is the answer

upvoted 1 times

 **navidlaji** 3 years, 2 months ago

My answer is C , using service account to give permissions and storing it in a secured variable is a proper way

upvoted 3 times

 **StelSen** 3 years, 2 months ago

Storing SA key file in repo is not recommended. Everyone can access it. Instead we can use this.

<https://stackoverflow.com/questions/48602546/google-cloud-functions-how-to-securely-store-service-account-private-key-when>

upvoted 1 times

Question #40

Topic 1

You are planning to deploy your application in a Google Kubernetes Engine (GKE) cluster. Your application can scale horizontally, and each instance of your application needs to have a stable network identity and its own persistent disk.

Which GKE object should you use?

- A. Deployment
- B. StatefulSet
- C. ReplicaSet
- D. ReplicaController

**Correct Answer: B**

Reference:

<https://livebook.manning.com/book/kubernetes-in-action/chapter-10/46>

*Community vote distribution*

 **jonclem** Highly Voted  3 years ago

B is the best option here. You can refer to : <https://cloud.google.com/kubernetes-engine/docs/concepts/statefulset>  
upvoted 11 times

 **syu31svc** 2 years, 9 months ago

"The state information and other resilient data for any given StatefulSet Pod is maintained in persistent disk storage associated with the StatefulSet."

upvoted 3 times

 **\_rajan\_** Most Recent  7 months, 1 week ago

**Selected Answer: B**

A StatefulSet is the Kubernetes object best suited for workloads where each pod needs a stable network identity and its own persistent disk.  
upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

The correct answer is B. StatefulSet.

StatefulSets are used to manage the deployment and scaling of stateful applications. They provide a stable network identity and persistent storage for each instance of the application. They are designed to work with applications that require a stable network identity and persistent storage, such as databases, message brokers, and other stateful applications. In contrast, Deployments are used to manage the deployment scaling of stateless applications, which do not require a stable network identity or persistent storage. ReplicaSets and ReplicaControllers are similar to Deployments, but are older and less commonly used in GKE.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: B**

B is correct

upvoted 3 times

 **nehaxlpb** 1 year, 9 months ago

**Selected Answer: B**

Once created, the StatefulSet ensures that the desired number of Pods are running and available at all times. The StatefulSet automatically replaces Pods that fail or are evicted from their nodes, and automatically associates new Pods with the storage resources, resource requests limits, and other configurations defined in the StatefulSet's Pod specification

upvoted 2 times

 **AKr** 3 years, 2 months ago

B is ok

upvoted 2 times

 **Fellipo** 3 years, 5 months ago

B its OK

upvoted 2 times

 **whigy** 3 years, 5 months ago

C doesn't provide a stable network identity and its own persistent disk

upvoted 2 times

 **saurabh1805** 3 years, 5 months ago

you are right

upvoted 1 times

 **saurabh1805** 3 years, 5 months ago

For me C is correct answer

upvoted 1 times

you want the build history to clearly display the stage at which the build failed.

What should you do?

- A. Add RUN commands in the Dockerfile to execute unit and integration tests.
- B. Create a Cloud Build build config file with a single build step to compile unit and integration tests.
- C. Create a Cloud Build build config file that will spawn a separate cloud build pipeline for unit and integration tests.
- D. Create a Cloud Build build config file with separate cloud builder steps to compile and execute unit and integration tests.

**Correct Answer: D**

*Community vote distribution*

D (100%)

 **saurabh1805** Highly Voted 3 years, 5 months ago

D is correct answer here  
upvoted 10 times

 **\_rajan\_** Most Recent 7 months, 1 week ago

**Selected Answer: D**  
I would go with D.  
upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

D - Create a Cloud Build build config file with separate cloud builder steps to compile and execute unit and integration tests. This is the best option because it allows you to clearly specify and separate the different stages of the build process (compiling unit tests, executing unit tests, compiling integration tests, executing integration tests). This makes it easier to understand the build history and identify any failures that may occur. In addition, using separate build steps allows you to specify different properties (such as timeout values or environment variables) for each stage of the build process.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: D**  
D is correct  
upvoted 3 times

 **kinoko1330** 1 year, 8 months ago

**Selected Answer: D**  
Vote D  
upvoted 1 times

 **syu31svc** 2 years, 10 months ago

<https://cloud.google.com/build/docs/build-config-file-schema>:  
"A build step specifies an action that you want Cloud Build to perform. For each build step, Cloud Build executes a docker container as an instance of docker run. Build steps are analogous to commands in a script and provide you with the flexibility of executing arbitrary instructions in your build."

D makes the most sense here  
upvoted 1 times

Your code is running on Cloud Functions in project A. It is supposed to write an object in a Cloud Storage bucket owned by project B. However, the write call is failing with the error "403 Forbidden".

What should you do to correct the problem?

- A. Grant your user account the roles/storage.objectCreator role for the Cloud Storage bucket.
- B. Grant your user account the roles/iam.serviceAccountUser role for the service-PROJECTA@gcf-admin-robot.iam.gserviceaccount.com service account.
- C. Grant the service-PROJECTA@gcf-admin-robot.iam.gserviceaccount.com service account the roles/storage.objectCreator role for the Cloud Storage bucket.
- D. Enable the Cloud Storage API in project B.

**Correct Answer: B***Community vote distribution*

C (100%)

**✉️ 🚫 [Removed] Highly Voted** 3 years, 10 months ago

The answer is C : the default service account used by cloud function is service-PROJECT\_NUMBER@gcf-admin-robot.iam.gserviceaccount.com (cf. [https://cloud.google.com/functions/docs/concepts/iam#troubleshooting\\_permission\\_errors](https://cloud.google.com/functions/docs/concepts/iam#troubleshooting_permission_errors))  
upvoted 17 times

**✉️ 🚫 saurabh1805** 3 years, 5 months ago

Yes correct answer.  
upvoted 2 times

**✉️ 🚫 santoshchauhan** Most Recent 1 month, 3 weeks ago**Selected Answer: C**

C. Grant the service-PROJECTA@gcf-admin-robot.iam.gserviceaccount.com service account the roles/storage.objectCreator role for the Cloud Storage bucket.

The error "403 Forbidden" typically indicates a permissions issue. When a Google Cloud Function tries to access a resource in another project (in this case, a Cloud Storage bucket in project B), it does so using its associated service account. By default, this service account is service-PROJECT\_ID@gcf-admin-robot.iam.gserviceaccount.com where PROJECT\_ID is the ID of the project where the Cloud Function is running (project A).

upvoted 1 times

**✉️ 🚫 \_\_rajan\_\_** 7 months, 1 week ago**Selected Answer: C**

Correct : C

upvoted 1 times

👤 **omermahgoub** 1 year, 3 months ago

C. Grant the service-PROJECTA@gcf-admin-robot.iam.gserviceaccount.com service account the roles/storage.objectCreator role for the Cloud Storage bucket.

In order for the Cloud Functions code running in project A to write to a Cloud Storage bucket in project B, the service account that is used to execute the code needs to be granted the appropriate permissions. In this case, you should grant the service-PROJECTA@gcf-admin-robot.iam.gserviceaccount.com service account the roles/storage.objectCreator role for the Cloud Storage bucket in project B. This will allow code to write objects to the bucket. Option A would not work because it is the service account, not your user account, that needs to be granted permissions.

upvoted 1 times

👤 **omermahgoub** 1 year, 3 months ago

Option B would not work because the roles/iam.serviceAccountUser role does not grant any permissions to access Cloud Storage. Option C would not solve the problem, as the Cloud Storage API is already enabled in both projects by default.

upvoted 1 times

👤 **tomato123** 1 year, 8 months ago

**Selected Answer: C**

C is correct

upvoted 3 times

👤 **ParagSanyashiv** 2 years, 3 months ago

**Selected Answer: C**

Answer is C

upvoted 2 times

👤 **trungtran** 2 years, 6 months ago

Appeared exam 26/10

upvoted 2 times

👤 **KevT94** 2 years, 5 months ago

How about the other question ? Does it appear also ?

upvoted 2 times

👤 **syu31svc** 2 years, 10 months ago

<https://cloud.google.com/functions/docs/troubleshooting>:

"The Cloud Functions service uses the Cloud Functions Service Agent service account (service-<PROJECT\_NUMBER>@gcf-admin-robot.iam.gserviceaccount.com) when performing administrative actions on your project. By default this account is assigned the Cloud Functions serviceAgent role. This role is required for Cloud Pub/Sub, IAM, Cloud Storage and Firebase integrations. If you have changed the role for this service account, deployment fails."

Answer is C

upvoted 3 times

👤 **kernel1973** 2 years, 10 months ago

Answer is C.

service-PROJECTA@gcf-admin-robot.iam.gserviceaccount.com is a google-managed SA.

upvoted 1 times

👤 **kubosuke** 2 years, 12 months ago

defenitely C

upvoted 1 times

👤 **emmet** 3 years, 10 months ago

Seems there is no correct answer here... The correct answer should be grant add service account used by cloud function as a member to target bucket with roles/storage.objectCreator role

upvoted 3 times

👤 **samuelmorher** 9 months ago

The correct answer is the C but like you say, is not the best. To leave the default account is a bad procedure. The best answer must be "Create a new service account and assign it to the cloud build, and grant the object creator permission to that account".

upvoted 1 times

**Case study -**

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

**To start the case study -**

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

**Company Overview -**

HipLocal is a community application designed to facilitate communication between people in close proximity. It is used for event planning and organizing sporting events, and for businesses to connect with their local communities. HipLocal launched recently in a few neighborhoods in Dallas and is rapidly growing into a global phenomenon. Its unique style of hyper-local community communication and business outreach is in demand around the world.

**Executive Statement -**

We are the number one local community app; it's time to take our local community services global. Our venture capital investors want to see rapid growth and the same great experience for new local and virtual communities that come online, whether their members are 10 or 10000 miles away from each other.

**Solution Concept -**

HipLocal wants to expand their existing service, with updated functionality, in new regions to better serve their global customers. They want to hire and train a new team to support these regions in their time zones. They will need to ensure that the application scales smoothly and provides clear uptime data.

**Existing Technical Environment -**

HipLocal's environment is a mix of on-premises hardware and infrastructure running in Google Cloud Platform. The HipLocal team understands their application well, but has limited experience in global scale applications. Their existing technical environment is as follows:

- \* Existing APIs run on Compute Engine virtual machine instances hosted in GCP.
- \* State is stored in a single instance MySQL database in GCP.
- \* Data is exported to an on-premises Teradata/Vertica data warehouse.
- \* Data analytics is performed in an on-premises Hadoop environment.
- \* The application has no logging.
- \* There are basic indicators of uptime; alerts are frequently fired when the APIs are unresponsive.

**Business Requirements -**

HipLocal's investors want to expand their footprint and support the increase in demand they are seeing. Their requirements are:

- \* Expand availability of the application to new regions.
- \* Increase the number of concurrent users that can be supported.

- \* Ensure a consistent experience for users when they travel to different regions.
- \* Obtain user activity metrics to better understand how to monetize their product.
- \* Ensure compliance with regulations in the new regions (for example, GDPR).
- \* Reduce infrastructure management time and cost.
- \* Adopt the Google-recommended practices for cloud computing.

#### Technical Requirements -

- \* The application and backend must provide usage metrics and monitoring.
- \* APIs require strong authentication and authorization.
- \* Logging must be increased, and data should be stored in a cloud analytics platform.
- \* Move to serverless architecture to facilitate elastic scaling.
- \* Provide authorized access to internal apps in a secure manner.

HipLocal's .net-based auth service fails under intermittent load.

What should they do?

- Use App Engine for autoscaling.
- Use Cloud Functions for autoscaling.
- Use a Compute Engine cluster for the service.
- Use a dedicated Compute Engine virtual machine instance for the service.

**Correct Answer: D**

Reference:

<https://www.qwiklabs.com/focuses/611?parent=catalog>

*Community vote distribution*

A (43%)	C (36%)	B (21%)
---------	---------	---------

✉️  **saurabh1805**  3 years, 5 months ago

A is correct answer here App engine, as app engine flexible support .net  
upvoted 11 times

✉️  **fraloca** 3 years, 4 months ago

A is wrong because appengine is single region: <https://cloud.google.com/appengine/docs/locations>. For me the correct answer is C, comp engine with instance Group.  
upvoted 3 times

✉️  **donchick** 3 years, 3 months ago

One of reqs is "Move to serverless architecture to facilitate elastic scaling". I vote for A.  
upvoted 7 times

✉️  **StelSen** 3 years, 2 months ago

A is correct  
upvoted 3 times

✉️  **santoshchauhan**  1 month, 3 weeks ago

**Selected Answer: B**

B. Use Cloud Functions for autoscaling: Cloud Functions is a serverless execution environment that automatically scales based on the load. It is well-suited for applications with intermittent or unpredictable traffic patterns, such as HipLocal's auth service. The serverless nature of Cloud Functions also reduces infrastructure management overhead, aligning with the business requirement to reduce management time and cost. However, it's important to note that the runtime support for .NET in Cloud Functions is limited, and a migration or use of an alternative supported runtime might be necessary.

upvoted 1 times

 **Aeglas** 5 months ago

**Selected Answer: A**

A, since AppEngine can be deployed in several regions with a Load Balancer in front as demonstrated by Google. This will make the deployment serverless as requested, sticking to .net framework.

upvoted 1 times

 **wanrltw** 5 months, 1 week ago

**Selected Answer: A**

Serverless architecture -> App Engine

upvoted 1 times

 **xiaofeng\_0226** 5 months, 3 weeks ago

Vote for B

upvoted 1 times

 **\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: B**

B is correct.

upvoted 2 times

 **\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: C**

Option C is correct as AppEngine is regional.

upvoted 1 times

 **\_rajan\_\_** 7 months, 1 week ago

I would go with Option B Cloud Function. Since it is a global resource and is scalable on demand.

upvoted 1 times

 **wanrltw** 5 months, 1 week ago

Cloud Functions isn't an optimal solution for an entire app.

upvoted 1 times

 **minagmaxwell** 9 months, 2 weeks ago

**Selected Answer: A**

A is correct. Don't get thrown off by app engine being regional.

Google has demonstrated you can deploy to multiple regions by creating multiple projects and throwing a load balancer in front. Check their demo toward the end:

[https://www.youtube.com/watch?v=JCvzUTmKakQ&ab\\_channel=GoogleCloudTech](https://www.youtube.com/watch?v=JCvzUTmKakQ&ab_channel=GoogleCloudTech)

upvoted 1 times

 **edward\_zhang** 1 year, 2 months ago

I vote A. App Engine cannot run in multi-region. But we can create multiple projects for supporting different region app engine.

upvoted 1 times

 **Foxal** 1 year, 2 months ago

**Selected Answer: C**

C is correct, A option is for regional solutions

upvoted 1 times

 **telp** 1 year, 3 months ago

**Selected Answer: C**

C is correct because app engine is regional only so it not answer the need of global application

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: A**

A is correct

upvoted 1 times

 **kinoko1330** 1 year, 8 months ago

**Selected Answer: A**

A for "serverless architecture to facilitate elastic scaling"

upvoted 1 times

 **nehaxlpb** 1 year, 9 months ago

**Selected Answer: A**

A is correct answer here App engine, as app engine flexible support .net  
upvoted 1 times

 **akshaychavan7** 1 year, 9 months ago

**Selected Answer: C**

Initially, I had picked option A considering the flexible request support. However, it imposes the limitation of a single region which is not expected in the case study. So, the only suitable option here is to use Compute Engine Cluster.  
upvoted 2 times

 **akshaychavan7** 1 year, 8 months ago

Also, note that "Existing APIs run on Compute Engine virtual machine instances hosted in Google Cloud", which is given in the existing technical environment.

Considering this, it is advisable that instead of using a single VM we can create a cluster of such VMs and distribute the load among them.  
upvoted 1 times

 **gfr892** 2 years, 3 months ago

App Engine is regional. C is correct, because is the only multi-regional solution  
upvoted 4 times

 **syu31svc** 2 years, 10 months ago

<https://cloud.google.com/appengine/docs/flexible/dotnet/how-instances-are-managed>:  
"Automatic scaling creates instances based on request rate, response latencies, and other application metrics. You can specify thresholds for each of these metrics, as well as a minimum number instances to keep running at all times."

A is the answer  
upvoted 4 times

Question #44

Topic 1

#### Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

#### To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

#### **Company Overview -**

HipLocal is a community application designed to facilitate communication between people in close proximity. It is used for event planning and organizing sporting events, and for businesses to connect with their local communities. HipLocal launched recently in a few neighborhoods in Dallas and is rapidly growing into a global phenomenon. Its unique style of hyper-local community communication and business outreach is in demand around the world.

#### **Executive Statement -**

We are the number one local community app; it's time to take our local community services global. Our venture capital investors want to see rapid growth and the same great experience for new local and virtual communities that come online, whether their members are 10 or 10000 miles away from each other.

#### **Solution Concept -**

HipLocal wants to expand their existing service, with updated functionality, in new regions to better serve their global customers. They want to hire and train a new team to support these regions in their time zones. They will need to ensure that the application scales smoothly and provides clear uptime data.

#### **Existing Technical Environment -**

HipLocal's environment is a mix of on-premises hardware and infrastructure running in Google Cloud Platform. The HipLocal team understands their application well, but has limited experience in global scale applications. Their existing technical environment is as follows:

- \* Existing APIs run on Compute Engine virtual machine instances hosted in GCP.
- \* State is stored in a single instance MySQL database in GCP.
- \* Data is exported to an on-premises Teradata/Vertica data warehouse.
- \* Data analytics is performed in an on-premises Hadoop environment.
- \* The application has no logging.
- \* There are basic indicators of uptime; alerts are frequently fired when the APIs are unresponsive.

#### **Business Requirements -**

HipLocal's investors want to expand their footprint and support the increase in demand they are seeing. Their requirements are:

- \* Expand availability of the application to new regions.
- \* Increase the number of concurrent users that can be supported.
- \* Ensure a consistent experience for users when they travel to different regions.
- \* Obtain user activity metrics to better understand how to monetize their product.
- \* Ensure compliance with regulations in the new regions (for example, GDPR).
- \* Reduce infrastructure management time and cost.
- \* Adopt the Google-recommended practices for cloud computing.

#### **Technical Requirements -**

- \* The application and backend must provide usage metrics and monitoring.
- \* APIs require strong authentication and authorization.
- \* Logging must be increased, and data should be stored in a cloud analytics platform.
- \* Move to serverless architecture to facilitate elastic scaling.
- \* Provide authorized access to internal apps in a secure manner.

HipLocal's APIs are having occasional application failures. They want to collect application information specifically to troubleshoot the issue.

What should they do?

- A. Take frequent snapshots of the virtual machines.
- B. Install the Cloud Logging agent on the virtual machines.
- C. Install the Cloud Monitoring agent on the virtual machines.
- D. Use Cloud Trace to look for performance bottlenecks.

**Correct Answer: C***Community vote distribution*

B (83%)

D (17%)

  **dishum** Highly Voted  2 years, 1 month ago

B is the correct answer

upvoted 6 times

  **dishum** 1 year, 11 months ago

No.. C is the right answer

upvoted 1 times

  **santoshchauhan** Most Recent  1 month, 3 weeks ago**Selected Answer: B**

B. Install the Cloud Logging agent on the virtual machines.

To troubleshoot occasional application failures, HipLocal needs to collect detailed logs that provide insights into what's happening within their applications. Installing the Cloud Logging agent on the virtual machines is the most direct approach to achieving this. The Cloud Logging agent will collect logs from various applications and system components running on the VMs, which can be invaluable for diagnosing issues.

upvoted 1 times

  **\_rajan\_\_** 7 months, 1 week ago**Selected Answer: B**

I would go with B.

upvoted 1 times

  **Google** 9 months, 1 week ago

C is the correct answer

upvoted 1 times

  **zanhsieh** 10 months, 2 weeks ago**Selected Answer: B**

B.

A: No. This is for VM boot failed or other not related to API. The question didn't mention VM failed, nor the scenario.

B: Yes.

C: No. Monitoring agent is for metrics collection, such as memory. Not related to API.

D: No. If the question stated something like the API works perfectly but slow, then this would be valid.

upvoted 1 times

  **telp** 1 year, 3 months ago**Selected Answer: B**

They don't have logging so need to add logging agent so we can have logs to study. Tracr is for latency issue and it's not the issue here.

upvoted 1 times

  **tomato123** 1 year, 8 months ago**Selected Answer: D**

D is correct

upvoted 1 times

  **akshaychavan7** 1 year, 8 months ago

I might be wrong here, but Cloud Trace is also kind of suitable for this use case, isn't it?

Reference - <https://cloud.google.com/trace>

Fast, automatic issue detection

Trace continuously gathers and analyzes trace data from your project to automatically identify recent changes to your application's performance. These latency distributions, available through the Analysis Reports feature, can be compared over time or versions, and Cloud Trace will automatically alert you if it detects a significant shift in your app's latency profile.

upvoted 1 times

  **akshaychavan7** 1 year, 8 months ago

I will still go for option B here, as Trace is majorly used for finding out performance bottlenecks which is not specified in the problem statement.

upvoted 1 times

 **GCPCloudArchitectUser** 2 years, 2 months ago

**Selected Answer: B**

Yep they don't have any logging so it should be B

upvoted 1 times

 **gfr892** 2 years, 3 months ago

B is correct too.

upvoted 2 times

Question #45

*Topic 1*

#### Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

#### To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

#### Company Overview -

HipLocal is a community application designed to facilitate communication between people in close proximity. It is used for event planning and organizing sporting events, and for businesses to connect with their local communities. HipLocal launched recently in a few neighborhoods in Dallas and is rapidly growing into a global phenomenon. Its unique style of hyper-local community communication and business outreach is in demand around the world.

#### Executive Statement -

We are the number one local community app; it's time to take our local community services global. Our venture capital investors want to see rapid growth and the same great experience for new local and virtual communities that come online, whether their members are 10 or 10000 miles away from each other.

#### Solution Concept -

HipLocal wants to expand their existing service, with updated functionality, in new regions to better serve their global customers. They want to hire and train a new team to support these regions in their time zones. They will need to ensure that the application scales smoothly and provides clear uptime data.

#### Existing Technical Environment -

HipLocal's environment is a mix of on-premises hardware and infrastructure running in Google Cloud Platform. The HipLocal team understands their application well, but has limited experience in global scale applications. Their existing technical environment is as follows:

- \* Existing APIs run on Compute Engine virtual machine instances hosted in GCP.
- \* State is stored in a single instance MySQL database in GCP.
- \* Data is exported to an on-premises Teradata/Vertica data warehouse.
- \* Data analytics is performed in an on-premises Hadoop environment.
- \* The application has no logging.
- \* There are basic indicators of uptime; alerts are frequently fired when the APIs are unresponsive.

**Business Requirements -**

HipLocal's investors want to expand their footprint and support the increase in demand they are seeing. Their requirements are:

- \* Expand availability of the application to new regions.
- \* Increase the number of concurrent users that can be supported.
- \* Ensure a consistent experience for users when they travel to different regions.
- \* Obtain user activity metrics to better understand how to monetize their product.
- \* Ensure compliance with regulations in the new regions (for example, GDPR).
- \* Reduce infrastructure management time and cost.
- \* Adopt the Google-recommended practices for cloud computing.

**Technical Requirements -**

- \* The application and backend must provide usage metrics and monitoring.
- \* APIs require strong authentication and authorization.
- \* Logging must be increased, and data should be stored in a cloud analytics platform.
- \* Move to serverless architecture to facilitate elastic scaling.
- \* Provide authorized access to internal apps in a secure manner.

HipLocal has connected their Hadoop infrastructure to GCP using Cloud Interconnect in order to query data stored on persistent disks.

Which IP strategy should they use?

- A. Create manual subnets.
- B. Create an auto mode subnet.
- C. Create multiple peered VPCs.
- D. Provision a single instance for NAT.

**Correct Answer: A**

*Community vote distribution*

B (50%)

A (50%)

 **santoshchauhan** 1 month, 3 weeks ago

**Selected Answer: B**

B. Create an auto mode subnet.

When integrating Hadoop infrastructure with Google Cloud Platform (GCP) via Cloud Interconnect and querying data stored on persistent disk the IP strategy should simplify network management while ensuring efficient and secure data access. Creating an auto mode subnet in their VPC is a suitable approach for this scenario.

upvoted 1 times

 **Bessa24** 2 months ago

**Selected Answer: B**

B is correct

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: B**

For simplicity and ease of management, an auto mode subnet (option B) could be a good choice.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: A**

A is correct

upvoted 1 times

 **bk7** 1 year, 8 months ago

**Selected Answer: A**

A - Need to take control of the IP assignment thru manual subnet especially when establishing the connectivity between on-prem/cloud

upvoted 4 times

 **akshaychavan7** 1 year, 8 months ago

**Selected Answer: B**

I will go with auto mode subnet creation as it will automatically create a subnet inside each region. Moreover, one of the business requirement states that 'Reduce infrastructure management time and cost.'. Thus, with auto mode subnet we avoid infrastructure management.

upvoted 2 times

 **syu31svc** 2 years, 10 months ago

<https://cloud.google.com/architecture/hadoop/hadoop-gcp-migration-data>

I would take A based on the 2nd figure given in the link

upvoted 1 times

 **saurabh1805** 3 years, 5 months ago

A is correct answer here.

upvoted 1 times

there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

#### To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

#### Company Overview -

HipLocal is a community application designed to facilitate communication between people in close proximity. It is used for event planning and organizing sporting events, and for businesses to connect with their local communities. HipLocal launched recently in a few neighborhoods in Dallas and is rapidly growing into a global phenomenon. Its unique style of hyper-local community communication and business outreach is in demand around the world.

#### Executive Statement -

We are the number one local community app; it's time to take our local community services global. Our venture capital investors want to see rapid growth and the same great experience for new local and virtual communities that come online, whether their members are 10 or 10000 miles away from each other.

#### Solution Concept -

HipLocal wants to expand their existing service, with updated functionality, in new regions to better serve their global customers. They want to hire and train a new team to support these regions in their time zones. They will need to ensure that the application scales smoothly and provides clear uptime data.

#### Existing Technical Environment -

HipLocal's environment is a mix of on-premises hardware and infrastructure running in Google Cloud Platform. The HipLocal team understands their application well, but has limited experience in global scale applications. Their existing technical environment is as follows:

- \* Existing APIs run on Compute Engine virtual machine instances hosted in GCP.
- \* State is stored in a single instance MySQL database in GCP.
- \* Data is exported to an on-premises Teradata/Vertica data warehouse.
- \* Data analytics is performed in an on-premises Hadoop environment.
- \* The application has no logging.
- \* There are basic indicators of uptime; alerts are frequently fired when the APIs are unresponsive.

#### Business Requirements -

HipLocal's investors want to expand their footprint and support the increase in demand they are seeing. Their requirements are:

- \* Expand availability of the application to new regions.
- \* Increase the number of concurrent users that can be supported.
- \* Ensure a consistent experience for users when they travel to different regions.
- \* Obtain user activity metrics to better understand how to monetize their product.
- \* Ensure compliance with regulations in the new regions (for example, GDPR).
- \* Reduce infrastructure management time and cost.
- \* Adopt the Google-recommended practices for cloud computing.

#### Technical Requirements -

- \* The application and backend must provide usage metrics and monitoring.
- \* APIs require strong authentication and authorization.
- \* Logging must be increased, and data should be stored in a cloud analytics platform.
- \* Move to serverless architecture to facilitate elastic scaling.
- \* Provide authorized access to internal apps in a secure manner.

Which service should HipLocal use to enable access to internal apps?

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

**Correct Answer: D**

Reference:

<https://cloud.google.com/iap/docs/cloud-iap-for-on-prem-apps-overview>

*Community vote distribution*

D (100%)

 **MickeyRourke** Highly Voted 3 years, 3 months ago

I think it should be D .  
upvoted 7 times

 **\_rajan\_** Most Recent 7 months, 1 week ago

**Selected Answer: D**

Cloud IAP works by verifying user identity and context of the request to determine if a user should be allowed to access the application. It provides secure application-level access control and does not require a traditional VPN connection.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: D**

D is correct  
upvoted 1 times

 **dishum** 2 years, 1 month ago

D is correct  
upvoted 1 times

 **dishum** 2 years, 1 month ago

I think it is A, not D  
upvoted 1 times

 **syu31svc** 2 years, 10 months ago

<https://cloud.google.com/network-connectivity/docs/vpn/concepts/overview>  
<https://cloud.google.com/armor>

D is the answer for sure  
upvoted 2 times

 **kernel1973** 2 years, 10 months ago

D.  
<https://cloud.google.com/iap/docs/concepts-overview>  
upvoted 1 times

 **saurabh1805** 3 years, 5 months ago

if internal app mens app hosted on-prem then option A seems to be correct one  
upvoted 3 times

**Case study -**

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

**To start the case study -**

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

#### **Company Overview -**

HipLocal is a community application designed to facilitate communication between people in close proximity. It is used for event planning and organizing sporting events, and for businesses to connect with their local communities. HipLocal launched recently in a few neighborhoods in Dallas and is rapidly growing into a global phenomenon. Its unique style of hyper-local community communication and business outreach is in demand around the world.

#### **Executive Statement -**

We are the number one local community app; it's time to take our local community services global. Our venture capital investors want to see rapid growth and the same great experience for new local and virtual communities that come online, whether their members are 10 or 10000 miles away from each other.

#### **Solution Concept -**

HipLocal wants to expand their existing service, with updated functionality, in new regions to better serve their global customers. They want to hire and train a new team to support these regions in their time zones. They will need to ensure that the application scales smoothly and provides clear uptime data.

#### **Existing Technical Environment -**

HipLocal's environment is a mix of on-premises hardware and infrastructure running in Google Cloud Platform. The HipLocal team understands their application well, but has limited experience in global scale applications. Their existing technical environment is as follows:

- \* Existing APIs run on Compute Engine virtual machine instances hosted in GCP.
- \* State is stored in a single instance MySQL database in GCP.
- \* Data is exported to an on-premises Teradata/Vertica data warehouse.
- \* Data analytics is performed in an on-premises Hadoop environment.
- \* The application has no logging.
- \* There are basic indicators of uptime; alerts are frequently fired when the APIs are unresponsive.

#### **Business Requirements -**

HipLocal's investors want to expand their footprint and support the increase in demand they are seeing. Their requirements are:

- \* Expand availability of the application to new regions.
- \* Increase the number of concurrent users that can be supported.
- \* Ensure a consistent experience for users when they travel to different regions.
- \* Obtain user activity metrics to better understand how to monetize their product.
- \* Ensure compliance with regulations in the new regions (for example, GDPR).
- \* Reduce infrastructure management time and cost.
- \* Adopt the Google-recommended practices for cloud computing.

#### **Technical Requirements -**

- \* The application and backend must provide usage metrics and monitoring.
- \* APIs require strong authentication and authorization.
- \* Logging must be increased, and data should be stored in a cloud analytics platform.
- \* Move to serverless architecture to facilitate elastic scaling.
- \* Provide authorized access to internal apps in a secure manner.

HipLocal wants to reduce the number of on-call engineers and eliminate manual scaling.

Which two services should they choose? (Choose two.)

- A. Use Google App Engine services.
- B. Use serverless Google Cloud Functions.
- C. Use Knative to build and deploy serverless applications.
- D. Use Google Kubernetes Engine for automated deployments.
- E. Use a large Google Compute Engine cluster for deployments.

**Correct Answer: BC***Community vote distribution*

CD (69%)

AB (31%)

**saurabh1805** Highly Voted 3 years, 5 months ago

A and B are correct option here.

upvoted 16 times

**santoshchauhan** Most Recent 1 month, 3 weeks ago**Selected Answer: AB**

A. Google App Engine: This is a fully managed serverless platform that automatically scales your application up and down while balancing the load. With App Engine, you don't need to manage the underlying infrastructure, and it scales automatically in response to the traffic it receives. This can significantly reduce the operational overhead and the need for on-call engineers to handle scaling issues.

B. Google Cloud Functions: This is another serverless execution environment that automatically scales the number of instances running your function in response to the incoming event rate. This is ideal for applications that respond to events (e.g., HTTP requests, Cloud Pub/Sub events). Like App Engine, it abstracts away infrastructure management and auto-scales based on demand.

upvoted 1 times

**\_\_rajan\_\_** 7 months, 1 week ago**Selected Answer: AB**

I Think It should be A and B for serverless autoscaling. Since there are extra steps involved in configuring Knative it is not fit for this situation.

upvoted 1 times

**minagmaxwell** 9 months, 2 weeks ago**Selected Answer: AB**

you CAN go global with app engine and cloud functions

upvoted 1 times

**telp** 1 year, 3 months ago**Selected Answer: CD**

C and D because need to be global

upvoted 1 times

**brunoguzzo18** 1 year, 8 months ago**Selected Answer: CD**

App must be global

upvoted 2 times

**tomato123** 1 year, 8 months ago**Selected Answer: CD**

CD are correct

upvoted 1 times

**nehaxlpb** 1 year, 9 months ago**Selected Answer: CD**

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

upvoted 1 times

**nhadi82** 1 year, 9 months ago**Selected Answer: CD**

Vote for C & D

upvoted 1 times

**akshaychavan7** 1 year, 9 months ago**Selected Answer: CD**

App Engine cannot be a solution here as it limits the application to be in a single region. We need to note that the case study has explicitly mentioned that the application needs to be global, which means multi-regional.

So, I will go with C & D.

upvoted 3 times

 **hitmax87** 2 years ago

C+D are correct. Because k8s is global plus on-premises nodes can be connected.

upvoted 1 times

 **dishum** 2 years, 1 month ago

AB is correct

upvoted 2 times

 **gfr892** 2 years, 3 months ago

App Engine and Cloud Functions are regional.

D and E are correct, because they are global and they have autoscaler for deployments.

upvoted 1 times

 **gfr892** 2 years, 3 months ago

Correction: C and D are correct.

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

<https://cloud.google.com/blog/products/serverless/knative-based-cloud-run-services-are-ga>

<https://cloud.google.com/run/docs/multiple-regions>

upvoted 1 times

 **raja77** 2 years, 3 months ago

**Selected Answer: AB**

[https://cloud.google.com/appengine/docs/standard/python/how-instances-are-managed#apps\\_with\\_automatic\\_scaling](https://cloud.google.com/appengine/docs/standard/python/how-instances-are-managed#apps_with_automatic_scaling)

upvoted 1 times

 **syu31svc** 2 years, 10 months ago

[https://cloud.google.com/appengine/docs/standard/python/how-instances-are-managed#apps\\_with\\_automatic\\_scaling](https://cloud.google.com/appengine/docs/standard/python/how-instances-are-managed#apps_with_automatic_scaling)

A and B for sure; "eliminate manual scaling" as per what the qn states

upvoted 2 times

Question #48

Topic 1

#### Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

#### To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

#### Company Overview -

HipLocal is a community application designed to facilitate communication between people in close proximity. It is used for event planning and organizing sporting events, and for businesses to connect with their local communities. HipLocal launched recently in a few neighborhoods in Dallas and is rapidly growing into a global phenomenon. Its unique style of hyper-local community communication and business outreach is in demand around the world.

#### Executive Statement -

We are the number one local community app; it's time to take our local community services global. Our venture capital investors want to see rapid growth and the same great experience for new local and virtual communities that come online, whether their members are 10 or 10000 miles away from each other.

#### Solution Concept -

HipLocal wants to expand their existing service, with updated functionality, in new regions to better serve their global customers. They want to hire and train a new team to support these regions in their time zones. They will need to ensure that the application scales smoothly and provides clear uptime data.

#### Existing Technical Environment -

HipLocal's environment is a mix of on-premises hardware and infrastructure running in Google Cloud Platform. The HipLocal team understands their application well, but has limited experience in global scale applications. Their existing technical environment is as follows:

- \* Existing APIs run on Compute Engine virtual machine instances hosted in GCP.
- \* State is stored in a single instance MySQL database in GCP.
- \* Data is exported to an on-premises Teradata/Vertica data warehouse.
- \* Data analytics is performed in an on-premises Hadoop environment.
- \* The application has no logging.
- \* There are basic indicators of uptime; alerts are frequently fired when the APIs are unresponsive.

#### Business Requirements -

HipLocal's investors want to expand their footprint and support the increase in demand they are seeing. Their requirements are:

- \* Expand availability of the application to new regions.
- \* Increase the number of concurrent users that can be supported.
- \* Ensure a consistent experience for users when they travel to different regions.
- \* Obtain user activity metrics to better understand how to monetize their product.
- \* Ensure compliance with regulations in the new regions (for example, GDPR).
- \* Reduce infrastructure management time and cost.
- \* Adopt the Google-recommended practices for cloud computing.

#### Technical Requirements -

- \* The application and backend must provide usage metrics and monitoring.
- \* APIs require strong authentication and authorization.
- \* Logging must be increased, and data should be stored in a cloud analytics platform.
- \* Move to serverless architecture to facilitate elastic scaling.
- \* Provide authorized access to internal apps in a secure manner.

In order to meet their business requirements, how should HipLocal store their application state?

- A. Use local SSDs to store state.
- B. Put a memcache layer in front of MySQL.
- C. Move the state storage to Cloud Spanner.
- D. Replace the MySQL instance with Cloud SQL.

**Correct Answer: B**

*Community vote distribution*

D (50%)

C (50%)

 **fraloca** Highly Voted 3 years, 4 months ago

For me the answer is C. A is not valid because local SSD is volatile memory. B and D is bad solution because it don't reduce latency in world

wide but they are a regional location.

upvoted 13 times

✉  **mastodilu** 2 years, 11 months ago

exactly, plus the state is already stored in a single instance MySQL database in GCP, so it basically says "do nothing". Spanner is correct ↗  
upvoted 3 times

✉  **gcp0omkar** 2 years, 6 months ago

"State is stored in a single instance MySQL database in GCP." so Cloud SQL is enough! (Option D) so Correct answer is D  
Spanner would be costly (Option C)

upvoted 1 times

✉  **santoshchauhan** Most Recent 1 month, 3 weeks ago

**Selected Answer: C**

C. Move the state storage to Cloud Spanner: Cloud Spanner is a fully managed, horizontally scalable database service with global distribution and strong consistency. It's well-suited for applications that require a high degree of scalability and reliability, making it a good choice for HipLocal as they expand globally.

Given HipLocal's need for scalability and global distribution, Cloud Spanner (option C) is likely the best fit. It provides the scalability and global reach necessary for their expansion, along with the relational database capabilities that their application likely relies on. Cloud SQL (option D) is also a good choice if their current scale and distribution requirements can be met within its limits.

upvoted 1 times

✉  **wanrltw** 5 months, 1 week ago

**Selected Answer: C**

Moving the state storage to Cloud Spanner, is the best solution for HipLocal because Cloud Spanner is a globally distributed, horizontally scalable, and strongly consistent relational database service.

Cloud Spanner provides high availability and can handle automatic scaling, backups, and updates. In addition, it provides support for distributed transactions, and it's designed to provide low latency and high throughput.

Cloud Spanner can also help HipLocal meet their compliance requirements, as it supports HIPAA, GDPR, and other regulatory standards.  
upvoted 2 times

✉  **\_rajan\_** 7 months, 1 week ago

**Selected Answer: C**

Given HipLocal's requirements for global expansion and high availability, moving the state storage to Cloud Spanner (option C) would likely be the most suitable choice.

upvoted 1 times

✉  **closer89** 11 months, 3 weeks ago

**Selected Answer: D**

to meet their business requirements  
spanner is very expensive, we need to reduce costs after all  
cloud sql with multi-regional replication fits our needs  
[https://cloud.google.com/sql/docs/mysqlreplication#replication\\_use\\_cases](https://cloud.google.com/sql/docs/mysqlreplication#replication_use_cases)  
upvoted 2 times

✉  **brunoguzzo18** 1 year, 8 months ago

**Selected Answer: C**

<https://stackoverflow.com/questions/60412688/whats-the-difference-between-google-cloud-spanner-and-cloud-sql#:~:text=The%20main%20difference%20between%20Cloud,of%20writes%20per%20second%2C%20globally.>

C is correct for me.

upvoted 2 times

✉  **brunoguzzo18** 1 year, 8 months ago

But, Spanner is not a formal relational DB so Cloud SQL is the best solution, plus it has the data replication for global purpose.  
upvoted 1 times

✉  **tomato123** 1 year, 8 months ago

**Selected Answer: D**

D is correct

upvoted 1 times

 **nhadi82** 1 year, 9 months ago

**Selected Answer: D**

vote for D as also cloud SQL could be built for multi-region replica  
<https://cloud.google.com/blog/products/databases/introducing-cross-region-replica-for-cloud-sql>  
upvoted 2 times

 **closer89** 11 months, 3 weeks ago

replica is OK to read data.  
but you have to write to master node which could be in a different continent  
<https://cloud.google.com/sql/docs/mysql/replication#read-replicas>  
<https://cloud.google.com/sql/docs/mysql/replication#cross-region-read-replicas>  
upvoted 1 times

 **akshaychavan7** 1 year, 9 months ago

**Selected Answer: C**

Let's go with Cloud Spanner as it is the only supported global solution.  
upvoted 1 times

 **brewpike** 1 year, 11 months ago

C- Spanner, business requirements are to expand globally.  
upvoted 1 times

 **dishum** 2 years, 1 month ago

Looks like C is the answer  
upvoted 2 times

 **GCPCloudArchitectUser** 2 years, 2 months ago

**Selected Answer: D**

CloudSQL is better and cheaper option compared to Spanner  
upvoted 2 times

 **hitmax87** 2 years ago

CloudSQL is regional.  
upvoted 1 times

 **syu31svc** 2 years, 10 months ago

"Expand availability of the application to new regions"  
"Ensure a consistent experience for users when they travel to different regions"

The above would indicate use of Cloud Spanner; answer should be C

upvoted 3 times

 **syu31svc** 2 years, 8 months ago

Changing to D Cloud SQL since qn50 answer is Cloud SQL  
Matter of consistency I believe  
upvoted 1 times

 **Kadhem** 4 months, 1 week ago

each question for case study is independent  
upvoted 1 times

Question #49

Topic 1

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Company Overview -

HipLocal is a community application designed to facilitate communication between people in close proximity. It is used for event planning and organizing sporting events, and for businesses to connect with their local communities. HipLocal launched recently in a few neighborhoods in Dallas and is rapidly growing into a global phenomenon. Its unique style of hyper-local community communication and business outreach is in demand around the world.

Executive Statement -

We are the number one local community app; it's time to take our local community services global. Our venture capital investors want to see rapid growth and the same great experience for new local and virtual communities that come online, whether their members are 10 or 10000 miles away from each other.

Solution Concept -

HipLocal wants to expand their existing service, with updated functionality, in new regions to better serve their global customers. They want to hire and train a new team to support these regions in their time zones. They will need to ensure that the application scales smoothly and provides clear uptime data.

Existing Technical Environment -

HipLocal's environment is a mix of on-premises hardware and infrastructure running in Google Cloud Platform. The HipLocal team understands their application well, but has limited experience in global scale applications. Their existing technical environment is as follows:

- \* Existing APIs run on Compute Engine virtual machine instances hosted in GCP.
- \* State is stored in a single instance MySQL database in GCP.
- \* Data is exported to an on-premises Teradata/Vertica data warehouse.
- \* Data analytics is performed in an on-premises Hadoop environment.
- \* The application has no logging.
- \* There are basic indicators of uptime; alerts are frequently fired when the APIs are unresponsive.

Business Requirements -

HipLocal's investors want to expand their footprint and support the increase in demand they are seeing. Their requirements are:

- \* Expand availability of the application to new regions.
- \* Increase the number of concurrent users that can be supported.
- \* Ensure a consistent experience for users when they travel to different regions.
- \* Obtain user activity metrics to better understand how to monetize their product.
- \* Ensure compliance with regulations in the new regions (for example, GDPR).
- \* Reduce infrastructure management time and cost.
- \* Adopt the Google-recommended practices for cloud computing.

Technical Requirements -

- \* The application and backend must provide usage metrics and monitoring.
- \* APIs require strong authentication and authorization.
- \* Logging must be increased, and data should be stored in a cloud analytics platform.

- \* Move to serverless architecture to facilitate elastic scaling.
  - \* Provide authorized access to internal apps in a secure manner.
- Which service should HipLocal use for their public APIs?

- A. Cloud Armor
- B. Cloud Functions
- C. Cloud Endpoints
- D. Shielded Virtual Machines

**Correct Answer: D**

*Community vote distribution*

C (100%)

 santoshchauhan 1 month, 3 weeks ago

Selected Answer: C

C. Cloud Endpoints

Cloud Endpoints is a service in Google Cloud that helps you create, deploy, and manage APIs. It offers features like monitoring, logging,

Question #50

Topic 1

#### Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

#### To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

#### Company Overview -

HipLocal is a community application designed to facilitate communication between people in close proximity. It is used for event planning and organizing sporting events, and for businesses to connect with their local communities. HipLocal launched recently in a few neighborhoods in Dallas and is rapidly growing into a global phenomenon. Its unique style of hyper-local community communication and business outreach is in demand around the world.

#### Executive Statement -

We are the number one local community app; it's time to take our local community services global. Our venture capital investors want to see rapid growth and the same great experience for new local and virtual communities that come online, whether their members are 10 or 10000 miles away from each other.

#### Solution Concept -

HipLocal wants to expand their existing service, with updated functionality, in new regions to better serve their global customers. They want to hire and train a new team to support these regions in their time zones. They will need to ensure that the application scales smoothly and provides clear uptime data.

#### Existing Technical Environment -

HipLocal's environment is a mix of on-premises hardware and infrastructure running in Google Cloud Platform. The HipLocal team understands their application well, but has limited experience in global scale applications. Their existing technical environment is as follows:

- \* Existing APIs run on Compute Engine virtual machine instances hosted in GCP.
- \* State is stored in a single instance MySQL database in GCP.
- \* Data is exported to an on-premises Teradata/Vertica data warehouse.
- \* Data analytics is performed in an on-premises Hadoop environment.
- \* The application has no logging.
- \* There are basic indicators of uptime; alerts are frequently fired when the APIs are unresponsive.

#### Business Requirements -

HipLocal's investors want to expand their footprint and support the increase in demand they are seeing. Their requirements are:

- \* Expand availability of the application to new regions.
- \* Increase the number of concurrent users that can be supported.
- \* Ensure a consistent experience for users when they travel to different regions.
- \* Obtain user activity metrics to better understand how to monetize their product.
- \* Ensure compliance with regulations in the new regions (for example, GDPR).
- \* Reduce infrastructure management time and cost.
- \* Adopt the Google-recommended practices for cloud computing.

#### Technical Requirements -

- \* The application and backend must provide usage metrics and monitoring.
- \* APIs require strong authentication and authorization.
- \* Logging must be increased, and data should be stored in a cloud analytics platform.
- \* Move to serverless architecture to facilitate elastic scaling.
- \* Provide authorized access to internal apps in a secure manner.

HipLocal wants to improve the resilience of their MySQL deployment, while also meeting their business and technical requirements.

Which configuration should they choose?

- A. Use the current single instance MySQL on Compute Engine and several read-only MySQL servers on Compute Engine.
- B. Use the current single instance MySQL on Compute Engine, and replicate the data to Cloud SQL in an external master configuration.
- C. Replace the current single instance MySQL instance with Cloud SQL, and configure high availability.
- D. Replace the current single instance MySQL instance with Cloud SQL, and Google provides redundancy without further configuration.

**Correct Answer: B**

*Community vote distribution*

C (100%)

✉️  **saurabh1805** Highly Voted 3 years, 5 months ago

C is correct answer

upvoted 10 times

✉️  **mastodilu** 2 years, 11 months ago

true, though with high availability data can be replicated in multiple regions with the risk of not being compliant with GDPR.  
The database should be replicated in specific regions, not globally, and I guess that this is achieved using multiple cloud sql instances rather than a single instance (or spanner) with high availability. Then those instances are kept synchronized with pubsub triggers.

I'm not sure though

upvoted 2 times

✉️  **GoReplyGCPExam** 1 year, 11 months ago

The HA configuration, sometimes called a cluster, provides data redundancy. A Cloud SQL instance configured for HA is also called a regional instance and is located in a primary and secondary zone within the configured region.

So the problem related to be GDPR compliant doesn't exist with Cloud SQL HA

<https://cloud.google.com/sql/docs/mysql/high-availability>

upvoted 1 times

✉️  **santoshchauhan** Most Recent 1 month, 3 weeks ago

**Selected Answer: C**

C. Replace the current single instance MySQL instance with Cloud SQL, and configure high availability.

Given HipLocal's requirements for improved resilience and considering their business and technical needs, moving to Cloud SQL with a high availability (HA) configuration is the most suitable choice. Cloud SQL is a fully managed database service that simplifies database maintenance, backups, and scalability. The high availability configuration in Cloud SQL ensures that there is a failover replica in a different zone, which provides automatic failover in case of an outage, thus improving the resilience of the deployment.

upvoted 1 times

 **Kadhem** 5 months, 4 weeks ago

D is the correct answer a cloud sql provide redundancy without further configuration.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: C**

C is correct.

upvoted 1 times

 **subesingh** 1 year, 7 months ago

C is the correct answer.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: C**

C is correct

upvoted 1 times

 **mariorossi** 2 years, 3 months ago

Probabilly is C, but they want use their implementation -> B

upvoted 1 times

 **ParagSanyashiv** 2 years, 3 months ago

**Selected Answer: C**

Correct Answer is C

upvoted 1 times

 **Flavio80** 2 years, 3 months ago

C is correct

upvoted 1 times

 **syu31svc** 2 years, 10 months ago

MySQL; so use Cloud SQL

<https://cloud.google.com/sql/docs/mysql/high-availability>

Answer is C

upvoted 2 times

Question #51

Topic 1

Your application is running in multiple Google Kubernetes Engine clusters. It is managed by a Deployment in each cluster. The Deployment has created multiple replicas of your Pod in each cluster. You want to view the logs sent to stdout for all of the replicas in your Deployment in all clusters.

Which command should you use?

- A. kubectl logs [PARAM]
- B. gcloud logging read [PARAM]
- C. kubectl exec -it [PARAM] journalctl
- D. gcloud compute ssh [PARAM] --command="sudo journalctl"

**Correct Answer: D**

*Community vote distribution*

B (100%)

 **tomato123** Highly Voted 1 year, 8 months ago

**Selected Answer: B**

B is correct

upvoted 5 times

✉  **omermahgoub**  1 year, 3 months ago

Answer is A:

To view the logs sent to stdout for all replicas in a Deployment in multiple clusters, the correct command to use would be kubectl logs [PARAM]

The gcloud logging read command reads log entries from the specified logs. It does not allow you to view the logs of specific replicas in a Deployment across multiple clusters. kubectl logs allows you to view the logs of a specific Pod or Deployment across multiple clusters. You can specify the Deployment name and the relevant parameters to view the logs of all replicas in the Deployment.

For example, the following command would allow you to view the logs of all replicas in a Deployment named "my-deployment" in all clusters:

kubectl logs -l app=my-deployment --all-containers

upvoted 5 times

✉  **omermahgoub** 1 year, 3 months ago

gcloud logging read [PARAM], can be used to read log entries from Stackdriver Logging, but it is not specifically designed for viewing the logs of Pods in a Kubernetes cluster. Additionally, gcloud logging read does not have a way to filter the log entries based on the Pod or Deployment, so it would not be possible to use it to view the logs for all of the replicas in a Deployment across multiple clusters

upvoted 1 times

✉  **santoshchauhan**  1 month, 3 weeks ago

**Selected Answer: B**

B. gcloud logging read [PARAM]: Google Cloud's operations suite (formerly known as Stackdriver) aggregates logs from all the pods across all the GKE clusters. By using gcloud logging read, you can query these logs with specific parameters (like the name of the Deployment, container or other filters) to view the combined logs from all replicas across all clusters. This command provides a centralized way to access logs at scale.

upvoted 1 times

✉  **\_rajan\_** 7 months, 1 week ago

**Selected Answer: B**

B is correct

upvoted 1 times

✉  **edward\_zhang** 1 year, 2 months ago

choose B. gcloud logging also can be used for querying pod log

<https://stackoverflow.com/questions/62007471/how-to-view-container-logs-via-stackdriver-on-gke>

upvoted 2 times

✉  **yogi\_508** 2 years ago

B

<https://cloud.google.com/sdk/gcloud/reference/logging/read>

upvoted 2 times

✉  **ParagSanyashiv** 2 years, 3 months ago

**Selected Answer: B**

Correct answer is B

upvoted 1 times

✉  **PrissMedrano** 2 years, 5 months ago

**Selected Answer: B**

Correct answer is B

upvoted 2 times

✉  **Valant** 2 years, 5 months ago

Correct answer is B

[https://cloud.google.com/logging/docs/reference/tools/gcloud-logging#examples\\_2](https://cloud.google.com/logging/docs/reference/tools/gcloud-logging#examples_2)

upvoted 2 times

✉  **therealsohail** 2 years, 6 months ago

A and B

upvoted 1 times

✉  **[Removed]** 2 years, 9 months ago

B with parameters : resource.type=( "k8s\_container" OR "container" OR "k8s\_cluster" OR "gke\_cluster" OR "gke\_nodepool" OR "k8s\_node" )  
upvoted 1 times

✉️ **celia20200410** 2 years, 9 months ago

B: gcloud logging read

Using the "gcloud logging read" command, select the appropriate cluster, node, pod, and container logs.  
[https://cloud.google.com/stackdriver/docs/solutions/gke/using-logs#accessing\\_your\\_logs](https://cloud.google.com/stackdriver/docs/solutions/gke/using-logs#accessing_your_logs)

However if you use "kubectl logs" to see logs on CLI, logs won't be seen readable. It prints each line as a JSON object.  
<https://medium.com/google-cloud/display-gke-logs-in-a-text-format-with-kubectl-db0169be0282>

upvoted 3 times

✉️ **syu31svc** 2 years, 9 months ago

<https://kubernetes.io/docs/reference/kubectl/cheatsheet/>

I would take A

upvoted 1 times

✉️ **syu31svc** 2 years, 9 months ago

Changing to B

<https://cloud.google.com/blog/products/management-tools/using-logging-your-apps-running-kubernetes-engine>:  
"gcloud command line tool – Using the gcloud logging read command, select the appropriate cluster, node, pod and container logs."  
upvoted 3 times

✉️ **kernel1973** 2 years, 10 months ago

B for me.

gcloud logging read

upvoted 3 times

✉️ **StelSen** 3 years, 2 months ago

Option: B. (Link1: <https://cloud.google.com/blog/products/management-tools/finding-your-gke-logs>, Link2:  
<https://cloud.google.com/sdk/gcloud/reference/logging/read>)

upvoted 3 times

✉️ **saurabh1805** 3 years, 5 months ago

A seems to be correct answer.

upvoted 4 times

✉️ **mastodilu** 2 years, 11 months ago

doesn't this view the logs of a single cluster?

upvoted 2 times

✉️ **kernel1973** 2 years, 10 months ago

You need to change the cluster connection's in order to view the logs for a specific deployments.

upvoted 1 times

Question #52

Topic 1

You are using Cloud Build to create a new Docker image on each source code commit to a Cloud Source Repositories repository. Your application is built on every commit to the master branch. You want to release specific commits made to the master branch in an automated method.

What should you do?

- A. Manually trigger the build for new releases.
- B. Create a build trigger on a Git tag pattern. Use a Git tag convention for new releases.
- C. Create a build trigger on a Git branch name pattern. Use a Git branch naming convention for new releases.
- D. Commit your source code to a second Cloud Source Repositories repository with a second Cloud Build trigger. Use this repository for new releases only.

**Correct Answer: C**

Reference:

<https://docs.docker.com/docker-hub/builds/>

*Community vote distribution*

B (100%)

 **saurabh1805** Highly Voted 3 years, 5 months ago

B is correct answer  
upvoted 19 times

 **santoshchauhan** Most Recent 1 month, 3 weeks ago

**Selected Answer: B**

B. Create a build trigger on a Git tag pattern. Use a Git tag convention for new releases.

This approach is effective for managing releases in an automated yet controlled manner. By creating a Cloud Build trigger that activates based on a specific Git tag pattern, you can automate the build and deployment process for new releases. Git tags are often used to mark release points in the repository, so this aligns well with common development practices.

When a commit is tagged in the repository with a specific pattern (e.g., "v1.0", "release-\*"), Cloud Build can automatically trigger a build and potentially a deployment process. This allows for a more deliberate release process compared to triggering on every commit to the master branch.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: B**

B is correct.  
upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: B**

B is correct  
upvoted 3 times

 **nehaxlpb** 1 year, 9 months ago

**Selected Answer: B**

I don't know why people are selecting C , the question says commit to master . C literally does not make sense how commit to a feature branch can trigger a master build.

upvoted 3 times

 **nqthien041292** 2 years ago

**Selected Answer: B**

Vote B  
upvoted 2 times

 **Khratata** 2 years, 6 months ago

I think C correct answer  
upvoted 1 times

 **[Removed]** 2 years, 9 months ago

C) is not correct because the question says the commits are made in master branch.  
B) is good answer. When you want a release create a tag release-\* , in Cloud Build use this pattern for tag.  
upvoted 4 times

 **syu31svc** 2 years, 9 months ago

<https://cloud.google.com/source-repositories/docs/integrating-with-cloud-build>:  
"you can set a trigger to start a build on commits that are made to a particular branch, or on commits that contain a particular tag"

I would take C since the qn states that the commit is made to a branch

upvoted 2 times

 **gcp0omkar** 2 years, 6 months ago

specific commits made to the master branch --> Tag would work here, team can continue pushing further changes in master branch, tag v point to specific version, so I feel correct answer is B

upvoted 1 times

 **pythonrocks** 3 years ago

C. <https://cloud.google.com/build/docs/automating-builds/create-manage-triggers> has either branch pattern or tag pattern

upvoted 1 times

 **maxdanny** 3 years, 1 month ago

Also B is correct, but in the questions is specified "branch name" , not tag

upvoted 4 times

 **lollo1234** 2 years, 10 months ago

"You want to release specific commits made to the master branch in an automated method"

Looks like they're committing to the master branch, hence a tag would make more sense than a branch name.

upvoted 4 times

 **boof** 2 years, 7 months ago

"Your application is built on every commit to the master branch. You want to release SPECIFIC commits made to the master branch in an automated method."

Question #53

Topic 1

You are designing a schema for a table that will be moved from MySQL to Cloud Bigtable. The MySQL table is as follows:

```
AccountActivity
(
  Account_id int,
  Event_timestamp datetime,
  Transaction_type string,
  Amount numeric(18, 4)
) primary key (Account_id, Event_timestamp)
```

How should you design a row key for Cloud Bigtable for this table?

- A. Set Account\_id as a key.
- B. Set Account\_id\_Event\_timestamp as a key.
- C. Set Event\_timestamp\_Account\_id as a key.
- D. Set Event\_timestamp as a key.

**Correct Answer: C**

*Community vote distribution*

B (100%)

 **salgabri** Highly Voted 3 years, 5 months ago

correct answer is B

<https://cloud.google.com/bigtable/docs/schema-design>

upvoted 20 times

 **syu31svc** 2 years, 9 months ago

From the link:

"Include a timestamp as part of your row key if you often need to retrieve data based on the time when it was recorded."

For example, your application might need to record performance-related data, such as CPU and memory usage, once per second for a large number of machines. Your row key for this data could combine an identifier for the machine with a timestamp for the data (for example, machine\_4223421#1425330757685). Keep in mind that row keys are sorted lexicographically."

upvoted 3 times

 **santoshchauhan** Most Recent 1 month, 3 weeks ago

**Selected Answer: B**

Designing an appropriate row key for Cloud Bigtable requires considering the access patterns and ensuring that the read and write operations are spread evenly across the key space to avoid hotspots.

B. Set Account\_id\_Event\_timestamp as a key.

This option is likely the best choice because:

Combining Account\_id with Event\_timestamp in the row key would allow you to maintain a good level of data distribution while preserving the ability to query efficiently by Account\_id and sort by Event\_timestamp within each account. This aligns well with Bigtable's strengths in handling large, scalable, and sparse datasets.

By leading with Account\_id, you group all events for a single account close together in the key space, which can be efficient for reads that are interested in the activity of a specific account.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: B**

I would go with B.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

B. Set Account\_id\_Event\_timestamp as a key.

The primary key in the MySQL table is a composite key consisting of Account\_id and Event\_timestamp, so it would make sense to use both of these values as the row key in Cloud Bigtable. This allows for efficient querying and sorting by both Account\_id and Event\_timestamp.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

A would not be a good choice because the row key would not include the Event\_timestamp, which is part of the primary key in the MySQL table. Option

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

D would not be a good choice because it would not include the Account\_id, which is also part of the primary key in the MySQL table.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

C would not be a good choice because it would make it difficult to query and sort by Account\_id.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: B**

B is correct

upvoted 3 times

 **maxdanny** 1 year, 9 months ago

**Selected Answer: B**

<https://cloud.google.com/bigtable/docs/schema-design#row-keys>

It's B because :

"Row keys that start with a timestamp. This pattern causes sequential writes to be pushed onto a single node, creating a hotspot. If you put a timestamp in a row key, precede it with a high-cardinality value like a user ID to avoid hotspotting."

upvoted 3 times

 **saumabhaM** 2 years ago

**Selected Answer: B**

Include a timestamp as part of your row key and avoid having timestamp at the start of the key  
upvoted 1 times

 **whigy** 3 years, 5 months ago

Should be C. Account id as the first part of the key has no benifit for search  
upvoted 1 times

 **mastodilu** 2 years, 11 months ago

<https://cloud.google.com/bigtable/docs/schema-design#row-keys>  
avoid row keys that starts with a timestamp.

Also using a key such as userID\_timestamp allows bigtable to query related rows in a range rather than parsing the entire database.  
upvoted 4 times

 **donchick** 3 years, 4 months ago

<https://cloud.google.com/bigtable/docs/schema-design#timestamps> - avoid placing a timestamp at the start of the row key. I vote for B.  
upvoted 6 times

 **fraloca** 3 years, 3 months ago

"Row keys that start with a timestamp. This will cause sequential writes to be pushed onto a single node, creating a hotspot. If you put timestamp in a row key, you need to precede it with a high-cardinality value like a user ID to avoid hotspotting."  
upvoted 8 times

Question #54

Topic 1

You want to view the memory usage of your application deployed on Compute Engine.

What should you do?

- A. Install the Stackdriver Client Library.
- B. Install the Stackdriver Monitoring Agent.
- C. Use the Stackdriver Metrics Explorer.
- D. Use the Google Cloud Platform Console.

**Correct Answer: C**

Reference:

<https://stackoverflow.com/questions/43991246/google-cloud-platform-how-to-monitor-memory-usage-of-vm-instances>

*Community vote distribution*

B (100%)

-  **StelSen** Highly Voted  3 years, 2 months ago  
Option-B is correct. [https://cloud.google.com/monitoring/api/metrics\\_agent#agent-memory](https://cloud.google.com/monitoring/api/metrics_agent#agent-memory) (By default Memory metrics is not collected). To double confirm. Just goto Console->Operations->Monitoring->Dashboards->VM Instances->Memory Tab (Assume you have VM running already). You will see a info message saying that No agents detected. Monitoring agents collect memory metrics, disk metrics, and more. Learn more about agents and how to manage them across multiple VMs.  
upvoted 16 times
-  **Ram02** 2 years, 7 months ago  
Correct, see following link for more detail  
<https://stackoverflow.com/questions/43991246/google-cloud-platform-how-to-monitor-memory-usage-of-vm-instances>  
upvoted 3 times
-  **dxxdd7** Highly Voted  3 years, 3 months ago  
For me B si the correct answer as you can not read memory usage directly from stackdriver without the monitoring agent  
upvoted 8 times
-  **santoshchauhan** Most Recent  1 month, 3 weeks ago  
Selected Answer: B  
B. Install the Stackdriver Monitoring Agent.  
  
The Stackdriver Monitoring Agent allows you to collect more system-level and third-party application metrics than what is provided by default with Google Cloud's operations suite. By installing the agent on your Compute Engine instances, you can collect detailed memory usage metrics which can then be viewed in the Google Cloud Console or through the Metrics Explorer in Google Cloud's operations suite (formerly Stackdriver).  
upvoted 1 times
-  **\_rajan\_** 7 months, 1 week ago  
Selected Answer: B  
I would go with B.  
upvoted 1 times
-  **tomato123** 1 year, 8 months ago  
Selected Answer: B  
B is correct  
upvoted 3 times
-  **nqthien041292** 2 years ago  
Selected Answer: B  
Vote B  
upvoted 1 times
-  **syu31svc** 2 years, 9 months ago  
<https://cloud.google.com/monitoring/agent>  
  
B is correct  
upvoted 3 times
-  **dwbi\_shrikant** 3 years, 1 month ago

Question #55

Topic 1

You have an analytics application that runs hundreds of queries on BigQuery every few minutes using BigQuery API. You want to find out how much time these queries take to execute.

What should you do?

- A. Use Stackdriver Monitoring to plot slot usage.
- B. Use Stackdriver Trace to plot API execution time.
- C. Use Stackdriver Trace to plot query execution time.
- D. Use Stackdriver Monitoring to plot query execution times.

Correct Answer: D

*Community vote distribution*

D (67%)

C (33%)

 **saurabh1805** Highly Voted 3 years, 5 months ago

You dont need to enable trace for this, Best and correct option is D

upvoted 7 times

 **fraloca** 3 years, 4 months ago

D is correct answer: <https://cloud.google.com/bigquery/docs/monitoring>

upvoted 8 times

 **syu31svc** 2 years, 9 months ago

"Use Cloud Monitoring to view BigQuery metrics and create charts and alerts"

upvoted 2 times

 **StelSen** 3 years, 2 months ago

Use this link and locate BigQuery: [https://cloud.google.com/monitoring/api/metrics\\_gcp#gcp-bigquery](https://cloud.google.com/monitoring/api/metrics_gcp#gcp-bigquery)

upvoted 2 times

 **santoshchauhan** Most Recent 1 month, 3 weeks ago

Selected Answer: D

D. Use Stackdriver Monitoring to plot query execution times.

Stackdriver Monitoring (now part of Google Cloud's operations suite) provides capabilities to monitor BigQuery and create custom dashboard visualize various metrics, including query execution times. You can track how long your queries take to run by plotting the query\_execution\_time metric in a custom dashboard.

upvoted 1 times

 **mohammeddigital** 3 months, 4 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

Selected Answer: C

Option C is best suited here.

upvoted 1 times

 **maxdanny** 8 months, 1 week ago

Selected Answer: C

<https://www.exam-answer.com/the-best-way-to-measure-query-execution-time-in-bigquery>

upvoted 1 times

 **Teraflow** 1 year, 1 month ago

Selected Answer: C

The correct answer is C. Use Stackdriver Trace to plot query execution time. Stackdriver Trace is a distributed tracing system that allows you profile and debug your application's performance. It allows you to trace requests across multiple services, and it provides a detailed breakdown of where time is being spent within your application. Since you want to find out how much time your queries take to execute, using Stackdriver Trace to plot query execution time would be the most appropriate approach.

upvoted 1 times

 **telp** 1 year, 3 months ago

Selected Answer: D

D is correct

<https://cloud.google.com/bigquery/docs/monitoring>

upvoted 1 times

 **tomato123** 1 year, 8 months ago

Selected Answer: D

D is correct

upvoted 3 times

You are designing a schema for a Cloud Spanner customer database. You want to store a phone number array field in a customer table. You also want to allow users to search customers by phone number.

How should you design this schema?

- A. Create a table named Customers. Add an Array field in a table that will hold phone numbers for the customer.
- B. Create a table named Customers. Create a table named Phones. Add a CustomerId field in the Phones table to find the CustomerId from a phone number.
- C. Create a table named Customers. Add an Array field in a table that will hold phone numbers for the customer. Create a secondary index on the Array field.
- D. Create a table named Customers as a parent table. Create a table named Phones, and interleave this table into the Customer table. Create an index on the phone number field in the Phones table.

**Correct Answer: C**

*Community vote distribution*

D (88%)

13%

 **dendut** Highly Voted 3 years, 3 months ago

i vote D since it said 'interleave'

upvoted 12 times

 **StelSen** 3 years, 2 months ago

Correct. Just sharing a link: [https://cloud.google.com/spanner/docs/schema-and-data-model#creating\\_a\\_hierarchy\\_of\\_interleaved\\_tables](https://cloud.google.com/spanner/docs/schema-and-data-model#creating_a_hierarchy_of_interleaved_tables)  
upvoted 7 times

 **fosky94** Highly Voted 3 years ago

Correct answer is C, as in the question states: "You want to store a phone number array field in a customer table". So... adding the phone number as array field and adding a secondary index should be the best option in this case.

upvoted 7 times

 **mastodilu** 2 years, 11 months ago

i say B, because if a user has more numbers you are storing the same user multiple times each time changing the phone number.  
Having a second table for phone numbers and having a foreign key that points to the user with this phone number avoid this duplication problem.

upvoted 1 times

 **santoshchauhan** Most Recent 1 month, 3 weeks ago

**Selected Answer: D**

D. Create a table named Customers as a parent table. Create a table named Phones, and interleave this table into the Customer table. Create index on the phone number field in the Phones table.

This design will allow you to store multiple phone numbers for each customer and efficiently search for customers by their phone numbers. In Cloud Spanner, tables can be interleaved, which means that the child table's rows are co-located with the parent table's rows. This setup can offer better performance for certain types of queries and data models, especially when there's a strong relational structure.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: D**

I will go with D.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

The correct answer is D. You should create a table named Customers as a parent table and a table named Phones, and interleave this table in the Customer table. You should also create an index on the phone number field in the Phones table. This allows you to store the phone number array field in the Customers table and search for customers by phone number using the index on the Phones table.

upvoted 3 times

 **omermahgoub** 1 year, 3 months ago

C is not a valid solution because Cloud Spanner does not allow creating secondary indexes on array fields.

upvoted 3 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: D**

D is correct

upvoted 3 times

 **akshaychavan7** 1 year, 9 months ago

**Selected Answer: D**

It's D.

upvoted 1 times

 **keshav1** 1 year, 10 months ago

**Selected Answer: A**

Search on ARRAY column is best here. Answer: A

upvoted 1 times

 **Ksamilosb** 2 years, 2 months ago

D seems quite nice, but what do u think about statement "You want to store a phone number array field in a customer table.", and interleave it another table, not customer one.

In sql there is array field, and using UNNEST function is possible to filter records based on array, then answer A

upvoted 3 times

 **ParagSanyashiv** 2 years, 3 months ago

**Selected Answer: D**

D is the correct answer

upvoted 1 times

 **syu31svc** 2 years, 9 months ago

<https://cloud.google.com/spanner/docs/schema-design#creating-indexes>:  
"bad idea to create non-interleaved indexes on columns whose values are monotonically increasing or decreasing"

Since phone numbers monotonically increase/decrease, I would take D as the answer

upvoted 1 times

 **yuchun** 2 years, 10 months ago

<https://cloud.google.com/spanner/docs/data-types> -->can't set secondary index in array  
so I vote D

upvoted 4 times

Question #57

Topic 1

You are deploying a single website on App Engine that needs to be accessible via the URL <http://www.altostrat.com/>.

What should you do?

- A. Verify domain ownership with Webmaster Central. Create a DNS CNAME record to point to the App Engine canonical name ghs.googlehosted.com.
- B. Verify domain ownership with Webmaster Central. Define an A record pointing to the single global App Engine IP address.
- C. Define a mapping in dispatch.yaml to point the domain www.altostrat.com to your App Engine service. Create a DNS CNAME record to point to the App Engine canonical name ghs.googlehosted.com.

D. Define a mapping in dispatch.yaml to point the domain www.altostrat.com to your App Engine service. Define an A record pointing to the single global App Engine IP address.

**Correct Answer: A**

Reference:

<https://cloud.google.com/appengine/docs/flexible/dotnet/mapping-custom-domains?hl=fa>

*Community vote distribution*

A (100%)

 **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: A**

A is correct.

upvoted 1 times

 **telp** 1 year, 3 months ago

**Selected Answer: A**

A, I have done that on a project and you don't need to fo routing with a dispatch.yaml file so A is enough to have a custom domain link to you app engine.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Yes, you are correct guys that you can use a custom domain with App Engine and map it to your app. However, option A is incorrect because not sufficient to just create a DNS CNAME record pointing to the App Engine canonical name ghs.googlehosted.com. You also need to map t! domain to your app in App Engine as described in option C or D.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

D is incorrect because it involves defining an A record, which can cause issues with latency and is not the recommended method for mapr a custom domain to App Engine. Additionally, it does not include the dispatch.yaml mapping, which is necessary to associate the custom domain with your App Engine service.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

The correct answer is C. To use a custom domain with App Engine, you need to define a mapping in the dispatch.yaml file to point the dor to your App Engine service. Additionally, you should create a DNS CNAME record to point to the App Engine canonical name ghs.googlehosted.com.

upvoted 2 times

 **omermahgoub** 1 year, 3 months ago

Option A is incorrect because it does not include the dispatch.yaml mapping, which is necessary to associate the custom domain with you App Engine service.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

B is incorrect because it involves defining an A record, which can cause issues with latency and is not the recommended method for mapr a custom domain to App Engine.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: A**

A is correct

upvoted 3 times

 **nqthien041292** 2 years ago

**Selected Answer: A**

Vote A

upvoted 2 times

 **herocc** 2 years, 3 months ago

A is right

upvoted 2 times

 **Gini** 2 years, 5 months ago

Agree with A. That is what we are doing in our current project.

upvoted 2 times

 **celia20200410** 2 years, 9 months ago

A:

<https://support.google.com/domains/answer/6009957?hl=en>  
app.mydomain.com CNAME 1H ghs.googlehosted.com.

upvoted 3 times

 **syu31svc** 2 years, 9 months ago

I would take B

<https://cloud.google.com/appengine/docs/flexible/dotnet/mapping-custom-domains?hl=fa>:

"In A or AAAA records, the record data is an IP address"

upvoted 2 times

 **syu31svc** 2 years, 9 months ago

Changing to A based on the link celia20200410 gave

upvoted 1 times

 **saurabh1805** 3 years, 5 months ago

A is correct option here.

upvoted 3 times

You are running an application on App Engine that you inherited. You want to find out whether the application is using insecure binaries or is vulnerable to XSS attacks.

Which service should you use?

- A. Cloud Armor
- B. Stackdriver Debugger
- C. Cloud Security Scanner
- D. Stackdriver Error Reporting

**Correct Answer: C**

Reference:

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

*Community vote distribution*

C (100%)

 **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: C**

C is correct.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: C**

C is correct

upvoted 3 times

 **nqthien041292** 2 years ago

**Selected Answer: C**

Vote C

upvoted 2 times

 **syu31svc** 2 years, 9 months ago

<https://cloud.google.com/appengine/docs/standard/python/application-security>:

"The Google Cloud Web Security Scanner discovers vulnerabilities by crawling your App Engine app, following all the links within the scope of your starting URLs, and attempting to exercise as many user inputs and event handlers as possible."

<https://cloud.google.com/security-command-center/docs/concepts-web-security-scanner-overview>:

"Web Security Scanner custom scans provide granular information about application vulnerability findings, like outdated libraries, cross-site scripting, or use of mixed content"

C is correct

upvoted 1 times

 **saurabh1805** 3 years, 5 months ago

C is correct answer here.

<https://cloud.google.com/appengine/docs/standard/python/application-security>

upvoted 2 times

You are working on a social media application. You plan to add a feature that allows users to upload images. These images will be 2 MB ~ 1 GB in size. You want to minimize their infrastructure operations overhead for this feature.

What should you do?

- A. Change the application to accept images directly and store them in the database that stores other user information.
- B. Change the application to create signed URLs for Cloud Storage. Transfer these signed URLs to the client application to upload images to Cloud Storage.
- C. Set up a web server on GCP to accept user images and create a file store to keep uploaded files. Change the application to retrieve images from the file store.
- D. Create a separate bucket for each user in Cloud Storage. Assign a separate service account to allow write access on each bucket. Transfer service account credentials to the client application based on user information. The application uses this service account to upload images to Cloud Storage.

**Correct Answer: B**

Reference:

<https://cloud.google.com/blog/products/storage-data-transfer/uploading-images-directly-to-cloud-storage-by-using-signed-url>

*Community vote distribution*

B (100%)

 **syu31svc** Highly Voted 2 years, 9 months ago

"upload images" so use Cloud Storage; leaving B and D

"minimize their infrastructure operations" so B is the answer

Also, signed URLs provide additional security

upvoted 5 times

 **\_\_rajan\_\_** Most Recent 7 months, 1 week ago

Selected Answer: B

B is correct

upvoted 1 times

 **tomato123** 1 year, 8 months ago

Selected Answer: B

B is correct

upvoted 3 times

 **nqthien041292** 2 years ago

Selected Answer: B

Vote B

upvoted 2 times

 **saurabh1805** 3 years, 5 months ago

B seems to be logical answer here.

upvoted 3 times

Your application is built as a custom machine image. You have multiple unique deployments of the machine image. Each deployment is a separate managed instance group with its own template. Each deployment requires a unique set of configuration values. You want to provide these unique

values to each deployment but use the same custom machine image in all deployments. You want to use out-of-the-box features of Compute Engine.

What should you do?

- A. Place the unique configuration values in the persistent disk.
- B. Place the unique configuration values in a Cloud Bigtable table.
- C. Place the unique configuration values in the instance template startup script.
- D. Place the unique configuration values in the instance template instance metadata.

**Correct Answer: A**

Reference:

<https://cloud.google.com/compute/docs/instance-groups>

*Community vote distribution*

D (100%)

✉️  **syu31svc** Highly Voted 2 years, 9 months ago

A and B are wrong for sure

<https://cloud.google.com/compute/docs/instances/startup-scripts>:

"A startup script is a file that contains commands that run when a virtual machine (VM) instance boots:

Answer is D

upvoted 7 times

✉️  **saurabh1805** Highly Voted 3 years, 5 months ago

C would be correct answer here.

upvoted 6 times

✉️  **santoshchauhan** Most Recent 1 month, 3 weeks ago

**Selected Answer: D**

D. Place the unique configuration values in the instance template instance metadata.

The instance metadata is a good place to store configuration values that are unique to each managed instance group while using the same machine image across all deployments. This allows you to use the same base image but customize the behavior of each instance group based on the metadata passed to them. Metadata can be accessed by the instances at startup, and scripts can be written to configure the instance based on these values.

upvoted 1 times

✉️  **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: D**

D is correct.

upvoted 1 times

✉️  **omermahgoub** 1 year, 3 months ago

Option D is the correct answer. Instance metadata is metadata that is associated with a Compute Engine instance and can be used to pass configuration values to the instance at startup. It can be accessed from within the instance itself, allowing you to use the same custom machine image in all deployments and still provide unique configuration values to each deployment. Option A is not a good solution because the persistent disk is not automatically attached to the instance at startup and is not intended for storing configuration values. Option B is not a good solution because Cloud Bigtable is a NoSQL database, which is not well-suited for storing configuration values. Option C is not a good solution because the startup script is executed after the instance has started, so it cannot be used to pass configuration values to the instance at startup.

upvoted 2 times

✉️  **brunoguzzo18** 1 year, 8 months ago

**Selected Answer: D**

Configuration values should be metadata

upvoted 2 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: D**

D is correct

upvoted 3 times

 **szl0144** 1 year, 11 months ago

the answer should be D

upvoted 1 times

 **ParagSanyashiv** 2 years, 3 months ago

**Selected Answer: D**

Correct answer is D

upvoted 2 times

 **Valant** 2 years, 5 months ago

No - In this case it is a stateful MIG - per this link the answer is indeed A:

[https://cloud.google.com/compute/docs/instance-groups/stateful-migs#per\\_instance\\_configs](https://cloud.google.com/compute/docs/instance-groups/stateful-migs#per_instance_configs)

upvoted 1 times

 **worheck93** 2 years, 7 months ago

Each deployment is a separate managed instance group with its own template.

Each deployment requires a unique set of configuration values.

Either be C or D

Configuration values should be metadata

Which leads the answer to be D

upvoted 3 times

 **kernel1973** 2 years, 10 months ago

Option could be D.

upvoted 4 times

 **dwbi\_shrikant** 3 years, 1 month ago

Option D: at the time of deployment, configuration values in the instance template instance metadata.

upvoted 4 times

 **ktktoh** 3 years ago

Agree with Option D based on this ref: <https://cloud.google.com/compute/docs/storing-retrieving-metadata#custom>

upvoted 5 times

 **yuchun** 2 years, 10 months ago

agree with option D

upvoted 4 times

Question #61

Topic 1

Your application performs well when tested locally, but it runs significantly slower after you deploy it to a Compute Engine instance. You need to diagnose the problem. What should you do?

What should you do?

- A. File a ticket with Cloud Support indicating that the application performs faster locally.
- B. Use Cloud Debugger snapshots to look at a point-in-time execution of the application.
- C. Use Cloud Profiler to determine which functions within the application take the longest amount of time.

D. Add logging commands to the application and use Cloud Logging to check where the latency problem occurs.

**Correct Answer: D**

*Community vote distribution*

C (100%)

 **santoshchauhan** 1 month, 3 weeks ago

**Selected Answer: C**

C. Use Cloud Profiler to determine which functions within the application take the longest amount of time.

Cloud Profiler is a tool provided by Google Cloud that helps you analyze and understand the performance characteristics of your application. It allows you to see where the application spends its time, how much CPU and memory it uses, and which functions or methods are the most time-consuming. This is particularly useful when you need to diagnose performance bottlenecks that are not apparent during local development but become evident in a production environment, such as a Compute Engine instance.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: C**

C is correct

upvoted 1 times

 **telp** 1 year, 3 months ago

**Selected Answer: C**

A is incorrect because the argument "it worked on my machine" but doesn't work on Google Cloud is never valid.

B is incorrect because Debugger snapshots only lets us review the application at a single point in time.

C is correct because it provides latency per function and historical latency information.

D is incorrect because while it works it requires a lot of work and is not the clear, optimal choice.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Option C is the correct answer. Cloud Profiler is a performance analysis tool that allows you to identify performance issues in your application. It provides detailed information about the time spent executing different functions in your application, which can help you identify the cause of the performance issue. Option A is not a good solution because filing a ticket with Cloud Support will not help you diagnose the problem. Option B is not a good solution because Cloud Debugger snapshots provide information about the state of variables at a specific point in time, but they do not provide information about the time spent executing different functions. Option D is not a good solution because adding logging commands to the application and using Cloud Logging can help you identify where the latency problem occurs, but it will not provide information about the time spent executing different functions.

upvoted 1 times

 **subesingh** 1 year, 7 months ago

C is the correct answer

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: C**

C is correct

upvoted 3 times

 **maxdanny** 1 year, 9 months ago

**Selected Answer: C**

Correct is C

upvoted 1 times

 **ParagSanyashiv** 2 years, 3 months ago

**Selected Answer: C**

Correct answer is C

upvoted 3 times

 **mister** 2 years, 3 months ago

This should be C

upvoted 1 times

You have an application running in App Engine. Your application is instrumented with Stackdriver Trace. The /product-details request reports details about four known unique products at /sku-details as shown below. You want to reduce the time it takes for the request to complete. What should you do?

**Timeline**

- A. Increase the size of the instance class.
- B. Change the Persistent Disk type to SSD.
- C. Change /product-details to perform the requests in parallel.
- D. Store the /sku-details information in a database, and replace the webservice call with a database query.

**Correct Answer: C**

*Community vote distribution*

C (100%)

 **certificationguru**  3 years, 2 months ago

I agree with this, answer is C

upvoted 9 times

 **\_rajan\_**  7 months, 1 week ago

**Selected Answer: C**

C is correct.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Option C is the correct answer. By changing /product-details to perform the requests in parallel, you can reduce the time it takes for the request to complete by making multiple requests at the same time rather than sequentially. This will allow you to retrieve the information for all four products more quickly. Option A is not a good solution because increasing the size of the instance class may not necessarily reduce the time it takes for the request to complete. Option B is not a good solution because changing the Persistent Disk type to SSD will not have any impact on the time it takes for the request to complete. Option D is not a good solution because storing the /sku-details information in a database and replacing the webservice call with a database query will not necessarily reduce the time it takes for the request to complete, and it will add unnecessary complexity to the application.

upvoted 1 times

 **N8dagr8** 1 year, 7 months ago

**Selected Answer: C**

C feels right

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: C**

C is correct

upvoted 1 times

 **kinoko1330** 1 year, 8 months ago

**Selected Answer: C**

Question #63

Topic 1

Your company has a data warehouse that keeps your application information in BigQuery. The BigQuery data warehouse keeps 2 PBs of user data.

Recently, your company expanded your user base to include EU users and needs to comply with these requirements:

⇒ Your company must be able to delete all user account information upon user request.

⇒ All EU user data must be stored in a single region specifically for EU users.

Which two actions should you take? (Choose two.)

- A. Use BigQuery federated queries to query data from Cloud Storage.
- B. Create a dataset in the EU region that will keep information about EU users only.
- C. Create a Cloud Storage bucket in the EU region to store information for EU users only.
- D. Re-upload your data using to a Cloud Dataflow pipeline by filtering your user records out.
- E. Use DML statements in BigQuery to update/delete user records based on their requests.

**Correct Answer: CE**

Reference:

<https://cloud.google.com/solutions/bigquery-data-warehouse>

*Community vote distribution*

BE (88%)

13%

 **saurabh1805**  3 years, 5 months ago

B and E is correct answer for me.

upvoted 11 times

cloud\_mk 3 years ago

Second point "must be stored in a single region specifically for EU users" will achieve through option C only hence for me C and E is correct answer

upvoted 2 times

Ayuewinc 3 years ago

Bigquery dataset can choose single region to store data, so B would be better

upvoted 3 times

syu31svc Highly Voted 2 years, 9 months ago

<https://cloud.google.com/bigquery/docs/reference/standard-sql/data-manipulation-language>

The link above supports E since "delete all user account information upon user request" as per qn

<https://cloud.google.com/architecture/bigquery-data-warehouse>:

"A dataset is bound to a location. The dataset locations are as follows:

Multi-regional: A large geographic area, such as the United States, that contains two or more geographic places."

B is the other answer

upvoted 5 times

santoshchauhan Most Recent 1 month, 3 weeks ago

Selected Answer: BE

B. Creating a separate dataset in the EU region for EU users allows your company to ensure that all data for these users is stored in a specific geographic location, complying with regional data residency requirements. BigQuery allows you to select the region where your dataset resides and having a dedicated dataset for EU users makes it easier to manage and enforce policies specific to EU data.

E. Using Data Manipulation Language (DML) statements in BigQuery (such as DELETE and UPDATE) enables your company to comply with requests to delete or modify user account information. This capability is essential for adhering to regulations like the GDPR, which may require companies to delete users' personal data upon request.

upvoted 1 times

\_rajan\_ 7 months, 1 week ago

Selected Answer: BE

Best option is BE.

upvoted 1 times

omermahgoub 1 year, 3 months ago

B and E are the correct answers. To comply with the requirements, you should create a dataset in the EU region that will keep information about EU users only. This will allow you to store all EU user data in a single region specifically for EU users. Additionally, you should use DML statements in BigQuery to update or delete user records based on their requests. This will allow you to delete all user account information upon user request as required.

upvoted 1 times

omermahgoub 1 year, 3 months ago

A is not a good solution because using BigQuery federated queries to query data from Cloud Storage does not address either of the requirements. Federated queries allow you to query data that is stored outside of BigQuery, such as in Cloud Storage, but they do not help you store data in a specific region or delete data upon request

upvoted 1 times

omermahgoub 1 year, 3 months ago

C is not a good solution because creating a Cloud Storage bucket in the EU region does not address either of the requirements. A Cloud Storage bucket is simply a storage location, and it does not allow you to store data in a specific region or delete data upon request.

upvoted 1 times

omermahgoub 1 year, 3 months ago

D is not a good solution because re-uploading your data using a Cloud Dataflow pipeline is unnecessarily complex and does not address either of the requirements. Filtering user records out during the re-upload process does not allow you to store data in a specific region or delete data upon request.

upvoted 1 times

tomato123 1 year, 8 months ago

Selected Answer: BE

BE are correct sorry

upvoted 2 times

✉️  **tomato123** 1 year, 8 months ago

**Selected Answer: BD**

BD are correct

upvoted 1 times

✉️  **maxdanny** 1 year, 9 months ago

**Selected Answer: BE**

Cloud Storage is out of scope !!

upvoted 1 times

✉️  **nqthien041292** 2 years ago

**Selected Answer: BE**

Vote BE

upvoted 1 times

✉️  **ParagSanyashiv** 2 years, 3 months ago

**Selected Answer: BE**

B and E are the correct answer

upvoted 1 times

✉️  **Gini** 2 years, 4 months ago

B & E. Data is already stored in BigQuery, I do not see any reason to have anything to do with Cloud Storage. Also, BigQuery allows DML to d updates and deletes. So I would choose B & E

upvoted 2 times

Question #64

Topic 1

Your App Engine standard configuration is as follows:

service: production

instance\_class: B1

You want to limit the application to 5 instances.

Which code snippet should you include in your configuration?

- A. manual\_scaling: instances: 5 min\_pending\_latency: 30ms
- B. manual\_scaling: max\_instances: 5 idle\_timeout: 10m
- C. basic\_scaling: instances: 5 min\_pending\_latency: 30ms
- D. basic\_scaling: max\_instances: 5 idle\_timeout: 10m

**Correct Answer: C**

*Community vote distribution*

D (91%)

9%

✉️  **santoshchauhan** 1 month, 3 weeks ago

**Selected Answer: D**

Basic Scaling with max\_instances (Option D): Basic scaling is suitable for applications that do not need to keep instances running all the time may require instances to handle requests and then shut down when idle. The max\_instances parameter sets the maximum number of instances and idle\_timeout specifies the amount of time that an instance can stay idle before it is shut down.

upvoted 1 times

✉  **\_\_rajan\_\_** 7 months, 1 week ago

D is correct.

upvoted 1 times

✉  **maxdanny** 8 months ago

The correct answer is D, only configuration permitted and lawful according to documentation:

[https://cloud.google.com/appengine/docs/standard/reference/app-yaml?tab=python#manual\\_scaling](https://cloud.google.com/appengine/docs/standard/reference/app-yaml?tab=python#manual_scaling)

upvoted 1 times

✉  **omermahgoub** 1 year, 3 months ago

The correct answer is D, which specifies the max\_instances parameter of the basic\_scaling configuration to limit the application to a maximum of 5 instances. The basic\_scaling configuration is used for applications that are driven by user activity, and it allows you to specify the maximum number of instances that you want to run using the max\_instances parameter.

upvoted 1 times

✉  **omermahgoub** 1 year, 3 months ago

B is not a good solution because the manual\_scaling configuration is not being used, and the idle\_timeout parameter has no effect on the maximum number of instances.

upvoted 1 times

✉  **omermahgoub** 1 year, 3 months ago

A is not a good solution because the manual\_scaling configuration is not being used, and the min\_pending\_latency parameter has no effect on the maximum number of instances.

upvoted 1 times

✉  **omermahgoub** 1 year, 3 months ago

C is not a good solution because the min\_pending\_latency parameter is used to specify a minimum amount of time that a request should wait before an instance is started, but it has no effect on the maximum number of instances.

upvoted 1 times

✉  **tomato123** 1 year, 8 months ago

**Selected Answer: D**

D is correct

upvoted 4 times

✉  **nehaxlpb** 1 year, 9 months ago

**Selected Answer: D**

[https://cloud.google.com/appengine/docs/legacy/standard/python/how-instances-are-managed#scaling\\_types](https://cloud.google.com/appengine/docs/legacy/standard/python/how-instances-are-managed#scaling_types)

upvoted 2 times

✉  **maxdanny** 1 year, 9 months ago

**Selected Answer: C**

C because the question says limit to 5 instances, not at max 5 instances

upvoted 1 times

✉  **kchp** 5 months, 2 weeks ago

but seems no min\_latency\_instance for basic scaling

[https://cloud.google.com/appengine/docs/standard/reference/app-yaml?tab=python#basic\\_scaling](https://cloud.google.com/appengine/docs/standard/reference/app-yaml?tab=python#basic_scaling)

upvoted 1 times

✉  **kchp** 5 months, 2 weeks ago

sorry, no option min\_pending\_latency for basic scaling i mean

upvoted 1 times

✉  **[Removed]** 1 year, 11 months ago

**Selected Answer: D**

Option D - Max of 5

upvoted 2 times

✉  **ParagSanyashiv** 2 years, 3 months ago

**Selected Answer: D**

D is the correct answer

upvoted 1 times

 **syu31svc** 2 years, 9 months ago

<https://cloud.google.com/appengine/docs/standard/python/how-instances-are-managed>:

"A service with basic scaling is configured by setting the maximum number of instances in the max\_instances parameter of the basic\_scaling setting. The number of live instances scales with the processing volume."

Answer is D

upvoted 3 times

 **StelSen** 3 years, 2 months ago

Option: D is correct. Link: <https://cloud.google.com/appengine/docs/standard/python/how-instances-are-managed>

upvoted 2 times

 **Dinit** 3 years, 2 months ago

Ya Answer is D

[https://cloud.google.com/appengine/docs/standard/python/config/appref#scaling\\_elements](https://cloud.google.com/appengine/docs/standard/python/config/appref#scaling_elements)

upvoted 1 times

 **saurabh1805** 3 years, 5 months ago

D is correct answer here.

upvoted 4 times

Question #65

Topic 1

Your analytics system executes queries against a BigQuery dataset. The SQL query is executed in batch and passes the contents of a SQL file to the BigQuery

CLI. Then it redirects the BigQuery CLI output to another process. However, you are getting a permission error from the BigQuery CLI when the queries are executed.

You want to resolve the issue. What should you do?

- A. Grant the service account BigQuery Data Viewer and BigQuery Job User roles.
- B. Grant the service account BigQuery Data Editor and BigQuery Data Viewer roles.
- C. Create a view in BigQuery from the SQL query and SELECT\* from the view in the CLI.
- D. Create a new dataset in BigQuery, and copy the source table to the new dataset Query the new dataset and table from the CLI.

**Correct Answer: B**

*Community vote distribution*

A (100%)

 **donchick** Highly Voted  3 years, 4 months ago

I think A is the correct one.

upvoted 14 times

 **santoshchauhan** Most Recent  1 month, 3 weeks ago

**Selected Answer: A**

A. Grant the service account BigQuery Data Viewer and BigQuery Job User roles.

The permission error from the BigQuery CLI suggests that the service account used to execute the queries does not have the necessary permissions. To resolve this, you need to ensure that the service account has the appropriate roles:

**BigQuery Data Viewer role:** This role allows the service account to read data from BigQuery tables and views. It's necessary for the service account to access and read the dataset against which the queries are being executed.

**BigQuery Job User role:** This role allows the service account to create and run jobs in BigQuery, including query jobs, which is necessary for executing SQL queries.

upvoted 1 times

 **theseawillclaim** 2 months, 2 weeks ago

**Selected Answer: A**

A is the one. No need to edit data is specified.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: A**

A is correct.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

The correct answer is Option A. In order to allow the analytics system to execute queries against the BigQuery dataset, the service account must be granted the BigQuery Data Viewer and BigQuery Job User roles. The BigQuery Data Viewer role allows the service account to read data from tables, and the BigQuery Job User role allows the service account to run jobs, which includes executing queries. Option B is not a good solution because the BigQuery Data Editor role allows the service account to modify data in tables, which is not necessary to execute queries. Option C is not a good solution because creating a view in BigQuery and selecting from the view in the CLI will not resolve the permission issue. Option D is not a good solution because creating a new dataset and copying the source table to the new dataset will not resolve the permission issue.

upvoted 3 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: A**

A is correct

upvoted 3 times

 **maxdanny** 1 year, 9 months ago

**Selected Answer: A**

A it's correct for the principle of least privilege

upvoted 1 times

 **ParagSanyashiv** 2 years, 3 months ago

**Selected Answer: A**

According to the best practice - "User should have least privilege i.e. only those permissions which are required to perform an operation" - Option A is Correct

Question #66

Topic 1

Your application is running on Compute Engine and is showing sustained failures for a small number of requests. You have narrowed the cause down to a single

Compute Engine instance, but the instance is unresponsive to SSH.

What should you do next?

- A. Reboot the machine.
- B. Enable and check the serial port output.
- C. Delete the machine and create a new one.

D. Take a snapshot of the disk and attach it to a new machine.

**Correct Answer: A**

*Community vote distribution*

B (100%)

 **donchick** Highly Voted 3 years, 4 months ago

Difficult to choose because either B([https://cloud.google.com/compute/docs/troubleshooting/troubleshooting-ssh#debug\\_with\\_serial\\_console](https://cloud.google.com/compute/docs/troubleshooting/troubleshooting-ssh#debug_with_serial_console)) or D([https://cloud.google.com/compute/docs/troubleshooting/troubleshooting-ssh#inspect\\_vm](https://cloud.google.com/compute/docs/troubleshooting/troubleshooting-ssh#inspect_vm)) is recommended by google. I'd stay with B.

upvoted 5 times

 **mastodilu** 2 years, 11 months ago

Using the first link you provided: [https://cloud.google.com/compute/docs/troubleshooting/troubleshooting-ssh#debug\\_with\\_serial\\_console](https://cloud.google.com/compute/docs/troubleshooting/troubleshooting-ssh#debug_with_serial_console)

We recommend that you review the logs from the serial console for connection errors. You can access the serial console from your local workstation by using a browser.

Enable read/write access to an instance's serial console, so you can log into the console and troubleshoot problems with the instance. This approach is useful when you cannot log in with SSH, or if the instance has no connection to the network. The serial console remains accessible in both of these situations

upvoted 4 times

 **santoshchauhan** Most Recent 1 month, 3 weeks ago

**Selected Answer: B**

B. Enable and check the serial port output.

When a Compute Engine instance becomes unresponsive to SSH, one of the best ways to diagnose the issue is to check the serial port output. The serial console can provide valuable information about the state of the instance and any errors that may be occurring at the system level. It is particularly useful when you can't connect via SSH. Google Cloud allows you to enable interactive access to the serial console, which can be a crucial tool for troubleshooting.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: B**

B is correct.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Option B is correct. According to Google Cloud documentation, if a Compute Engine instance is unresponsive to SSH and you have narrowed the cause down to a single instance, you should enable and check the serial port output. The serial port output is a log of system messages and can help you diagnose the issue causing the instance to become unresponsive. To enable and check the serial port output, you can access the serial console as the root user from your local workstation using a browser. This will allow you to review the logs and potentially identify the cause of the problem.

upvoted 4 times

 **omermahgoub** 1 year, 3 months ago

Option A is not a good solution because rebooting the machine may not resolve the issue that is causing the instance to become unresponsive.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Option C is not a good solution because deleting the machine and creating a new one will not resolve the issue that caused the original instance to become unresponsive.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Option D is not a good solution because taking a snapshot of the disk and attaching it to a new machine will not resolve the issue that caused the original instance to become unresponsive.

upvoted 2 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: B**

B is correct

upvoted 2 times

 **ParagSanyashiv** 2 years, 3 months ago

**Selected Answer: B**

B is correct, because it will be the first step to check the serial port 22 is responsive or not.  
upvoted 2 times

 **syu31svc** 2 years, 9 months ago

I would take B as the answer

"What should you do next?"

SSH is port 22 so it makes sense to check for the port

upvoted 3 times

 **StelSen** 3 years, 2 months ago

Option-B is most suitable: In a real world I will try this and even if doesn't work then I will try Option-D which will help me to troubleshoot in details.

upvoted 4 times

Question #67

*Topic 1*

You configured your Compute Engine instance group to scale automatically according to overall CPU usage. However, your application's response latency increases sharply before the cluster has finished adding up instances. You want to provide a more consistent latency experience for your end users by changing the configuration of the instance group autoscaler.

Which two configuration changes should you make? (Choose two.)

- A. Add the label `AUTOSCALE` to the instance group template.
- B. Decrease the cool-down period for instances added to the group.
- C. Increase the target CPU usage for the instance group autoscaler.
- D. Decrease the target CPU usage for the instance group autoscaler.
- E. Remove the health-check for individual VMs in the instance group.

**Correct Answer: AC**

*Community vote distribution*

BD (100%)

 **donchick** Highly Voted 3 years, 4 months ago

I'd choose B and D.

upvoted 16 times

 **fraloca** 3 years, 4 months ago

For me the answer is B and D.

"A cool down period value that is significantly longer causing a delay in scaling out".

[https://cloud.google.com/compute/docs/autoscaler#cool\\_down\\_period](https://cloud.google.com/compute/docs/autoscaler#cool_down_period)

[https://cloud.google.com/compute/docs/autoscaler/scaling-cpu#scaling\\_based\\_on\\_cpu\\_utilization](https://cloud.google.com/compute/docs/autoscaler/scaling-cpu#scaling_based_on_cpu_utilization)

upvoted 5 times

 **santoshchauhan** Most Recent 1 month, 3 weeks ago

**Selected Answer: BD**

B. Decrease the cool-down period for instances added to the group: The cool-down period is the time the autoscaler waits after a new instance is healthy before it collects usage metrics from the instance. A shorter cool-down period allows the autoscaler to react more quickly to changes in load, potentially starting to scale up sooner when there is a sudden increase in traffic.

D. Decrease the target CPU usage for the instance group autoscaler: Lowering the target CPU utilization means that the autoscaler will start adding instances sooner as the CPU usage approaches the lower target. This can help to alleviate the issue where response latency increases sharply because new instances are added before the CPU usage hits a higher threshold.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: BD**

B and D are the best option here.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Options B and D are correct. To provide a more consistent latency experience for your end users, you should make the following configuration changes:

Option B: Decrease the cool-down period for instances added to the group. The cool-down period is the time that must pass before the instance group autoscaler can add more instances after it has already added instances to the group. Decreasing the cool-down period can allow the instance group to scale more quickly in response to changes in CPU usage, which may help to reduce latency.

Option D: Decrease the target CPU usage for the instance group autoscaler. The target CPU usage is the average CPU usage that the instance group autoscaler aims to maintain for the group. Decreasing the target CPU usage may allow the instance group to scale down more quickly in response to changes in CPU usage, which may also help to reduce latency.

upvoted 4 times

 **omermahgoub** 1 year, 3 months ago

Option E is not a correct solution because removing the health-check for individual VMs in the instance group may not improve latency and could potentially cause other issues with the instance group.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Option C is not a correct solution because increasing the target CPU usage for the instance group autoscaler will not help to reduce latency.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Option A is not a correct solution because adding the label "AUTOSCALE" to the instance group template will not affect the configuration of the instance group autoscaler.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: BD**

BD are correct

upvoted 3 times

 **GCPCloudArchitectUser** 2 years, 2 months ago

**Selected Answer: BD**

I would choose these two

upvoted 3 times

 **syu31svc** 2 years, 9 months ago

Adding label won't solve the issue so A is wrong for sure

Removing health check is not recommended so E is wrong as well

Increase CPU target is wrong since scaling will take place at a higher usage which is not what we want

B and D are the correct options

upvoted 4 times

👤 whigy 3 years, 5 months ago

D is more correct than C. If C, the auto-scale up will be further delayed  
upvoted 2 times

Question #68

Topic 1

You have an application controlled by a managed instance group. When you deploy a new version of the application, costs should be minimized and the number of instances should not increase. You want to ensure that, when each new instance is created, the deployment only continues if the new instance is healthy.

What should you do?

- A. Perform a rolling-action with maxSurge set to 1, maxUnavailable set to 0.
- B. Perform a rolling-action with maxSurge set to 0, maxUnavailable set to 1
- C. Perform a rolling-action with maxHealthy set to 1, maxUnhealthy set to 0.
- D. Perform a rolling-action with maxHealthy set to 0, maxUnhealthy set to 1.

**Correct Answer: A**

Reference:

<https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups>

*Community vote distribution*

B (63%)

A (38%)

👤 donchick Highly Voted 3 years, 4 months ago

B(maxSurge = 0, maxUnavailable = 1)  
upvoted 22 times

👤 Ayuewinc 3 years ago

"costs should be minimized and the number of instances should not increase", maxSurge = 1 will increase the number of instances, so B would be the correct answer  
upvoted 4 times

👤 syu31svc Highly Voted 2 years, 9 months ago

"number of instances should not increase"

B would be correct  
upvoted 5 times

👤 santoshchauhan Most Recent 1 month, 3 weeks ago

**Selected Answer: A**

Here's the reasoning:

maxSurge: This parameter determines the number of additional instances that can be created above the target size of the instance group during the update. Setting maxSurge to 1 allows the instance group to create one extra instance beyond its target size. This extra instance is used to start a new version of your application, ensuring that there's always a running instance during the update process.

maxUnavailable: This parameter specifies the number of instances that can be unavailable at any time during the update. Setting maxUnavailable to 0 ensures that there is no reduction in the number of available instances below the target size during the update process.

upvoted 2 times

👤 Aeglas 5 months ago

**Selected Answer: B**

maxSurge controls in a rolling update how many resources can be added above threshold of the MIG (managed instance group), while maxUnavailable controls the max number of instances that can be taken offline during update at the same time

upvoted 2 times

👤 Kadhem 5 months, 3 weeks ago

**Selected Answer: A**

the correct answer is A i think

If you do not want any unavailable machines during an update, set the maxUnavailable value to 0 and the maxSurge value to greater than 0. With these settings, Compute Engine removes each old machine only after its replacement new machine is created and running.

[https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups#max\\_surge](https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups#max_surge)

upvoted 1 times

👤 \_\_rajan\_\_ 7 months, 1 week ago

**Selected Answer: A**

Option A is best suited here as if we go with option B it does not ensure that deployment only continues if the new instance is healthy.

upvoted 1 times

👤 Teraflow 1 year, 1 month ago

**Selected Answer: A**

The correct answer is A.

Performing a rolling update with maxSurge set to 1 and maxUnavailable set to 0 ensures that the deployment only continues if the new instance is healthy. The maxSurge parameter ensures that only one new instance is created at a time, while the maxUnavailable parameter ensures that the number of healthy instances does not decrease during the deployment. This will minimize costs by not creating unnecessary instances and will also ensure that the deployment is safe and does not impact the application's availability.

Option B is incorrect because setting maxUnavailable to 1 would mean that one instance will be taken offline at a time, which could impact the application's availability during the deployment.

Options C and D are incorrect because maxHealthy and maxUnhealthy are not valid parameters for a rolling update.

upvoted 1 times

👤 closer89 11 months, 3 weeks ago

"costs should be minimized and the number of instances should not increase"

its B

with maxUnavailable=1, maxSurge=0 - your instance group will be decreased by 1 which is not prohibited

upvoted 1 times

👤 Foxal 1 year, 2 months ago

**Selected Answer: A**

the correct answers is A

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

the correct answer would be A. Perform a rolling-action with maxSurge set to 1, maxUnavailable set to 0. This will minimize costs by only creating one new instance at a time, and will only continue the deployment if the new instance is healthy, ensuring a consistent latency experience for end users.

[https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups#max\\_surge](https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups#max_surge)

upvoted 2 times

 **omermahgoub** 1 year, 3 months ago

Option B is not a correct solution because setting maxSurge to 0 and maxUnavailable to 1 will not allow the deployment to continue if the instance is not healthy. Option C is not a correct solution because maxHealthy and maxUnhealthy are not valid options for rolling-actions. Option D is not a correct solution because setting maxHealthy to 0 and maxUnhealthy to 1 will not allow the deployment to continue if the new instance is not healthy.

upvoted 1 times

 **tab02733** 1 year, 6 months ago

**Selected Answer: B**

This is the best site here.

<https://tech-lab.sios.jp/archives/18553>

The site is in Japanese, so please translate and read it.

upvoted 2 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: B**

B is correct

upvoted 2 times

 **cloud\_enth0325** 1 year, 11 months ago

**Selected Answer: B**

maxSurge specifies the maximum number (or percentage) of pods above the specified number of replicas (is the maximum number of new pc that will be created at a time) and maxUnavailable is the maximum number of old pods that will be deleted at a time.

maxSurge = 0 would mean no extra pods with be created.

upvoted 1 times

 **yogi\_508** 2 years ago

i'll go with A( number of instances should not increase--- for this number shouldn't increase than target size i think, it doesn't mean no new instances should be created,

they are asking in question, like when new instance is being created, so surge >0,)

[https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups#max\\_unavailable](https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups#max_unavailable)

If you do not want any unavailable machines during an update, set the maxUnavailable value to 0 and the maxSurge value to greater than 0. V these settings, Compute Engine removes each old machine only after its replacement new machine is created and running.

upvoted 2 times

 **morenocasado** 2 years ago

**Selected Answer: B**

As others suggested, B is the correct option.

I am adding this to highlight the community choice.

upvoted 2 times

✉️ **GCPCloudArchitectUser** 2 years, 2 months ago

Selected Answer: B

Yes it should be B as question states deployment should stop if it is unhealthy... the only we can happen is to make it to 0 for maxSurge =1 upvoted 1 times

✉️ **GCPCloudArchitectUser** 2 years, 2 months ago

I am confused here ... it's either A or B

upvoted 1 times

✉️ **GCPCloudArchitectUser** 2 years, 2 months ago

Ok thanks for link reference

Excerpt

upvoted 1 times

✉️ **GCPCloudArchitectUser** 2 years, 2 months ago

Note: If you set both maxSurge and maxUnavailable properties and both properties resolve to 0, the Updater automatically sets maxUnavailable=1, to ensure that the automated update can always proceed.

upvoted 1 times

✉️ **GCPCloudArchitectUser** 2 years, 2 months ago

That will be B

upvoted 1 times

✉️ **celia20200410** 2 years, 9 months ago

ANS: A

Note: If you set both maxSurge and maxUnavailable properties and both properties resolve to 0, the Updater automatically sets maxUnavailable=1, to ensure that the automated update can always proceed.

[https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups#max\\_surge](https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups#max_surge)

Setting a higher maxSurge value speeds up your update, at the cost of additional instances, which are billed according to the Compute Engine price sheet.

upvoted 2 times

✉️ **celia20200410** 2 years, 9 months ago

ans: a

[https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups#max\\_unavailable](https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups#max_unavailable)

If you do not want any unavailable machines during an update, set the maxUnavailable value to 0 and the maxSurge value to greater than 0. With these settings, Compute Engine removes each old machine only after its replacement new machine is created and running.

upvoted 1 times

Question #69

Topic 1

Your application requires service accounts to be authenticated to GCP products via credentials stored on its host Compute Engine virtual machine instances. You want to distribute these credentials to the host instances as securely as possible.

What should you do?

- A. Use HTTP signed URLs to securely provide access to the required resources.
- B. Use the instance's service account Application Default Credentials to authenticate to the required resources.
- C. Generate a P12 file from the GCP Console after the instance is deployed, and copy the credentials to the host instance before starting the application.

D. Commit the credential JSON file into your application's source repository, and have your CI/CD process package it with the software that is deployed to the instance.

**Correct Answer: B**

Reference:

<https://cloud.google.com/compute/docs/api/how-tos/authorization>

*Community vote distribution*

B (71%)

14%

14%

 **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: B**

Option B is Correct: This approach ensures that the credentials are securely managed and automatically provided to the instances when needed.  
upvoted 1 times

 **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: A**

This approach ensures that the credentials are securely managed and automatically provided to the instances when needed.  
upvoted 1 times

 **telp** 1 year, 3 months ago

**Selected Answer: B**

Answer B because best practice is to not store file with account service information when possible. With compute engine, the account service the vm can be used to call google api if the roles are added to this account service.  
upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

B. Use the instance's service account Application Default Credentials to authenticate to the required resources.

Using the instance's service account Application Default Credentials is the most secure method for distributing credentials to the host instances. This method allows the instance to automatically authenticate with the required resources using the instance's built-in service account, without requiring the credentials to be stored on the instance or transmitted over the network. This eliminates the risk of the credentials being compromised or exposed. Additionally, this method is the most convenient, as it requires no manual steps to set up the credentials on the instance.  
upvoted 3 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: B**

I think B is correct  
upvoted 2 times

 **cloud\_enth0325** 1 year, 11 months ago

**Selected Answer: B**

I'm also considering this part -- "distribute these credentials to the host instances as securely as possible"

This falls under B.  
upvoted 1 times

 **GoReplyGCPExam** 1 year, 11 months ago

**Selected Answer: C**

Your application requires service accounts to be authenticated to GCP products via credentials stored on its host Compute Engine virtual machine instances.

The application requires the credentials to be stored on the VM instance, so I think the application code points to a file stored in the Instance.  
upvoted 1 times

 **worheck93** 2 years, 7 months ago

Answer is B

<https://cloud.google.com/docs/authentication/production#automatically>

If the environment variable GOOGLE\_APPLICATION\_CREDENTIALS isn't set, ADC uses the service account that is attached to the resource that is running your code.

upvoted 4 times

✉️  **syu31svc** 2 years, 9 months ago

"authenticated to GCP" is the key part of the qn

<https://cloud.google.com/iam/docs/creating-managing-service-account-keys>:

"To use a service account from outside of Google Cloud, such as on other platforms or on-premises, you must first establish the identity of the service account"

"You can create service account keys in JSON or PKCS#12 (P12) format. "

C is the answer

upvoted 2 times

✉️  **syu31svc** 2 years, 9 months ago

<https://cloud.google.com/compute/docs/api/how-tos/authorization>:

"If you run applications on your Compute Engine instances, application default credentials can get credentials through built-in service accounts"

Answer is B not C

upvoted 4 times

✉️  **ralf\_cc** 2 years, 10 months ago

Only C sounds right

upvoted 1 times

Question #70

*Topic 1*

Your application is deployed in a Google Kubernetes Engine (GKE) cluster. You want to expose this application publicly behind a Cloud Load Balancing HTTP(S) load balancer.

What should you do?

- A. Configure a GKE Ingress resource.
- B. Configure a GKE Service resource.
- C. Configure a GKE Ingress resource with type: LoadBalancer.
- D. Configure a GKE Service resource with type: LoadBalancer.

**Correct Answer: A**

Reference:

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

*Community vote distribution*

A (60%)

D (40%)

✉️  **donchick** Highly Voted 3 years, 4 months ago

A(<https://cloud.google.com/kubernetes-engine/docs/tutorials/http-balancer>)

upvoted 7 times

✉  **mastodilu** 2 years, 11 months ago

an ingress works if you already have a service, like an https load balancer or a NodePort.

upvoted 1 times

✉  **GoReplyGCPExam** 1 year, 11 months ago

For me the right answer is D.

The Ingress Object create a global http(s) L.B. The advantage of having a layer 7 load balancer is that we can configure advanced things at network layer 7. For example to route traffic based on the path of the request and so on. In the question it seems that is not needed, so for a Load Balancer Service is ok since it creates a network load balancer (TCP/UDP) that is ok for HTTP or HTTPS exposing (since we can configure any TCP/UDP port to be exposed to The Internet)

upvoted 2 times

✉  **Valant**  2 years, 5 months ago

A)

The important part of the question is this "...expose this application publicly behind a Cloud Load Balancing HTTP(S) load balancer." This means it is an L7 exposure using HTTPS (a Service of type "LoadBalancer" would only create an L4 exposure - IP only... No HTTPS).

So Ingress is the choice you should make. And in GKE, luckily this is one thing - create an ingress and the LB will be attached automatically ; upvoted 5 times

✉  **\_rajan\_**  7 months, 1 week ago

**Selected Answer: A**

To expose your application publicly behind a Cloud Load Balancing HTTP(S) load balancer in a Google Kubernetes Engine (GKE) cluster, we should configure a GKE Ingress resource. This approach allows you to define rules for routing external HTTP(S) traffic to internal services based on hostnames and URL paths.

upvoted 3 times

✉  **[Removed]** 1 year, 2 months ago

**Selected Answer: D**

The correct answer is D

Configuring a GKE ingress resource is not enough, you also need to expose the service with the type NodePort and then configure the ingress resource to point to that service.

D is sufficient, then D is the correct answer. A lacks some more work.

upvoted 4 times

✉  **omermahgoub** 1 year, 3 months ago

To expose your application publicly behind a Cloud Load Balancing HTTP(S) load balancer in a GKE cluster, you should configure a GKE Ingress resource or a GKE Service resource with type: LoadBalancer.

To configure a GKE Ingress resource, you need to define rules for routing HTTP(S) traffic to the application in the cluster. This is done by creating an Ingress object, which is associated with one or more Service objects, each of which is associated with a set of Pods. The GKE Ingress controller will then create a Google Cloud HTTP(S) Load Balancer and configure it according to the information in the Ingress and its associated Services.

Alternatively, you can configure a GKE Service resource with type: LoadBalancer to expose your application publicly. This will create a Cloud Load Balancing HTTP(S) load balancer and associate it with the Service. The Service will then route traffic to the application Pods.

upvoted 2 times

✉  **tomato123** 1 year, 8 months ago

**Selected Answer: A**

A is correct

upvoted 2 times

✉  **nehaxlpb** 1 year, 9 months ago

**Selected Answer: A**

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

GKE Ingress for HTTP(S) Load Balancing

This page provides a general overview of what Ingress for HTTP(S) Load Balancing is and how it works. Google Kubernetes Engine (GKE) provides a built-in and managed Ingress controller called GKE Ingress. This controller implements Ingress resources as Google Cloud load balancers for HTTP(S) workloads in GKE.

upvoted 1 times

✉️  **ruben82** 1 year, 11 months ago

I think it's D.

They need a Load Balancer too.

Ingress just permits to expose a cluster, then A answer is not complete according to requirement.

upvoted 2 times

✉️  **ruben82** 1 year, 11 months ago

It's A... 'Cos Kind: Ingress create automatically a LB HTTP(S)

upvoted 1 times

✉️  **lxs** 1 year, 3 months ago

kind Service in GKE creates TCP/IP LB. If you want to leverage HTTP(s) you need to create Ingress class.

upvoted 1 times

✉️  **[Removed]** 2 years, 9 months ago

(D) is not correct as service with type LoadBalancer create network load balancer not http load balancer.

(A) is correct ingress will create http balancer without the need of specify type

<https://cloud.google.com/kubernetes-engine/docs/concepts/ingress#overview>

upvoted 4 times

✉️  **syu31svc** 2 years, 9 months ago

<https://cloud.google.com/kubernetes-engine/docs/tutorials/http-balancer>:

"When you specify kind: Service with type: LoadBalancer in the resource manifest, GKE creates a Service of type LoadBalancer"

D is correct

upvoted 2 times

✉️  **syu31svc** 2 years, 9 months ago

Changing my answer to A

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

"In GKE, an Ingress object defines rules for routing HTTP(S) traffic to applications running in a cluster. An Ingress object is associated with one or more Service objects, each of which is associated with a set of Pods. To learn more about how Ingress exposes applications using Services, see Service networking overview."

When you create an Ingress object, the GKE Ingress controller creates a Google Cloud HTTP(S) Load Balancer and configures it according to the information in the Ingress and its associated Services."

upvoted 5 times

✉️  **mastodilu** 2 years, 11 months ago

answer is D

upvoted 3 times

Question #71

Topic 1

Your company is planning to migrate their on-premises Hadoop environment to the cloud. Increasing storage cost and maintenance of data stored in HDFS is a major concern for your company. You also want to make minimal changes to existing data analytics jobs and existing architecture. How should you proceed with the migration?

- A. Migrate your data stored in Hadoop to BigQuery. Change your jobs to source their information from BigQuery instead of the on-premises Hadoop environment.
- B. Create Compute Engine instances with HDD instead of SSD to save costs. Then perform a full migration of your existing environment into the new one in Compute Engine instances.
- C. Create a Cloud Dataproc cluster on Google Cloud Platform, and then migrate your Hadoop environment to the new Cloud Dataproc cluster. Move your HDFS data into larger HDD disks to save on storage costs.
- D. Create a Cloud Dataproc cluster on Google Cloud Platform, and then migrate your Hadoop code objects to the new cluster. Move your data to Cloud Storage and leverage the Cloud Dataproc connector to run jobs on that data.

**Correct Answer: D**

*Community vote distribution*

D (100%)

 **donchick** Highly Voted 3 years, 4 months ago

I'd choose D.

upvoted 7 times

 **syu31svc** Highly Voted 2 years, 9 months ago

<https://cloud.google.com/architecture/hadoop/hadoop-gcp-migration-overview>:

"Keeping your data in a persistent HDFS cluster using Dataproc is more expensive than storing your data in Cloud Storage, which is what we recommend, as explained later. Keeping data in an HDFS cluster also limits your ability to use your data with other Google Cloud products." "Google Cloud includes Dataproc, which is a managed Hadoop and Spark environment. You can use Dataproc to run most of your existing jobs with minimal alteration, so you don't need to move away from all of the Hadoop tools you already know"

D is the answer

upvoted 6 times

 **\_rajan\_** Most Recent 7 months, 1 week ago

**Selected Answer: D**

Option D is correct.

upvoted 1 times

 **tranvanchau9494** 8 months ago

D is correct

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Option D is the most appropriate choice because it allows you to migrate your Hadoop code objects to a Cloud Dataproc cluster, which is a fully managed Apache Hadoop and Apache Spark service on Google Cloud. This will allow you to make minimal changes to your existing data analytics jobs and existing architecture. Additionally, moving your data to Cloud Storage and using the Cloud Dataproc connector to run jobs on that data will allow you to take advantage of the scalability, durability, and security of Cloud Storage while also minimizing storage costs.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

A would involve a significant change to your existing data analytics jobs and architecture, as it would involve migrating your data to BigQuery and changing your jobs to source their information from BigQuery instead of Hadoop.

B is not a feasible option because Compute Engine instances do not have the capability to run HDFS.

C would not allow you to save on storage costs as it involves moving your data to larger HDD disks rather than a more cost-effective storage solution like Cloud Storage.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: D**

D is correct

upvoted 2 times

 **tomato123** 1 year, 8 months ago

D is correct

upvoted 1 times

 **szl0144** 1 year, 11 months ago

D is correct

upvoted 1 times

Your data is stored in Cloud Storage buckets. Fellow developers have reported that data downloaded from Cloud Storage is resulting in slow API performance.

You want to research the issue to provide details to the GCP support team.

Which command should you run?

- A. gsutil test -o output.json gs://my-bucket
- B. gsutil perfdiag -o output.json gs://my-bucket
- C. gcloud compute scp example-instance:~/test-data -o output.json gs://my-bucket
- D. gcloud services test -o output.json gs://my-bucket

**Correct Answer: B**

Reference:

<https://groups.google.com/forum/#topic/gce-discussion/xBl9Jq5HDsY>

*Community vote distribution*

B (100%)

✉  **donchick** Highly Voted 3 years, 4 months ago

B(<https://cloud.google.com/storage/docs/gsutil/commands/perfdiag#providing-diagnostic-output-to-cloud-storage-team>)  
upvoted 13 times

✉  **syu31svc** 2 years, 9 months ago

Spot-on link and answer  
upvoted 1 times

✉  **\_rajan\_** Most Recent 7 months, 1 week ago

**Selected Answer: B**

To research the issue of slow API performance when downloading data from Cloud Storage, you can use the gsutil perfdiag command. This command runs a set of tests to report the actual performance of a Cloud Storage bucket and provides detailed information on the performance of individual operations.

upvoted 1 times

✉  **omermahgoub** 1 year, 3 months ago

B. gsutil perfdiag -o output.json gs://my-bucket

The gsutil perfdiag command is used to diagnose performance issues with Cloud Storage. It can be used to perform various tests such as download, upload, and metadata operations. By using the -o flag, you can specify an output file where the results of the tests will be stored in JSON format. This output file can then be provided to the GCP support team to help them investigate the issue.

upvoted 2 times

✉  **ynaitam** 1 year, 4 months ago

CORRECT

upvoted 1 times

✉  **tomato123** 1 year, 8 months ago

**Selected Answer: B**

B is correct

upvoted 2 times

You are using Cloud Build build to promote a Docker image to Development, Test, and Production environments. You need to ensure that the same Docker image is deployed to each of these environments.

How should you identify the Docker image in your build?

- A. Use the latest Docker image tag.
- B. Use a unique Docker image name.
- C. Use the digest of the Docker image.
- D. Use a semantic version Docker image tag.

**Correct Answer: D**

*Community vote distribution*

C (82%)

D (18%)

 **LCL8338** Highly Voted 2 years, 10 months ago

C, since digests are immutable, whilst docker tags are mutable (hence not D).

<https://cloud.google.com/architecture/using-container-images>

upvoted 19 times

 **dxxdd7** Highly Voted 3 years, 3 months ago

For me it's D, it's not a best practice to use image with the latest tag. And using the semantic version will ensure that all the environment use exact same image with the wanted code.

upvoted 9 times

 **StelSen** 3 years, 2 months ago

This is correct

upvoted 3 times

 **lxs** 1 year, 3 months ago

You are not correct. The question is to ensure the images are the same not about docker image naming convention best practices. The only way to compare two images and say they are the same is digest hash. You can mistakenly tag two different images using the same semantic tag.

upvoted 3 times

 **santoshchauhan** Most Recent 1 month, 3 weeks ago

**Selected Answer: C**

C. Use the digest of the Docker image.

When promoting Docker images across different environments in a CI/CD pipeline, it's crucial to ensure that exactly the same image is deployed to each environment. The most reliable way to identify a Docker image is by using its digest.

Here's why using the digest is the best approach:

The digest is a SHA256 hash of the image's content and configuration, which uniquely identifies an image. If anything about the image changes, the digest changes. This means that if you deploy an image by its digest, you are guaranteed to deploy the exact same image in each environment.

Using the digest is more reliable than using tags like 'latest' or semantic versioning. Tags can be moved to point to different images, but digests are immutable. Once an image is pushed to a registry, its digest can never change.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: C**

I would go with C.

upvoted 1 times

 **Teraflow** 1 year, 1 month ago

**Selected Answer: C**

C. Use the digest of the Docker image.

Using the digest of the Docker image is the most reliable way to ensure that the exact same Docker image is deployed to each environment. A digest is a hash of the image content and metadata, which is unique to each image. This means that even if the image is tagged with different versions or names, the digest will remain the same as long as the content and metadata are identical.

On the other hand, using the latest Docker image tag or a semantic version tag may not guarantee that the exact same image is deployed to each environment. These tags are mutable and can be overwritten or updated, which could result in different images being deployed to different environments.

Using a unique Docker image name could work, but it may be more difficult to manage and track multiple images with different names, especially if there are many environments or frequent updates.

upvoted 2 times

 **telp** 1 year, 3 months ago

**Selected Answer: C**

Answer C because needs to be sure that the same image for the 3 envs. A tag version can be changed between the deployment of the env.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: C**

C. Use the digest of the Docker image.

The digest of the Docker image is a unique identifier for the specific version of the image. By using the digest, you can ensure that the same exact version of the image is deployed to each environment. Using the latest tag or a unique image name may not necessarily guarantee that same version is deployed, as these tags may change over time. Using a semantic version tag would only ensure that the same version is deployed if you follow a strict versioning policy and only update the image by incrementing the patch or minor version number.

upvoted 3 times

 **kisswd** 1 year, 4 months ago

**Selected Answer: C**

C is the answer

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: D**

D is correct

upvoted 2 times

 **szl0144** 1 year, 11 months ago

C is 100% correct

upvoted 3 times

 **KillerGoogle** 2 years, 2 months ago

Read the question, it asks to ensure that the 'same' Docker image is deployed to every environment, so to identify the docker image, we have to use digests

upvoted 4 times

 **nazonazonazo** 2 years, 2 months ago

C is correct.

another answers are not immutable.

upvoted 3 times

 **alex8081** 1 year, 8 months ago

"By design, the Git commit hash is immutable and references a specific version of your software"..  
<https://cloud.google.com/architecture/best-practices-for-building-containers>

upvoted 1 times

 **syu31svc** 2 years, 9 months ago

[https://cloud.google.com/architecture/best-practices-for-building-containers#tagging\\_using\\_semantic\\_versioning](https://cloud.google.com/architecture/best-practices-for-building-containers#tagging_using_semantic_versioning)

Answer is D

upvoted 3 times

 **Rupo7** 5 months ago

I vote for this. We are likely looking for the best-practice way to 'promote' an image through dev, test, and prod environments. It is normal to use a tag with standard naming convention to identify/select images to promote e.g. tag v1.0.0. Using the digest would work, but this is not

Question #74

*Topic 1*

Your company has created an application that uploads a report to a Cloud Storage bucket. When the report is uploaded to the bucket, you want to publish a message to a Cloud Pub/Sub topic. You want to implement a solution that will take a small amount of effort to implement.

What should you do?

- A. Configure the Cloud Storage bucket to trigger Cloud Pub/Sub notifications when objects are modified.
- B. Create an App Engine application to receive the file; when it is received, publish a message to the Cloud Pub/Sub topic.
- C. Create a Cloud Function that is triggered by the Cloud Storage bucket. In the Cloud Function, publish a message to the Cloud Pub/Sub topic.
- D. Create an application deployed in a Google Kubernetes Engine cluster to receive the file; when it is received, publish a message to the Cloud Pub/Sub topic.

**Correct Answer: C**

Reference:

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

*Community vote distribution*

A (100%)

 **donchick** Highly Voted 3 years, 4 months ago

Since one of the reqs is "You want to implement a solution that will take a small amount of effort to implement" I'd choose A because no code has to be written. However option C works great as well and is recommended by [https://cloud.google.com/storage/docs/pubsub-notifications#other\\_notification\\_options](https://cloud.google.com/storage/docs/pubsub-notifications#other_notification_options).

upvoted 16 times

 **closer89** 11 months, 3 weeks ago

you link says that you use cloud functions only when you don't want to publish message to pubsub

upvoted 1 times

 **santoshchauhan** Most Recent 1 month, 3 weeks ago

**Selected Answer: A**

A. Configure the Cloud Storage bucket to trigger Cloud Pub/Sub notifications when objects are modified.

This solution is straightforward and requires minimal effort to implement. Google Cloud Storage offers native support for publishing messages to Cloud Pub/Sub topics in response to changes in your bucket, like uploading a new file. By configuring Cloud Storage to automatically send a message to a Pub/Sub topic when a new report is uploaded, you can easily set up a real-time notification system without the need to write or maintain additional code.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: A**

A is correct.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

C. Create a Cloud Function that is triggered by the Cloud Storage bucket. In the Cloud Function, publish a message to the Cloud Pub/Sub topic. This would be the most straightforward and easiest solution to implement, as it only requires creating a Cloud Function and setting it up to be triggered by the Cloud Storage bucket. This solution would not require deploying any additional resources, such as App Engine or a Kubernetes cluster, and would not require any significant code changes to the application uploading the report.

upvoted 4 times

 **zevexWM** 1 year, 3 months ago

A does exactly the same just without Cloud Functions. Notifications triggered by a Cloud Storage event, work as a trigger for PubSub. No need for Cloud Functions.

upvoted 1 times

 **zevexWM** 1 year, 3 months ago

Changing to option C. Option A state "when objects are modified" which is not the request here.

upvoted 2 times

 **closer89** 11 months, 3 weeks ago

documentation says that you use cloud functions only when you don't want to publish message to pubsub.

but you need to publish message to pubsub - therefore answer is A

[https://cloud.google.com/storage/docs/pubsub-notifications#other\\_notification\\_options](https://cloud.google.com/storage/docs/pubsub-notifications#other_notification_options)

<https://cloud.google.com/storage/docs/pubsub-notifications#overview>

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: A**

I think A is correct

upvoted 3 times

 **cloud\_enth0325** 1 year, 11 months ago

A -- Least steps for the overall requirement.

Option C, the suggested, won't need to trigger pub/sub unless it requires heavyweight or many subsequent steps.

(<https://cloud.google.com/storage/docs/pubsub-notifications#:~:text=don%27t%20want%20to%20manage%20a%20Pub/Sub%20topic>)

upvoted 1 times

 **brewpike** 1 year, 11 months ago

Also, aren't cloud storage objects immutable you can't modify but version them.

upvoted 1 times

 **brewpike** 1 year, 11 months ago

A : <https://cloud.google.com/storage/docs/pubsub-notifications>

upvoted 1 times

 **mariorossi** 2 years, 3 months ago

A not is correct because trigger must to be only in insert and not modify. only C is possible

upvoted 2 times

 **ParagSanyashiv** 2 years, 3 months ago

**Selected Answer: A**

Answer A takes least effort to implement the solution

upvoted 3 times

 **StelSen** 3 years, 2 months ago

Option-A required least amount of effort to implement. <https://cloud.google.com/storage/docs/reporting-changes#enabling>

upvoted 4 times

 **syu31svc** 2 years, 9 months ago

Agree; just a one line code and you're done

upvoted 2 times

Which improvement should you suggest your teammate make?

```
public Entity creditAccount(long accountId, long
creditAmount) {
    Entity account = datastore.get
(keyFactory.newKey(accountId));
    account = Entity.builder(account).set(
        "balance", account.getLong("balance")
+ creditAmount).build()
    datastore.put(account);
    return account;
}
```

- A. Get the entity with an ancestor query.
- B. Get and put the entity in a transaction.
- C. Use a strongly consistent transactional database.
- D. Don't return the account entity from the function.

**Correct Answer: A**

*Community vote distribution*

B (100%)

 **santoshchauhan** 1 month, 3 weeks ago

**Selected Answer: B**

B. Get and put the entity in a transaction.

The code provided is updating an account balance in Cloud Datastore. To ensure data integrity and consistency, such an update should be done within a transaction to avoid issues with concurrent updates which could result in an incorrect balance if the account is accessed by multiple processes at the same time.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: B**

Put the entity in transaction

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

B. Get and put the entity in a transaction.

Question #76

Topic 1

Your company stores their source code in a Cloud Source Repositories repository. Your company wants to build and test their code on each source code commit to the repository and requires a solution that is managed and has minimal operations overhead.

Which method should they use?

- A. Use Cloud Build with a trigger configured for each source code commit.
- B. Use Jenkins deployed via the Google Cloud Platform Marketplace, configured to watch for source code commits.
- C. Use a Compute Engine virtual machine instance with an open source continuous integration tool, configured to watch for source code commits.
- D. Use a source code commit trigger to push a message to a Cloud Pub/Sub topic that triggers an App Engine service to build the source code.

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **syu31svc** Highly Voted  2 years, 9 months ago

<https://cloud.google.com/build/docs/automating-builds/create-manage-triggers#:~:text=A%20Cloud%20Build%20trigger%20automatically,changes%20that%20match%20certain%20criteria.>

A is the answer  
upvoted 6 times

 **omermahgoub** Most Recent  1 year, 3 months ago

A. Use Cloud Build with a trigger configured for each source code commit.

Cloud Build is a fully managed service for building, testing, and deploying software quickly. It integrates with Cloud Source Repositories and can be triggered by source code commits, which makes it an ideal solution for building and testing code on each commit. It requires minimal operations overhead as it is fully managed by Google Cloud.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: A**

A is correct

upvoted 3 times

Question #77

*Topic 1*

You are writing a Compute Engine hosted application in project A that needs to securely authenticate to a Cloud Pub/Sub topic in project B.

What should you do?

- A. Configure the instances with a service account owned by project B. Add the service account as a Cloud Pub/Sub publisher to project A.
- B. Configure the instances with a service account owned by project A. Add the service account as a publisher on the topic.
- C. Configure Application Default Credentials to use the private key of a service account owned by project B. Add the service account as a Cloud Pub/Sub publisher to project A.
- D. Configure Application Default Credentials to use the private key of a service account owned by project A. Add the service account as a publisher on the topic

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **donchick** Highly Voted  3 years, 4 months ago

I vote for B.

upvoted 13 times

 **\_rajan\_** Most Recent  7 months, 1 week ago

Selected Answer: B

I would go with B.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Option B is the correct answer because it involves creating a service account in project A and adding it as a publisher to the Cloud Pub/Sub topic in project B. This allows the Compute Engine instances in project A to authenticate to the Cloud Pub/Sub topic in project B using the service account's credentials. The other options do not involve creating a service account in project A or adding it as a publisher to the Cloud Pub/Sub topic in project B, so they are not valid solutions.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Option A is incorrect because it is not a secure way to authenticate to a Cloud Pub/Sub topic in project B. In this option, the instances in project A are using a service account owned by project B, but the service account is not added as a publisher on the topic. This means that the service account does not have the necessary permissions to publish messages to the topic.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Option D is incorrect because it does not authenticate to the Cloud Pub/Sub topic in project B. In this option, Application Default Credentials are being used to authenticate to the topic, but the private key of a service account owned by project A is being used. This service account does not have the necessary permissions to publish messages to the topic in project B.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Option C is incorrect because it does not properly authenticate to the Cloud Pub/Sub topic in project B. In this option, Application Default Credentials are being used to authenticate to the topic, but the private key of a service account owned by project B is being used. While the service account may have the necessary permissions to publish messages to the topic, using Application Default Credentials with a private key is not a secure way to authenticate to Cloud Pub/Sub.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

Selected Answer: B

B is correct

upvoted 2 times

 **JuanitoNN** 2 years, 4 months ago

why not D?

upvoted 3 times

 **akshaychavan7** 1 year, 8 months ago

Question #78

Topic 1

You are developing a corporate tool on Compute Engine for the finance department, which needs to authenticate users and verify that they are in the finance department. All company employees use G Suite.

What should you do?

- A. Enable Cloud Identity-Aware Proxy on the HTTP(s) load balancer and restrict access to a Google Group containing users in the finance department. Verify the provided JSON Web Token within the application.
- B. Enable Cloud Identity-Aware Proxy on the HTTP(s) load balancer and restrict access to a Google Group containing users in the finance department. Issue client-side certificates to everybody in the finance team and verify the certificates in the application.
- C. Configure Cloud Armor Security Policies to restrict access to only corporate IP address ranges. Verify the provided JSON Web Token within the application.
- D. Configure Cloud Armor Security Policies to restrict access to only corporate IP address ranges. Issue client side certificates to everybody in the finance team and verify the certificates in the application.

**Correct Answer: C***Community vote distribution*

A (100%)

**donchick** Highly Voted 3 years, 4 months ago

I'd say A(<https://cloud.google.com/endpoints/docs/openapi/authenticating-users-google-id>).

upvoted 17 times

**syu31svc** Highly Voted 2 years, 9 months ago

[https://cloud.google.com/armor/docs/security-policy-overview#:~:text=Google%20Cloud%20Armor%20security%20policies%20enable%20you%20to%20allow%20or,Private%20Cloud%20\(VP%20networks.](https://cloud.google.com/armor/docs/security-policy-overview#:~:text=Google%20Cloud%20Armor%20security%20policies%20enable%20you%20to%20allow%20or,Private%20Cloud%20(VP%20networks.)

"Google Cloud Armor security policies protect your application by providing Layer 7 filtering and by scrubbing incoming requests for common web attacks or other Layer 7 attributes to potentially block traffic before it reaches your load balanced backend services or backend buckets"

C and D are wrong.

<https://cloud.google.com/endpoints/docs/openapi/authenticating-users-google-id>:

"To authenticate a user, a client application must send a JSON Web Token (JWT) in the authorization header of the HTTP request to your back API"

A is correct

upvoted 5 times

**santoshchauhan** Most Recent 1 month, 3 weeks ago**Selected Answer: A**

A. Enable Cloud Identity-Aware Proxy (IAP) on the HTTP(s) load balancer and restrict access to a Google Group containing users in the finance department. Verify the provided JSON Web Token within the application.

Cloud IAP allows you to manage access to your web applications running on Compute Engine by verifying a user's identity and determining if that user should be allowed to access the application. You can integrate Cloud IAP with Google Groups to restrict access to specific groups within your G Suite domain, such as a group for the finance department. When a user authenticates via Cloud IAP, a JSON Web Token (JWT) is issued that can be used within your application to further verify the user's identity and departmental membership.

upvoted 1 times

**\_\_rajan\_\_** 7 months, 1 week ago**Selected Answer: A**

A is correct.

upvoted 1 times

**omermahgoub** 1 year, 3 months ago

Option A is the correct solution because it uses Cloud Identity-Aware Proxy (IAP) to authenticate and authorize users to access the application. IAP verifies the identity of users accessing the application through G Suite and checks if they are members of the specified Google Group. IAP also verifies the JSON Web Token (JWT) provided in the request to ensure that the request is legitimate.

upvoted 1 times

**omermahgoub** 1 year, 3 months ago

Option D is not a correct solution because it combines the use of Cloud Armor Security Policies and client-side certificates, but does not have a way to authenticate and authorize users. It also does not have a way to verify the legitimacy of the requests.

upvoted 1 times

**omermahgoub** 1 year, 3 months ago

Option C is not a correct solution because it uses Cloud Armor Security Policies to restrict access based on IP addresses, but does not have a way to authenticate and authorize users.

upvoted 1 times

**omermahgoub** 1 year, 3 months ago

Option B is not a correct solution because it does not use IAP to authenticate and authorize users. It only issues client-side certificates to users in the finance department, but does not have a way to verify that the user presenting the certificate is actually the owner of the certificate.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: A**

A is correct

upvoted 2 times

 **cloud\_enth0325** 1 year, 11 months ago

**Selected Answer: A**

A should be the answer -- IAP x G-Suite

upvoted 1 times

 **morenocasado** 2 years ago

**Selected Answer: A**

Community choice is A

upvoted 1 times

 **dishum** 2 years, 1 month ago

Ans is B

<https://cloud.google.com/iap/docs/tutorial-gce>

upvoted 1 times

 **dishum** 1 year, 11 months ago

Not B.

Answer is A

upvoted 1 times

 **worheck93** 2 years, 7 months ago

A

IAP and JWT

[https://cloud.google.com/iap/docs/signed-headers-howto#securing\\_iap\\_headers](https://cloud.google.com/iap/docs/signed-headers-howto#securing_iap_headers)

upvoted 3 times

Question #79

Topic 1

Your API backend is running on multiple cloud providers. You want to generate reports for the network latency of your API.

Which two steps should you take? (Choose two.)

- A. Use Zipkin collector to gather data.
- B. Use Fluentd agent to gather data.
- C. Use Stackdriver Trace to generate reports.
- D. Use Stackdriver Debugger to generate report.
- E. Use Stackdriver Profiler to generate report.

**Correct Answer: CE**

*Community vote distribution*

AC (90%)

10%

 **fraloca** Highly Voted 3 years, 4 months ago

for me the solution is A and C:

<https://cloud.google.com/trace/docs/zipkin>

upvoted 17 times

 **dxxdd7** Highly Voted 3 years, 3 months ago

AC as Zipkin is used for to gather data for latency issues and SD trace purpose is to enable us to have a better view on the application code latency

upvoted 6 times

👤 santoshchauhan [Most Recent] 1 month, 3 weeks ago

Selected Answer: AC

For generating reports on network latency for an API that is distributed across multiple cloud providers, you would typically need to gather data and then analyze it:

A. Use Zipkin collector to gather data: Zipkin is a distributed tracing system that helps gather timing data needed to troubleshoot latency problems in service architectures. You can use Zipkin collectors to gather trace data from your API backend regardless of where it's running. Trace data can provide insights into the latency of different service calls.

C. Use Stackdriver Trace to generate reports: Stackdriver Trace (part of Google Cloud's operations suite) allows you to analyze how requests propagate through your application and receive detailed latency reports for your API. If you are already using Stackdriver on Google Cloud, you can extend its usage to analyze trace data collected from other cloud providers as well.

upvoted 1 times

👤 maxdanny 8 months ago

Selected Answer: AC

solution is AC:

<https://cloud.google.com/trace/docs/zipkin>

upvoted 1 times

👤 Teraflow 1 year, 1 month ago

Selected Answer: AC

The two steps you should take to generate reports for the network latency of your API running on multiple cloud providers are:

A. Use Zipkin collector to gather data: Zipkin is a distributed tracing system that helps you gather data about the latency of requests made to your API. It allows you to trace requests as they flow through your system, and provides insight into the performance of your services. You can use Zipkin collectors to collect data from multiple cloud providers, and then generate reports to analyze the latency of your API.

C. Use Stackdriver Trace to generate reports: Stackdriver Trace is a distributed tracing system that helps you trace requests across multiple services and provides detailed performance data about your applications. It allows you to visualize and analyze the performance of your API and its dependencies. You can use Stackdriver Trace to generate reports about the network latency of your API running on multiple cloud providers.

Therefore, the correct options are A and C.

upvoted 2 times

👤 omermahgoub 1 year, 3 months ago

The correct answer would be: A. Use Zipkin collector to gather data and C. Use Stackdriver Trace to generate reports.

Using Zipkin collector will allow you to gather data from your instrumented application running on multiple cloud providers. Stackdriver Trace can then be used to generate reports based on this data.

Option B, using Fluentd agent, is not related to generating reports on network latency for an API.

Option D, using Stackdriver Debugger, is not related to generating reports on network latency for an API.

Option E, using Stackdriver Profiler, is not related to generating reports on network latency for an API.

upvoted 1 times

👤 miyakelp 1 year, 5 months ago

Selected Answer: AC

A/C

<https://cloud.google.com/trace/docs/zipkin>

upvoted 1 times

👤 tomato123 1 year, 8 months ago

Selected Answer: BD

BD are correct

upvoted 1 times

👤 nehaxlpb 1 year, 9 months ago

Selected Answer: AC

[https://cloud.google.com/trace/docs/zipkin#frequently\\_asked\\_questions](https://cloud.google.com/trace/docs/zipkin#frequently_asked_questions)

use a Zipkin server to receive traces from Zipkin clients and forward those traces to Cloud Trace for analysis.

upvoted 2 times

 **mariorossi** 2 years, 3 months ago  
CE. E for latency Cloud Profiler. For tracing can be use also zipkin but better tracing  
upvoted 1 times

 **ParagSanyashiv** 2 years, 3 months ago  
**Selected Answer: AC**  
A and C are correct solution.  
upvoted 2 times

 **celia20200410** 2 years, 9 months ago  
AC  
A: to support multiple cloud providers  
<https://cloud.google.com/trace>  
Zipkin tracers to submit data to Cloud Trace. Projects running on App Engine are automatically captured.  
  
C: to generate reports for the network latency  
[https://cloud.google.com/trace/docs/quickstart#analysis\\_reports\\_window](https://cloud.google.com/trace/docs/quickstart#analysis_reports_window)  
upvoted 4 times

 **syu31svc** 2 years, 9 months ago  
"latency" is the key word here so C is one of the answers; Stackdriver Trace  
  
<https://cloud.google.com/trace/docs/zipkin>:  
"receive traces from Zipkin clients and forward those traces to Cloud Trace for analysis."

A is the other answer  
upvoted 3 times

 **yuchun** 2 years, 10 months ago  
I think the answer is AC  
upvoted 1 times

 **shav789** 3 years ago  
for me it is C and E, as profiler is used for performance analysis  
upvoted 1 times

 **MickeyRourke** 3 years, 4 months ago  
I would go with BC  
upvoted 2 times

 **fraloca** 3 years, 4 months ago  
C is correct. But B is used for logging and not for monitoring.  
upvoted 1 times

Question #80

Topic 1

#### Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

#### Company Overview -

HipLocal is a community application designed to facilitate communication between people in close proximity. It is used for event planning and organizing sporting events, and for businesses to connect with their local communities. HipLocal launched recently in a few neighborhoods in Dallas and is rapidly growing into a global phenomenon. Its unique style of hyper-local community communication and business outreach is in demand around the world.

#### Executive Statement -

We are the number one local community app; it's time to take our local community services global. Our venture capital investors want to see rapid growth and the same great experience for new local and virtual communities that come online, whether their members are 10 or 10000 miles away from each other.

#### Solution Concept -

HipLocal wants to expand their existing service, with updated functionality, in new regions to better serve their global customers. They want to hire and train a new team to support these regions in their time zones. They will need to ensure that the application scales smoothly and provides clear uptime data.

#### Existing Technical Environment -

HipLocal's environment is a mix of on-premises hardware and infrastructure running in Google Cloud Platform. The HipLocal team understands their application well, but has limited experience in global scale applications. Their existing technical environment is as follows:

- \* Existing APIs run on Compute Engine virtual machine instances hosted in GCP.
- \* State is stored in a single instance MySQL database in GCP.
- \* Data is exported to an on-premises Teradata/Vertica data warehouse.
- \* Data analytics is performed in an on-premises Hadoop environment.
- \* The application has no logging.
- \* There are basic indicators of uptime; alerts are frequently fired when the APIs are unresponsive.

#### Business Requirements -

HipLocal's investors want to expand their footprint and support the increase in demand they are seeing. Their requirements are:

- \* Expand availability of the application to new regions.
- \* Increase the number of concurrent users that can be supported.
- \* Ensure a consistent experience for users when they travel to different regions.
- \* Obtain user activity metrics to better understand how to monetize their product.
- \* Ensure compliance with regulations in the new regions (for example, GDPR).
- \* Reduce infrastructure management time and cost.
- \* Adopt the Google-recommended practices for cloud computing.

#### Technical Requirements -

- \* The application and backend must provide usage metrics and monitoring.
- \* APIs require strong authentication and authorization.
- \* Logging must be increased, and data should be stored in a cloud analytics platform.
- \* Move to serverless architecture to facilitate elastic scaling.
- \* Provide authorized access to internal apps in a secure manner.

Which database should HipLocal use for storing user activity?

A. BigQuery

- B. Cloud SQL
- C. Cloud Spanner
- D. Cloud Datastore

**Correct Answer: C**

*Community vote distribution*

A (57%)

D (29%)

14%

 **fosky94** Highly Voted 3 years ago

In the case study is stated: "Obtain user activity metrics to better understand how to monetize their product", which means that they'll need to analyse the user activity, so... I'll go with answer A (BigQuery)

upvoted 13 times

 **syu31svc** 2 years, 9 months ago

Agree with you on this one

upvoted 3 times

 **santoshchauhan** Most Recent 1 month, 3 weeks ago

**Selected Answer: C**

Here's why Cloud Spanner is the best fit for HipLocal's needs:

**Global Scalability:** Cloud Spanner can scale horizontally to handle increased loads and number of concurrent users, which is aligned with the rapid growth that HipLocal is experiencing.

**Strong Consistency:** It provides strong consistency guarantees, ensuring that users have a consistent experience regardless of the region they're accessing the application from.

**High Availability:** Spanner's built-in replication across multiple regions makes it highly available, which helps to meet uptime requirements and ensure compliance with regulations like GDPR that may require data to be stored in certain regions.

**Managed Service:** As a fully managed service, it reduces the time and cost associated with infrastructure management, which meets the business requirement to minimize management overhead.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: D**

For Storing user data Datastore is best.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

I think A would be better fit for this. Please ignore the above answer.

upvoted 1 times

 **sbonesi** 11 months, 2 weeks ago

**Selected Answer: A**

A (BigQuery) is more appropriate for user activities.

If it was managing user states, I would consider D (Datastore/Firestore) but this is not the case.  
So, from my point of view, A is the correct answer.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: A**

A is correct

upvoted 1 times

 **nehaxlpb** 1 year, 9 months ago

**Selected Answer: A**

Bigquery for user activity analysis . And also the user activity is kind of raw data which being used to segment user or according age , choice so Bigquery fits best fr this use cases

upvoted 2 times

-  **brewpike** 1 year, 11 months ago  
Toss b/w A and D . It depends what needs to be done on user activity, if analytics then A. (Big query) else if customizing customer experience then D (Datastore)  
upvoted 1 times
-  **GCPCloudArchitectUser** 2 years, 2 months ago  
**Selected Answer: D**  
I agree with having to use Datstore  
upvoted 1 times
-  **mariorossi** 2 years, 3 months ago  
A. database only for user activity  
upvoted 1 times
-  **Nidie** 2 years, 3 months ago  
I choose D, datastore.  
upvoted 2 times
-  **boof** 2 years, 7 months ago  
#37 "Your existing application keeps user state information in a single MySQL database. This state information is very user-specific and depends heavily on how long a user has been using an application. The MySQL database is causing challenges to maintain and enhance the schema for various users. Which storage option should you choose?"  
[https://cloud.google.com/datastore/docs/concepts/overview#what\\_its\\_good\\_for](https://cloud.google.com/datastore/docs/concepts/overview#what_its_good_for)  
"Datastore/Firestore can store and query the following types of data:  
User profiles that deliver a customized experience based on the user's past activities and preferences"  
I feel like this is a toss up between these two since we're talking about user profiles/data, would vote for D here bc MySQL offers a really rigid schema and isn't well suited to massive scaling either.  
upvoted 3 times

Question #81

Topic 1

#### Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

#### To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

#### Company Overview -

HipLocal is a community application designed to facilitate communication between people in close proximity. It is used for event planning and organizing sporting events, and for businesses to connect with their local communities. HipLocal launched recently in a few neighborhoods in Dallas and is rapidly growing into a global phenomenon. Its unique style of hyper-local community communication and business outreach is in demand around the world.

#### Executive Statement -

We are the number one local community app; it's time to take our local community services global. Our venture capital investors want to see rapid growth and the same great experience for new local and virtual communities that come online, whether their members are 10 or 10000 miles away from each other.

#### Solution Concept -

HipLocal wants to expand their existing service, with updated functionality, in new regions to better serve their global customers. They want to hire and train a new team to support these regions in their time zones. They will need to ensure that the application scales smoothly and provides clear uptime data.

#### Existing Technical Environment -

HipLocal's environment is a mix of on-premises hardware and infrastructure running in Google Cloud Platform. The HipLocal team understands their application well, but has limited experience in global scale applications. Their existing technical environment is as follows:

- \* Existing APIs run on Compute Engine virtual machine instances hosted in GCP.
- \* State is stored in a single instance MySQL database in GCP.
- \* Data is exported to an on-premises Teradata/Vertica data warehouse.
- \* Data analytics is performed in an on-premises Hadoop environment.
- \* The application has no logging.
- \* There are basic indicators of uptime; alerts are frequently fired when the APIs are unresponsive.

#### Business Requirements -

HipLocal's investors want to expand their footprint and support the increase in demand they are seeing. Their requirements are:

- \* Expand availability of the application to new regions.
- \* Increase the number of concurrent users that can be supported.
- \* Ensure a consistent experience for users when they travel to different regions.
- \* Obtain user activity metrics to better understand how to monetize their product.
- \* Ensure compliance with regulations in the new regions (for example, GDPR).
- \* Reduce infrastructure management time and cost.
- \* Adopt the Google-recommended practices for cloud computing.

#### Technical Requirements -

- \* The application and backend must provide usage metrics and monitoring.
- \* APIs require strong authentication and authorization.
- \* Logging must be increased, and data should be stored in a cloud analytics platform.
- \* Move to serverless architecture to facilitate elastic scaling.
- \* Provide authorized access to internal apps in a secure manner.

HipLocal is configuring their access controls.

Which firewall configuration should they implement?

- A. Block all traffic on port 443.
- B. Allow all traffic into the network.
- C. Allow traffic on port 443 for a specific tag.
- D. Allow all traffic on port 443 into the network.

**Correct Answer: C**

*Community vote distribution*

C (100%)

 **[Removed]**  1 year, 11 months ago

It depends on which authentication we are talking about. If it is an authentication to internal app, the answer is C (with specific tag). If it is an authentication to 'the' app that HipLocal offers to general users, the answer is D (with tag, all users outside that tag will be rejected). It is not c to me, on which tag we are talking here.

upvoted 7 times

 **\_rajan\_**  7 months, 1 week ago

**Selected Answer: C**

C is correct

upvoted 1 times

 **closer89** 11 months, 3 weeks ago

**Selected Answer: C**

app is running on compute engine

i assume nginx ls running on compute instance and you need to expose 443 and 80 for network tag

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: C**

C is correct

upvoted 1 times

 **dishum** 2 years ago

C is correct

upvoted 1 times

 **syu31svc** 2 years, 9 months ago

Port 443 -> HTTPS

Blocking traffic on 443 does not make sense so A is wrong

Allow all traffic is definitely not secure so B is out too

Between C and D I'll take C

upvoted 3 times

 **syu31svc** 2 years, 9 months ago

On second thought, correct answer is D as the application needs to be exposed externally the port 443 can be opened for all traffic.

upvoted 4 times

 **p4** 2 years, 3 months ago

I would take C, to use tags as well, so that only traffic to selected VMs is allowed from outside, probably you don't want to expose every VM via port 443?

<https://cloud.google.com/vpc/docs/add-remove-network-tags>

upvoted 7 times

**Case study -**

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

**To start the case study -**

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

**Company Overview -**

HipLocal is a community application designed to facilitate communication between people in close proximity. It is used for event planning and organizing sporting events, and for businesses to connect with their local communities. HipLocal launched recently in a few neighborhoods in Dallas and is rapidly growing into a global phenomenon. Its unique style of hyper-local community communication and business outreach is in demand around the world.

**Executive Statement -**

We are the number one local community app; it's time to take our local community services global. Our venture capital investors want to see rapid growth and the same great experience for new local and virtual communities that come online, whether their members are 10 or 10000 miles away from each other.

**Solution Concept -**

HipLocal wants to expand their existing service, with updated functionality, in new regions to better serve their global customers. They want to hire and train a new team to support these regions in their time zones. They will need to ensure that the application scales smoothly and provides clear uptime data.

**Existing Technical Environment -**

HipLocal's environment is a mix of on-premises hardware and infrastructure running in Google Cloud Platform. The HipLocal team understands their application well, but has limited experience in global scale applications. Their existing technical environment is as follows:

- \* Existing APIs run on Compute Engine virtual machine instances hosted in GCP.
- \* State is stored in a single instance MySQL database in GCP.
- \* Data is exported to an on-premises Teradata/Vertica data warehouse.
- \* Data analytics is performed in an on-premises Hadoop environment.
- \* The application has no logging.
- \* There are basic indicators of uptime; alerts are frequently fired when the APIs are unresponsive.

**Business Requirements -**

HipLocal's investors want to expand their footprint and support the increase in demand they are seeing. Their requirements are:

- \* Expand availability of the application to new regions.
- \* Increase the number of concurrent users that can be supported.
- \* Ensure a consistent experience for users when they travel to different regions.
- \* Obtain user activity metrics to better understand how to monetize their product.
- \* Ensure compliance with regulations in the new regions (for example, GDPR).
- \* Reduce infrastructure management time and cost.
- \* Adopt the Google-recommended practices for cloud computing.

#### Technical Requirements -

- \* The application and backend must provide usage metrics and monitoring.
- \* APIs require strong authentication and authorization.
- \* Logging must be increased, and data should be stored in a cloud analytics platform.
- \* Move to serverless architecture to facilitate elastic scaling.
- \* Provide authorized access to internal apps in a secure manner.

HipLocal's data science team wants to analyze user reviews.

How should they prepare the data?

- A. Use the Cloud Data Loss Prevention API for redaction of the review dataset.
- B. Use the Cloud Data Loss Prevention API for de-identification of the review dataset.
- C. Use the Cloud Natural Language Processing API for redaction of the review dataset.
- D. Use the Cloud Natural Language Processing API for de-identification of the review dataset.

#### Correct Answer: D

Community vote distribution

B (63%)

D (38%)

 **MickeyRourke** Highly Voted 3 years, 4 months ago

Answer is B . Data loss prevention api is used for de-identification not natural language api  
upvoted 19 times

 **santoshchauhan** Most Recent 1 month, 3 weeks ago

Selected Answer: B

B. Use the Cloud Data Loss Prevention API for de-identification of the review dataset.

For analyzing user reviews, especially if they contain sensitive user information, it's important to protect user privacy. The Cloud Data Loss Prevention (DLP) API provides ways to de-identify sensitive data, which includes redaction, masking, tokenization, and other transformation techniques to obscure or remove sensitive information.

De-identification refers to the process of removing or altering information that could be used to identify an individual, making the data safe for analysis without exposing personal information. This is crucial when handling user data to ensure compliance with privacy regulations and maintain user trust.

upvoted 1 times

 **theseawillclaim** 2 months, 2 weeks ago

Selected Answer: B

Of course it's DLP.  
NLP API makes no sense here.  
upvoted 1 times

 **Kadhem** 4 months, 1 week ago

Selected Answer: B

Answer is B  
<https://cloud.google.com/dlp/docs/deidentify-sensitive-data>  
upvoted 1 times

 **wanrltw** 5 months, 1 week ago

**Selected Answer: D**

<https://www.exam-answer.com/hiplocal-data-preparation>

"De-identification is the process of removing or obfuscating personally identifiable information (PII) from a dataset, so that individuals cannot be identified. In this case, the data science team needs to analyze user reviews, which could potentially contain PII such as names, email addresses, or other personal information. To protect the privacy of the users, the data should be de-identified before it is analyzed."

The Cloud Natural Language Processing API provides various features such as entity recognition, sentiment analysis, and syntax analysis. This API also includes a feature for de-identification, which can be used to remove PII from text data. This feature uses machine learning models to identify and mask or replace PII in the text.

In contrast, the Cloud Data Loss Prevention API is designed to identify and redact sensitive data, such as credit card numbers, social security numbers, or other types of PII. It is not intended for general de-identification of text data."

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: D**

D is correct.

upvoted 1 times

 **jason0001** 1 year ago

**Selected Answer: D**

The Cloud Natural Language Processing API can help to extract insights from the user reviews, such as sentiment analysis and entity recognition. Additionally, de-identification can help to protect user privacy by removing any personal information from the review data.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: B**

B is correct

upvoted 1 times

 **[Removed]** 1 year, 11 months ago

It looks like 'redaction' is a type of 'de-identification'.

<https://cloud.google.com/dlp/docs/transformations-reference#redaction>

upvoted 1 times

 **[Removed]** 1 year, 11 months ago

B.

I suspect this is more an English problem than a cloud problem. "redaction of the review dataset" means removing the review itself. "de-identification of the review dataset" means you keep the review text itself, but mask the reviewer's identity so that we do not know any more who wrote it.

upvoted 2 times

 **p4** 2 years, 3 months ago

A or B?

what speaks for de-identification over reduction?

reduction: replace sensitive data with a mask

de-identification: replace sensitive data, while keeping possibility of re-identification by trusted party

reduction protects user's data even more, whereas de-identification might be better for analyzing the data and link them together, right?

upvoted 1 times

 **ParagSanyashiv** 2 years, 3 months ago

**Selected Answer: B**

B is the correct answer

upvoted 1 times

 **Gini** 2 years, 4 months ago

I would take C as the purpose is to "analyze user reviews". Generally there is not sensitive data in reviews so I eliminate A and B. Natural Language Processing API is for analyzing things like reviews and comments, it has nothing to do with de-identification.  
upvoted 1 times

 **Gini** 2 years, 4 months ago

Reviewing this question again, the question asks "how to prepare the data" so I change my mind to B, to de-identify the data by Cloud Data Loss Prevention first. After that Natural Language Processing can be used to analyze the data.  
upvoted 1 times

 **GoatSack** 2 years, 5 months ago

Answer B: <https://cloud.google.com/dlp/docs/deidentify-sensitive-data>  
upvoted 1 times

 **GoatSack** 2 years, 5 months ago

Backs up: "Ensure compliance with regulations in the new regions (for example, GDPR)."  
upvoted 1 times

 **celia20200410** 2 years, 9 months ago

B: <https://cloud.google.com/architecture/de-identification-re-identification-pii-using-cloud-dlp>  
De-identification of PII in large-scale datasets using Cloud DLP  
Cloud DLP enables transformations such as redaction, masking, tokenization, bucketing, and other methods of de-identification.  
upvoted 4 times

 **syu31svc** 2 years, 9 months ago

I would take C; Cloud Natural Language Processing API for redaction

Data Loss Prevention or DLP is not meant for analytics so A and B are wrong while de-identification is for DLP  
upvoted 2 times

 **fraloca** 3 years, 4 months ago

For me the solution is C  
upvoted 1 times

 **donchick** 3 years, 4 months ago

I'd choose Natural Language API de-identification.  
upvoted 1 times

Question #83

Topic 1

#### Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Company Overview -

HipLocal is a community application designed to facilitate communication between people in close proximity. It is used for event planning and organizing sporting events, and for businesses to connect with their local communities. HipLocal launched recently in a few neighborhoods in Dallas and is rapidly growing into a global phenomenon. Its unique style of hyper-local community communication and business outreach is in demand around the world.

Executive Statement -

We are the number one local community app; it's time to take our local community services global. Our venture capital investors want to see rapid growth and the same great experience for new local and virtual communities that come online, whether their members are 10 or 10000 miles away from each other.

Solution Concept -

HipLocal wants to expand their existing service, with updated functionality, in new regions to better serve their global customers. They want to hire and train a new team to support these regions in their time zones. They will need to ensure that the application scales smoothly and provides clear uptime data.

Existing Technical Environment -

HipLocal's environment is a mix of on-premises hardware and infrastructure running in Google Cloud Platform. The HipLocal team understands their application well, but has limited experience in global scale applications. Their existing technical environment is as follows:

- \* Existing APIs run on Compute Engine virtual machine instances hosted in GCP.
- \* State is stored in a single instance MySQL database in GCP.
- \* Data is exported to an on-premises Teradata/Vertica data warehouse.
- \* Data analytics is performed in an on-premises Hadoop environment.
- \* The application has no logging.
- \* There are basic indicators of uptime; alerts are frequently fired when the APIs are unresponsive.

Business Requirements -

HipLocal's investors want to expand their footprint and support the increase in demand they are seeing. Their requirements are:

- \* Expand availability of the application to new regions.
- \* Increase the number of concurrent users that can be supported.
- \* Ensure a consistent experience for users when they travel to different regions.
- \* Obtain user activity metrics to better understand how to monetize their product.
- \* Ensure compliance with regulations in the new regions (for example, GDPR).
- \* Reduce infrastructure management time and cost.
- \* Adopt the Google-recommended practices for cloud computing.

Technical Requirements -

- \* The application and backend must provide usage metrics and monitoring.
- \* APIs require strong authentication and authorization.
- \* Logging must be increased, and data should be stored in a cloud analytics platform.
- \* Move to serverless architecture to facilitate elastic scaling.
- \* Provide authorized access to internal apps in a secure manner.

In order for HipLocal to store application state and meet their stated business requirements, which database service should they migrate to?

- A. Cloud Spanner
- B. Cloud Datastore
- C. Cloud Memorystore as a cache
- D. Separate Cloud SQL clusters for each region

**Correct Answer: A**

*Community vote distribution*

A (80%)

D (20%)

 **celia20200410** (Highly Voted) 2 years, 9 months ago

<https://cloud.google.com/blog/products/databases/spanner-relational-database-for-all-size-applications-faqs>  
[https://cloud.google.com/architecture/best-practices-cloud-spanner-gaming-database#select\\_a\\_data\\_locality\\_to\\_meet\\_compliance\\_requirements](https://cloud.google.com/architecture/best-practices-cloud-spanner-gaming-database#select_a_data_locality_to_meet_compliance_requirements)  
<https://cloud.google.com/blog/products/gcp/introducing-cloud-spanner-a-global-database-service-for-mission-critical-applications>

A. Cloud Spanner

- global service
- supports durably store application data
- supports GDPR, to meet data locality

upvoted 10 times

 **GoatSack** 2 years, 5 months ago

Agree with Celia.

upvoted 1 times

 **santoshchauhan** (Most Recent) 1 month, 3 weeks ago

**Selected Answer: A**

Here's how Cloud Spanner aligns with HipLocal's business requirements:

It allows for a global distribution of databases, ensuring users have a consistent experience no matter their location.

Cloud Spanner's horizontal scalability supports an increasing number of concurrent users, which is necessary for HipLocal's rapid growth. It offers high availability and regional data replication, which can help HipLocal ensure compliance with various regional data regulations like GDPR.

Managed service reduces the infrastructure management time and cost, meeting another of HipLocal's key requirements.

upvoted 1 times

 **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: A**

A is best suited.

upvoted 1 times

 **TQM\_\_9MD** 9 months ago

**Selected Answer: A**

I think A

upvoted 1 times

 **mrvergara** 1 year, 2 months ago

**Selected Answer: D**

Cloud Spanner is a highly scalable, globally-distributed database service offered by Google Cloud, but it may not be the best fit for HipLocal's needs. While Cloud Spanner provides automatic and instant scaling, strong consistency guarantees, and high availability, it also comes with a higher operational overhead and cost compared to other Google Cloud databases. Additionally, Cloud Spanner is designed for large, mission-critical applications that require strict consistency guarantees across multiple regions, which may not be necessary for HipLocal's current requirements.

In this case, it would be more appropriate for HipLocal to separate Cloud SQL clusters for each region to store their application state, as this solution would provide the necessary data storage capabilities and be more cost-effective for their current requirements.

upvoted 1 times

 **mrvergara** 1 year, 2 months ago

Changing to A because of this requirement: Ensure a consistent experience for users when they travel to different regions.

upvoted 2 times

✉️  **tomato123** 1 year, 8 months ago

Selected Answer: A

A is correct

upvoted 1 times

✉️  **syu31svc** 2 years, 9 months ago

This is similar to qn 48; I would say A is the answer

upvoted 1 times

✉️  **syu31svc** 2 years, 8 months ago

Changing to D as qn 50 answer is Cloud SQL; consistency sake

upvoted 1 times

✉️  **GoatSack** 2 years, 5 months ago

From case study instructions: "Each question is independent of the other questions in this case study."

I am leaning towards Spanner here. What do you think?

upvoted 2 times

✉️  **mastodilu** 2 years, 11 months ago

I guess that the answer is D because of the GDPR

upvoted 3 times

✉️  **ralf\_cc** 2 years, 10 months ago

Tend to agree with you

upvoted 1 times

✉️  **GCPCloudArchitectUser** 2 years, 2 months ago

Seriously you want to spin up cloud sql in every region? ...

upvoted 1 times

✉️  **alex8081** 1 year, 8 months ago

" Reduce infrastructure management time and cost".. Cloud Spanner is a database for business critical applications that completely replaces one or more Data Warehouses... is out of scope. I Vote Cloud SQL

upvoted 1 times

✉️  **closer89** 11 months, 3 weeks ago

what about management time for cloud sql clusters?

you can tune your cloud spanner instances, nobody forces you to use 1000 nodes.

1. Cloud Spanner charges for the amount of storage used per month. The pricing starts at \$0.30/GB/month for regional storage and \$0.60/GB/month for multi-regional storage.

2. Cloud Spanner charges for the number of nodes used per month. The pricing starts at \$0.90/hour/node for regional instances and \$1.44/hour/node for multi-regional instances.

3. Cloud Spanner charges for the amount of data processed per month. The pricing starts at \$0.06/GB for regional instances and \$0.12/GB for multi-regional instances

upvoted 1 times

✉️  **closer89** 11 months, 3 weeks ago

isn't it affordable for hiplocal company that wants to "left footprint"??

upvoted 1 times

✉️  **TNT87** 1 year, 5 months ago

So spanner doesn't support GDPR??? kkkkkkkkkkkkkkk

upvoted 1 times

You have an application deployed in production. When a new version is deployed, you want to ensure that all production traffic is routed to the new version of your application. You also want to keep the previous version deployed so that you can revert to it if there is an issue with the new version.

Which deployment strategy should you use?

- A. Blue/green deployment
- B. Canary deployment
- C. Rolling deployment
- D. Recreate deployment

**Correct Answer: C**

*Community vote distribution*

A (89%)

11%

 **donchick** Highly Voted 3 years, 4 months ago  
Blue/green seems to be more appropriate(<https://www.redhat.com/en/topics/devops/what-is-blue-green-deployment>)  
upvoted 21 times

 **\_rajan\_** Most Recent 7 months, 1 week ago

**Selected Answer: A**

This can be achieved by using Blue/Green approach.  
upvoted 1 times

 **[Removed]** 1 year, 2 months ago

**Selected Answer: A**

Definitely Blue/Green Deployment  
upvoted 1 times

 **tab02733** 1 year, 6 months ago

**Selected Answer: A**

The difference between canary deployment and blue/green deployment is the presence or absence of a testing process.  
<https://www.sedesign.co.jp/dxinsight/what-is-canary-release>  
Since there is no testing process in the question I vote for Blue/Green Deployment

Question #85

Topic 1

You are porting an existing Apache/MySQL/PHP application stack from a single machine to Google Kubernetes Engine. You need to determine how to containerize the application. Your approach should follow Google-recommended best practices for availability.  
What should you do?

- A. Package each component in a separate container. Implement readiness and liveness probes.
- B. Package the application in a single container. Use a process management tool to manage each component.
- C. Package each component in a separate container. Use a script to orchestrate the launch of the components.
- D. Package the application in a single container. Use a bash script as an entrypoint to the container, and then spawn each component as a background job.

**Correct Answer: D**

Reference:

<https://cloud.google.com/architecture/best-practices-for-building-containers>

*Community vote distribution*

A (100%)

 **omermahgoub** Highly Voted 1 year, 3 months ago

A. Package each component in a separate container. Implement readiness and liveness probes.

This is the recommended approach for containerizing an application for use on Kubernetes. By packaging each component in a separate container, you can ensure that each component is isolated and can be managed independently. You can then use readiness and liveness probes to monitor the health and availability of each component, which will help ensure the overall availability of the application.

upvoted 6 times

 **omermahgoub** 1 year, 3 months ago

D. Package the application in a single container. Use a bash script as an entrypoint to the container, and then spawn each component as a background job.

This option is not recommended because it does not follow best practices for containerization. By packaging the entire application in a single container, you would not be able to manage the individual components of the application independently, which could make it more difficult to ensure their availability. Additionally, using a bash script to spawn each component as a background job is not an effective way to manage and monitor the availability of the components.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

C. Package each component in a separate container. Use a script to orchestrate the launch of the components.

This option is not recommended because it does not follow best practices for containerization. While packaging each component in a separate container is a good approach, using a script to orchestrate the launch of the components is not an effective way to ensure their availability. Instead, you should use readiness and liveness probes to monitor the health and availability of each component.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

B. Package the application in a single container. Use a process management tool to manage each component.

This option is not recommended because it does not follow best practices for containerization. By packaging the entire application in a single container, you would not be able to manage the individual components of the application independently, which could make it more difficult to ensure their availability.

upvoted 1 times

 **\_rajan\_** (Most Recent) 7 months, 1 week ago

**Selected Answer: A**

A is best suited here.

upvoted 1 times

 **zellck** 1 year, 4 months ago

**Selected Answer: A**

A is the answer.

[https://cloud.google.com/architecture/best-practices-for-building-containers#package\\_a\\_single\\_app\\_per\\_container](https://cloud.google.com/architecture/best-practices-for-building-containers#package_a_single_app_per_container)

When you start working with containers, it's a common mistake to treat them as virtual machines that can run many different things simultaneously. A container can work this way, but doing so reduces most of the advantages of the container model. For example, take a classic Apache/MySQL/PHP stack: you might be tempted to run all the components in a single container. However, the best practice is to use two or three different containers: one for Apache, one for MySQL, and potentially one for PHP if you are running PHP-FPM.

upvoted 1 times

 **TNT87** 1 year, 5 months ago

the best practice is to use two or three different containers: one for Apache, one for MySQL, and potentially one for PHP if you are running PHP-FPM.

Because a container is designed to have the same lifecycle as the app it hosts, each of your containers should contain only one app. When a container starts, so should the app, and when the app stops, so should the container. The following diagram shows this best practice.

[https://cloud.google.com/architecture/best-practices-for-building-containers#package\\_a\\_single\\_app\\_per\\_container](https://cloud.google.com/architecture/best-practices-for-building-containers#package_a_single_app_per_container)

Answer A

upvoted 1 times

 **[Removed]** 1 year, 5 months ago

did you take the exam?

upvoted 1 times

 **TNT87** 1 year, 5 months ago

Nope , not yet. im doing so soon

upvoted 2 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: A**

A is correct

upvoted 2 times

 **ParagSanyashiv** 2 years, 3 months ago

**Selected Answer: A**

According to me "A" is the correct answer, because the best practice says "classic Apache/MySQL/PHP stack: you might be tempted to run all the components in a single container. However, the best practice is to use two or three different containers: one for Apache, one for MySQL, and potentially one for PHP if you are running PHP-FPM."

upvoted 3 times

 **Blueocean** 2 years, 3 months ago

Agree with Option A.

<https://cloud.google.com/blog/products/containers-kubernetes/7-best-practices-for-building-containers>

upvoted 1 times

 **Blueocean** 2 years, 3 months ago

<https://cloud.google.com/architecture/best-practices-for-building-containers>

upvoted 1 times

Question #86

Topic 1

You are developing an application that will be launched on Compute Engine instances into multiple distinct projects, each corresponding to the environments in your software development process (development, QA, staging, and production). The instances in each project have the same application code but a different configuration. During deployment, each instance should receive the application's configuration based on the environment it serves. You want to minimize the number of steps to configure this flow. What should you do?

- A. When creating your instances, configure a startup script using the gcloud command to determine the project name that indicates the correct environment.
- B. In each project, configure a metadata key `environment` whose value is the environment it serves. Use your deployment tool to query the instance metadata and configure the application based on the `environment` value.
- C. Deploy your chosen deployment tool on an instance in each project. Use a deployment job to retrieve the appropriate configuration file from your version control system, and apply the configuration when deploying the application on each instance.
- D. During each instance launch, configure an instance custom-metadata key named `environment` whose value is the environment the instance serves. Use your deployment tool to query the instance metadata, and configure the application based on the `environment` value.

**Correct Answer: D**

Reference:

<https://cloud.google.com/compute/docs/metadata/overview>

*Community vote distribution*

B (100%)

 **wanrltw** 5 months, 1 week ago

**Selected Answer: B**

<https://cloud.google.com/compute/docs/metadata/setting-custom-metadata#set-custom-project-wide-metadata>

upvoted 1 times

 **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: B**

Option B is correct we usually put this details in Environment variable.

upvoted 1 times

👤 **omermahgoub** 1 year, 3 months ago

Option A, configuring a startup script using the gcloud command to determine the project name, is not a feasible solution because it requires additional steps to be taken during instance launch. Option C, deploying a deployment tool on an instance in each project and using a deployment job to retrieve the appropriate configuration file, is not a feasible solution because it requires additional steps to be taken during instance launch and involves the use of a separate deployment tool. Option D, configuring an instance custom-metadata key named "environment" during each instance launch, is not a feasible solution because it requires additional steps to be taken during instance launch.

upvoted 2 times

👤 **omermahgoub** 1 year, 3 months ago

Answer is B

You can configure a metadata key named "environment" in each project, with a value corresponding to the environment it serves (development, QA, staging, or production). Then, you can use your deployment tool to query the instance metadata and configure the application based on the "environment" value. This allows you to minimize the number of steps to configure the flow, as you only need to set the "environment" value in each project and use your deployment tool to query the metadata.

upvoted 2 times

👤 **zellck** 1 year, 4 months ago

**Selected Answer: B**

B is the answer.

<https://cloud.google.com/compute/docs/metadata/setting-custom-metadata#set-custom>

upvoted 1 times

👤 **TNT87** 1 year, 5 months ago

<https://cloud.google.com/compute/docs/metadata/querying-metadata>

upvoted 1 times

👤 **TNT87** 1 year, 5 months ago

<https://cloud.google.com/compute/docs/metadata/setting-custom-metadata#set-custom>

upvoted 1 times

👤 **[Removed]** 1 year, 5 months ago

Did you take the exam?

upvoted 1 times

👤 **tomato123** 1 year, 8 months ago

**Selected Answer: B**

B is correct

upvoted 2 times

👤 **nqthien041292** 2 years ago

**Selected Answer: B**

Vote B

upvoted 2 times

👤 **jitu028** 2 years ago

Answer should be B

upvoted 2 times

👤 **KillerGoogle** 2 years, 1 month ago

D,

'environment' is not in one of the default key

<https://cloud.google.com/compute/docs/metadata/default-metadata-values>

upvoted 3 times

👤 **GCPCloudArchitectUser** 2 years, 2 months ago

For Answer D :

Question says minimize steps and adding metadata to each instance seems longer route ?

upvoted 3 times

👤 **scaenrui** 2 years, 3 months ago

I vote B

upvoted 4 times

You are developing an ecommerce application that stores customer, order, and inventory data as relational tables inside Cloud Spanner. During a recent load test, you discover that Spanner performance is not scaling linearly as expected. Which of the following is the cause?

- A. The use of 64-bit numeric types for 32-bit numbers.
- B. The use of the STRING data type for arbitrary-precision values.
- C. The use of Version 1 UUIDs as primary keys that increase monotonically.
- D. The use of LIKE instead of STARTS\_WITH keyword for parameterized SQL queries.

**Correct Answer: B***Community vote distribution*

C (100%)

  **gfr892** Highly Voted 2 years, 3 months ago

C is correct [https://cloud.google.com/spanner/docs/schema-and-data-model#choosing\\_a\\_primary\\_key](https://cloud.google.com/spanner/docs/schema-and-data-model#choosing_a_primary_key)  
upvoted 8 times

  **santoshchauhan** Most Recent 1 month, 3 weeks agoSelected Answer: C

C. The use of Version 1 UUIDs as primary keys that increase monotonically.

When designing schemas for Cloud Spanner, it is important to consider how the choice of primary keys can impact performance, especially under heavy load. Cloud Spanner splits data among servers based on the primary key values, so if the keys are monotonically increasing, as in the case with Version 1 UUIDs, new inserts are constantly added to the end of the table. This can create hotspots, where a single node receives disproportionate amount of read and write requests, leading to performance bottlenecks and preventing linear scaling.

upvoted 1 times

  **\_rajan\_** 7 months, 1 week agoSelected Answer: C

C is the best option.

upvoted 1 times

  **omermahgoub** 1 year, 3 months ago

In Cloud Spanner, the use of Version 1 UUIDs as primary keys that increase monotonically can cause performance issues because they are not evenly distributed. This can lead to hot regions, where a disproportionate number of requests are sent to a specific node or range of nodes, causing those nodes to become overloaded and leading to decreased performance. To improve performance, you should consider using primary keys that are more evenly distributed, such as hash-based keys or random integers.

upvoted 2 times

  **omermahgoub** 1 year, 3 months ago

A, the use of 64-bit numeric types for 32-bit numbers, is not likely to cause performance issues in Cloud Spanner.

B, the use of the STRING data type for arbitrary-precision values, is not likely to cause performance issues in Cloud Spanner.

D, the use of LIKE instead of STARTS\_WITH keyword for parameterized SQL queries, is not likely to cause performance issues in Cloud Spanner.

upvoted 1 times

  **zellck** 1 year, 4 months agoSelected Answer: C

C is the answer.

<https://cloud.google.com/spanner/docs/schema-design#primary-key-prevent-hotspots>

Schema design best practice #1: Do not choose a column whose value monotonically increases or decreases as the first key part for a high write table.

upvoted 1 times

✉️ **TNT87** 1 year, 5 months ago  
[https://cloud.google.com/spanner/docs/schema-design#uuid\\_primary\\_key](https://cloud.google.com/spanner/docs/schema-design#uuid_primary_key)  
Ans C  
upvoted 1 times

✉️ **tomato123** 1 year, 8 months ago  
**Selected Answer: C**  
C is correct  
upvoted 2 times

✉️ **brewpike** 1 year, 11 months ago  
C - Version 1 is not recommended.  
upvoted 2 times

✉️ **morenocasado** 2 years ago  
**Selected Answer: C**  
Community choice is C  
upvoted 2 times

✉️ **scaenruy** 2 years, 3 months ago  
I vote C  
upvoted 3 times

Question #88

Topic 1

You are developing an application that reads credit card data from a Pub/Sub subscription. You have written code and completed unit testing. You need to test the Pub/Sub integration before deploying to Google Cloud. What should you do?

- A. Create a service to publish messages, and deploy the Pub/Sub emulator. Generate random content in the publishing service, and publish to the emulator.
- B. Create a service to publish messages to your application. Collect the messages from Pub/Sub in production, and replay them through the publishing service.
- C. Create a service to publish messages, and deploy the Pub/Sub emulator. Collect the messages from Pub/Sub in production, and publish them to the emulator.
- D. Create a service to publish messages, and deploy the Pub/Sub emulator. Publish a standard set of testing messages from the publishing service to the emulator.

**Correct Answer: D**

*Community vote distribution*

D (100%)

 **scaenruy** Highly Voted 2 years, 3 months ago

I vote D

upvoted 6 times

 **wanrltw** Most Recent 5 months, 1 week ago

**Selected Answer: D**

<https://cloud.google.com/pubsub/docs/emulator>

upvoted 1 times

 **amier** 9 months, 2 weeks ago

**Selected Answer: D**

D is correct

upvoted 1 times

 **zelliCK** 1 year, 4 months ago

**Selected Answer: D**

D is the answer.

upvoted 1 times

 **lakiluk** 1 year, 6 months ago

**Selected Answer: D**

Vote D

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: D**

D is correct

upvoted 2 times

Question #89

*Topic 1*

You are designing an application that will subscribe to and receive messages from a single Pub/Sub topic and insert corresponding rows into a database. Your application runs on Linux and leverages preemptible virtual machines to reduce costs. You need to create a shutdown script that will initiate a graceful shutdown.

What should you do?

- A. Write a shutdown script that uses inter-process signals to notify the application process to disconnect from the database.
- B. Write a shutdown script that broadcasts a message to all signed-in users that the Compute Engine instance is going down and instructs them to save current work and sign out.
- C. Write a shutdown script that writes a file in a location that is being polled by the application once every five minutes. After the file is read, the application disconnects from the database.
- D. Write a shutdown script that publishes a message to the Pub/Sub topic announcing that a shutdown is in progress. After the application reads the message, it disconnects from the database.

**Correct Answer: C**

Reference:

<https://cloud.google.com/compute/docs/shutdownscript>*Community vote distribution*

A (93%)

7%

**GCPCloudArchitectUser** Highly Voted 2 years, 2 months ago**Selected Answer: A**

IMO it should be A

upvoted 7 times

**JonathanSJ** Highly Voted 2 years, 3 months ago

I vote A

upvoted 5 times

**santoshchauhan** Most Recent 1 month, 3 weeks ago**Selected Answer: A**

A. Write a shutdown script that uses inter-process signals to notify the application process to disconnect from the database.

In the scenario of using preemptible virtual machines for running an application that interacts with a database, a graceful shutdown is essential to ensure data consistency and prevent potential issues like incomplete transactions. A shutdown script utilizing inter-process signals is an efficient and direct way to manage this process.

upvoted 1 times

**wanrltw** 5 months, 1 week ago**Selected Answer: A**

I vote A:

- <https://cloud.google.com/compute/docs/instances/preemptible#preemption>
- <https://cloud.google.com/compute/docs/shutdownscript>

Option D is not good as we only have a SINGLE pub/sub topic that is also receiving other messages. I wouldn't rely on the new (shutdown) message to come through and be read by the app timely to disconnect from the db.

upvoted 1 times

**braska** 5 months, 1 week ago**Selected Answer: D**

Option D is a suitable approach for initiating a graceful shutdown in a scenario where the application needs to receive a notification to disconnect from the database before the virtual machine is preempted. Here's how the process works:

upvoted 1 times

**braska** 5 months, 1 week ago

Shutdown Script: Write a shutdown script that is executed when the instance is being preempted.

Publish a Message to Pub/Sub: In the shutdown script, publish a message to the Pub/Sub topic, indicating that a shutdown is in progress. This message serves as a notification to the application.

Application Subscription: The application subscribes to the Pub/Sub topic and continuously listens for incoming messages

upvoted 1 times

**braska** 5 months, 1 week ago

Graceful Shutdown: When the application receives the shutdown message from Pub/Sub, it initiates a graceful shutdown, including disconnecting from the database.

upvoted 1 times

**Aeglas** 5 months ago

You have only one topic, so if there are multiple messages in the queue before the one announcing the disconnect, then a lot of time can pass before the retrieval of the message

upvoted 1 times

**\_rajan\_** 7 months, 1 week ago**Selected Answer: A**

I will go with A

upvoted 1 times

✉️  **maxdanny** 8 months ago

Selected Answer: A

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

upvoted 1 times

✉️  **omermahgoub** 1 year, 3 months ago

It's A

To handle the preemption notice and initiate a graceful shutdown, you should write a shutdown script that uses inter-process signals to notify application process to disconnect from the database. The application can then initiate a graceful shutdown by completing any in-progress tasks and disconnecting from the database, ensuring that data is not lost or corrupted during the shutdown process. This is the most reliable method for initiating a graceful shutdown in response to a preemption notice, as it allows the application to respond directly to the signal and initiate the shutdown process.

upvoted 2 times

✉️  **omermahgoub** 1 year, 3 months ago

Option B, broadcasting a message to signed-in users and instructing them to save current work and sign out, is not relevant to the shutdown process of the application. Option C, writing a file in a location that is being polled by the application, is not a reliable method for initiating a graceful shutdown because the application may not read the file in a timely manner. Option D, publishing a message to the Pub/Sub topic announcing that a shutdown is in progress, is not a reliable method for initiating a graceful shutdown because the application may not read the message in a timely manner.

upvoted 1 times

✉️  **tomato123** 1 year, 8 months ago

Selected Answer: A

A is correct

upvoted 2 times

✉️  **GossipDolphin** 1 year, 9 months ago

it's A

Compute Engine sends a preemption notice to the instance in the form of an ACPI G2 Soft Off signal. You can use a shutdown script to handle the preemption notice and complete cleanup actions before the instance stops.

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

upvoted 1 times

✉️  **szl0144** 1 year, 11 months ago

A seems correct, guys

upvoted 2 times

✉️  **dishum** 2 years ago

Looks like D

upvoted 2 times

✉️  **p4** 2 years, 3 months ago

C does not make sense, because you don't know when pub sub message will be consumed (there might be other events in the queue before) I'll go with option A

upvoted 1 times

✉️  **ParagSanyashiv** 2 years, 3 months ago

According to me , it should be D

upvoted 2 times

✉️  **ParagSanyashiv** 2 years, 3 months ago

Because for preemptible instances the script should run within 30 seconds of the instance being shutdown or restarted, in this case a pub trigger would be faster to perform.

upvoted 2 times

✉️  **morenocasado** 2 years ago

The issue with option D is that we have a SINGLE PubSub topic that is used to send the rows to be inserted; sending a completely different message seems wrong.

upvoted 2 times

You work for a web development team at a small startup. Your team is developing a Node.js application using Google Cloud services, including Cloud Storage and Cloud Build. The team uses a Git repository for version control. Your manager calls you over the weekend and instructs you to make an emergency update to one of the company's websites, and you're the only developer available. You need to access Google Cloud to make the update, but you don't have your work laptop. You are not allowed to store source code locally on a non-corporate computer. How should you set up your developer environment?

- A. Use a text editor and the Git command line to send your source code updates as pull requests from a public computer.
- B. Use a text editor and the Git command line to send your source code updates as pull requests from a virtual machine running on a public computer.
- C. Use Cloud Shell and the built-in code editor for development. Send your source code updates as pull requests.
- D. Use a Cloud Storage bucket to store the source code that you need to edit. Mount the bucket to a public computer as a drive, and use a code editor to update the code. Turn on versioning for the bucket, and point it to the team's Git repository.

**Correct Answer: A**

Reference:

<https://docs.github.com/en/enterprise-server@3.3/get-started/quickstart/contributing-to-projects>

*Community vote distribution*

C (100%)

 **Aeglas** 5 months, 1 week ago

**Selected Answer: C**

C is correct

upvoted 1 times

 **\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: C**

C is correct.

upvoted 1 times

 **zellck** 1 year, 4 months ago

**Selected Answer: C**

C is the answer.

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

Cloud Shell is an interactive shell environment for Google Cloud that lets you learn and experiment with Google Cloud and manage your projects and resources from your web browser.

With Cloud Shell, the Google Cloud CLI and other utilities you need are pre-installed, fully authenticated, up-to-date, and always available whenever you need them. Cloud Shell comes with a built-in code editor with an integrated Cloud Code experience, allowing you to develop, build, debug, and deploy your cloud-based apps entirely in the cloud.

upvoted 2 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: C**

C is correct

upvoted 2 times

Question #91

Topic 1

Your team develops services that run on Google Kubernetes Engine. You need to standardize their log data using Google-recommended practices and make the data more useful in the fewest number of steps. What should you do? (Choose two.)

- A. Create aggregated exports on application logs to BigQuery to facilitate log analytics.
- B. Create aggregated exports on application logs to Cloud Storage to facilitate log analytics.
- C. Write log output to standard output (stdout) as single-line JSON to be ingested into Cloud Logging as structured logs.
- D. Mandate the use of the Logging API in the application code to write structured logs to Cloud Logging.
- E. Mandate the use of the Pub/Sub API to write structured data to Pub/Sub and create a Dataflow streaming pipeline to normalize logs and write them to BigQuery for analytics.

**Correct Answer: AE**

*Community vote distribution*

AC (56%)

AD (24%)

CD (21%)

 **p4**  2 years, 3 months ago

I go for A, C

upvoted 10 times

 **ParagSanyashiv**  2 years, 3 months ago

C,D are the correct in this case.

upvoted 9 times

alpha\_canary Most Recent 1 week, 4 days ago

Selected Answer: AC

A: Obvious

C: [https://cloud.google.com/kubernetes-engine/docs/concepts/about-logs#best\\_practices](https://cloud.google.com/kubernetes-engine/docs/concepts/about-logs#best_practices):~:text=Structured%20logging%3A%20The%20logging%20agent%20integrated%20with%20GKE%20will%20read%20ON%20documents%20serialized%20to%20single%2Dline%20strings%20and%20written%20to%20standard%20output%20or%20standard%20error%20and%20will%20send%20them%20to%20Google%20Cloud%20Observability%20as%20structured%20log%20entries.

upvoted 1 times

santoshchauhan 1 month, 3 weeks ago

Selected Answer: AC

C. Writing log output to standard output (stdout) as single-line JSON: This is a recommended practice for containerized applications running on Kubernetes. Kubernetes captures everything written to stdout and stderr and routes it to its logging agent (in this case, Cloud Logging in GKE). By structuring logs as single-line JSON, you enable Cloud Logging to ingest them as structured logs, which are more queryable and readable. This approach is efficient and does not require any changes in the application to use specific logging APIs.

A. Create aggregated exports on application logs to BigQuery: Exporting logs to BigQuery allows for powerful analytics capabilities. BigQuery is well-suited for running fast, SQL-like queries on large datasets. By exporting logs to BigQuery, you can perform more complex analyses and gain deeper insights from your log data.

upvoted 3 times

Kadhem 4 months ago

Selected Answer: CD

[https://cloud.google.com/kubernetes-engine/docs/concepts/about-logs#best\\_practices](https://cloud.google.com/kubernetes-engine/docs/concepts/about-logs#best_practices)

upvoted 2 times

Kadhem 4 months, 1 week ago

Selected Answer: AC

fewest steps + make log useful (analytics)

upvoted 2 times

Kadhem 4 months ago

based on that link i change my answer to C and D

upvoted 1 times

Kadhem 4 months ago

[https://cloud.google.com/kubernetes-engine/docs/concepts/about-logs#best\\_practices](https://cloud.google.com/kubernetes-engine/docs/concepts/about-logs#best_practices)

upvoted 1 times

IF\_FI 5 months ago

Selected Answer: AC

in the fewest number of steps --> C

upvoted 2 times

wanrltw 5 months, 1 week ago

A & C:

Option A to “make the data more useful”, as BigQuery will allow us to use big data analysis capabilities on the stored logs:  
[https://cloud.google.com/logging/docs/export/aggregated\\_sinks#supported-destinations](https://cloud.google.com/logging/docs/export/aggregated_sinks#supported-destinations)

Option C to “to standardize their log data” creating structured logs: [https://cloud.google.com/kubernetes-engine/docs/concepts/about-logs#best\\_practices](https://cloud.google.com/kubernetes-engine/docs/concepts/about-logs#best_practices)

Option D is also a viable solution but C is preferred, considering the “fewest number of steps” requirement.

Choosing C and D together makes no sense, as both aim to achieve the same goal.

upvoted 2 times

braska 5 months, 1 week ago

Selected Answer: CD

Write log output to standard output (stdout) as single-line JSON:

This practice allows you to use structured logs, specifically in JSON format, making it easier to parse and analyze log data. Cloud Logging can ingest logs from standard output, and structured logs enhance the usability of log data. Mandate the use of the Logging API in the application code to write structured logs to Cloud Logging:

Using the Logging API allows your applications to send structured log data directly to Cloud Logging. Structured logs provide more context and are easier to filter, search, and analyze within Cloud Logging.

upvoted 1 times

wanrltw 5 months, 1 week ago

Both options for the same purpose then? Why would one implement option C having implemented option D?

upvoted 1 times

\_\_rajan\_\_ 7 months, 1 week ago

Selected Answer: AC

Option A: Create aggregated exports on application logs to BigQuery. This will facilitate log analytics by exporting application logs to BigQuery which is a fully-managed, serverless data warehouse. BigQuery allows you to perform advanced analytics on your log data, including running complex queries and visualizing the results.

Option C: Write log output to standard output (stdout) as single-line JSON to be ingested into Cloud Logging as structured logs. This approach involves writing log output to standard output in a specific format (single-line JSON) that can be easily ingested by Cloud Logging. By using structured logs, you can take advantage of advanced querying and filtering capabilities provided by Cloud Logging.

upvoted 2 times

maxdanny 8 months ago

Selected Answer: AC

[https://cloud.google.com/stackdriver/docs/solutions/gke/managing-logs#best\\_practices](https://cloud.google.com/stackdriver/docs/solutions/gke/managing-logs#best_practices)

upvoted 1 times

zanhsieh 10 months, 3 weeks ago

Selected Answer: CD

CD. Only C and D mentioned Cloud Logging. Other options involve extra steps and won't come out free.

"When you create a new GKE cluster, Cloud Operations for GKE integration with Cloud Logging and Cloud Monitoring is enabled by default."

<https://cloud.google.com/stackdriver/docs/solutions/gke/managing-logs#:~:text=When%20you%20create%20a%20new%20GKE%20cluster%2C%20Cloud%20Operations%20for%20GKE%20integration%20Cloud%20Logging%20and%20Cloud%20Monitoring%20is%20enabled%20by%20default>.

upvoted 1 times

ryuhei 12 months ago

Selected Answer: AC

fewest number of steps A &C

upvoted 1 times

Pime13 1 year, 2 months ago

Selected Answer: AC

fewest number of steps -> i believe this sentence is the key. option D would take take.

also: [https://cloud.google.com/stackdriver/docs/solutions/gke/managing-logs#best\\_practices](https://cloud.google.com/stackdriver/docs/solutions/gke/managing-logs#best_practices)

upvoted 1 times

👤 **omermahgoub** 1 year, 3 months ago

Anser is C&D

To standardize log data and make it more useful in the most efficient way, it is recommended to write log output to standard output (stdout) as single-line JSON to be ingested into Cloud Logging as structured logs. This method allows for easy and efficient ingestion of structured log data into Cloud Logging, which can then be easily queried and analyzed. Additionally, mandating the use of the Logging API in the application code allows for the writing of structured logs directly from the application code, improving the usability and reliability of the logs.

upvoted 2 times

👤 **omermahgoub** 1 year, 3 months ago

A and B, which involve creating aggregated exports of log data to either BigQuery or Cloud Storage, are not necessary for standardizing log data. These options may be useful for storing and analyzing log data, but they are not necessary for standardizing the format of the log data. To standardize log data, it is sufficient to write log output to standard output (stdout) as single-line JSON, which can be ingested into Cloud Logging as structured logs.

upvoted 2 times

👤 **omermahgoub** 1 year, 3 months ago

E, which involves using the Pub/Sub API and creating a Dataflow streaming pipeline to normalize logs and write them to BigQuery for analytics, is a more complex solution that requires more steps and is not necessary for standardizing log data. While this option may be useful for storing and analyzing log data, it is not necessary for standardizing the format of the log data. To standardize log data, it is sufficient to write log output to stdout and use the Logging API to write structured logs to Cloud Logging.

upvoted 2 times

👤 **cicciopuddu** 1 year, 4 months ago

Question #92

Topic 1

You are designing a deployment technique for your new applications on Google Cloud. As part of your deployment planning, you want to use live traffic to gather performance metrics for both new and existing applications. You need to test against the full production load prior to launch. What should you do?

- A. Use canary deployment
- B. Use blue/green deployment
- C. Use rolling updates deployment
- D. Use A/B testing with traffic mirroring during deployment

**Correct Answer: A**

Reference:

<https://cloud.google.com/architecture/application-deployment-and-testing-strategies>

*Community vote distribution*

D (82%)

A (18%)

👤 **Ksamilosb** [Highly Voted] 2 years, 2 months ago

D due to "full production load"

upvoted 8 times

👤 **Aeglas** [Most Recent] 5 months, 1 week ago

**Selected Answer: D**

Canary will only redirect a small portion of the traffic, while A/B with mirroring will test the new version in full load

upvoted 2 times

👤 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: D**

A/B testing with traffic mirroring during deployment. This technique allows you to divert a portion of the live production traffic to the new application version while still serving the majority of the traffic to the existing version. By comparing the performance metrics of both versions under real-world conditions, you can assess the impact of the new deployment on your application's performance and stability.

upvoted 2 times

 **Foxal** 1 year, 2 months ago

**Selected Answer: D**

"You need to test against the full production load prior to launch" It's impossible with canary.  
"A/B testing with traffic mirroring during deployment" is the only one possibility we have to test the entire traffic before the roll out.  
upvoted 3 times

 **zellick** 1 year, 4 months ago

**Selected Answer: D**

D is the answer.  
upvoted 1 times

 **[Removed]** 1 year, 6 months ago

D, the question requires more than just "a load" rather the "full load" the only strategy where this happens is A/B testing  
upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: D**

D is correct  
upvoted 2 times

 **akshaychavan7** 1 year, 8 months ago

**Selected Answer: D**

After giving a deliberate thought, I think it's option D.  
The keyword here is 'gather performance metrics,' and as everyone must know A/B testing's whole purpose is to gather performance metrics  
upvoted 1 times

 **nehaxlpb** 1 year, 9 months ago

**Selected Answer: A**

Correct Answer is Shadow test pattern, as it is not in the option selected D  
[https://cloud.google.com/architecture/application-deployment-and-testing-strategies#shadow\\_test\\_pattern](https://cloud.google.com/architecture/application-deployment-and-testing-strategies#shadow_test_pattern)  
upvoted 2 times

 **szl0144** 1 year, 11 months ago

D is my answer  
upvoted 2 times

 **nqthien041292** 2 years ago

**Selected Answer: A**

Vote A  
upvoted 1 times

 **dishum** 2 years ago

Full production - A/B testing, option D  
upvoted 1 times

 **htakami** 2 years, 1 month ago

Canary can test live production traffic on production (Answer A) [https://cloud.google.com/architecture/application-deployment-and-testing-strategies#key\\_benefits\\_4](https://cloud.google.com/architecture/application-deployment-and-testing-strategies#key_benefits_4)  
upvoted 2 times

 **plaffoniera** 1 year, 10 months ago

is it possible that right answer is not present. To me the answer is "Shadow Test Pattern" [https://cloud.google.com/architecture/application-deployment-and-testing-strategies#shadow\\_test\\_pattern](https://cloud.google.com/architecture/application-deployment-and-testing-strategies#shadow_test_pattern). Do you agree ?  
upvoted 1 times

 **ESP\_SAP** 2 years, 1 month ago

Correct answer is A:

Canary deployment is a technique to reduce the risk of introducing a software update in production by slowly rolling out the change to a small subset of users before making it available to everybody.

This deployment technique is one where the SRE of an application development team relies on a router or load balancer to target individual routes. They target a small fragment of the overall user base with the newer version of the application. Once this new set of users are have us the application important metrics will be collected and analyzed to decide whether the new update is good for a full scale rolled to all the user whether it needs to be rolled back for further troubleshooting.

upvoted 2 times

 **GCPCloudArchitectUser** 2 years, 2 months ago

**Selected Answer: D**

you want to use live traffic to gather performance metrics for both new and existing applications  
upvoted 3 times

 **Blueocean** 2 years, 3 months ago

Agree with Option A  
upvoted 1 times

 **scaenruy** 2 years, 3 months ago

I vote A  
upvoted 1 times

Question #93

*Topic 1*

You support an application that uses the Cloud Storage API. You review the logs and discover multiple HTTP 503 Service Unavailable error responses from the

API. Your application logs the error and does not take any further action. You want to implement Google-recommended retry logic to improve success rates.

Which approach should you take?

- A. Retry the failures in batch after a set number of failures is logged.
- B. Retry each failure at a set time interval up to a maximum number of times.
- C. Retry each failure at increasing time intervals up to a maximum number of tries.
- D. Retry each failure at decreasing time intervals up to a maximum number of tries.

**Correct Answer: C**

*Community vote distribution*

C (100%)

 **Aeglas** 5 months, 1 week ago

**Selected Answer: C**

Exponential backoff with limit  
upvoted 1 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: C**

exponential backoff algorithm retries  
upvoted 1 times

 **zellck** 1 year, 4 months ago

**Selected Answer: C**

C is the answer.

<https://cloud.google.com/storage/docs/retry-strategy#exponential-backoff>

Truncated exponential backoff is a standard error handling strategy for network applications in which a client periodically retries a failed request with increasing delays between requests.

An exponential backoff algorithm retries requests exponentially, increasing the waiting time between retries up to a maximum backoff time.  
upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: C**

C is correct

upvoted 2 times

 **Blueocean** 2 years, 3 months ago

Agree with Option C

upvoted 4 times

 **scaenruy** 2 years, 3 months ago

I vote C

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

upvoted 3 times

Question #94

Topic 1

You need to redesign the ingestion of audit events from your authentication service to allow it to handle a large increase in traffic. Currently, the audit service and the authentication system run in the same Compute Engine virtual machine. You plan to use the following Google Cloud tools in the new architecture:

- ☞ Multiple Compute Engine machines, each running an instance of the authentication service
- ☞ Multiple Compute Engine machines, each running an instance of the audit service
- ☞ Pub/Sub to send the events from the authentication services.

How should you set up the topics and subscriptions to ensure that the system can handle a large volume of messages and can scale efficiently?

- A. Create one Pub/Sub topic. Create one pull subscription to allow the audit services to share the messages.
- B. Create one Pub/Sub topic. Create one pull subscription per audit service instance to allow the services to share the messages.
- C. Create one Pub/Sub topic. Create one push subscription with the endpoint pointing to a load balancer in front of the audit services.
- D. Create one Pub/Sub topic per authentication service. Create one pull subscription per topic to be used by one audit service.
- E. Create one Pub/Sub topic per authentication service. Create one push subscription per topic, with the endpoint pointing to one audit service.

**Correct Answer: D**

### Community vote distribution

A (92%)

8%

✉ **gfr892** Highly Voted 2 years, 3 months ago

<https://cloud.google.com/pubsub/docs/subscriber>

"Multiple subscribers can make pull calls to the same "shared" subscription. Each subscriber will receive a subset of the messages." Response is A.

With C and D you can't scale efficiently, because you have to create a topic for each new instance of the authentication service.

upvoted 12 times

✉ **akshaychavan7** 1 year, 8 months ago

This seems to be a smart answer and follows the logic with which I was thinking.

upvoted 1 times

✉ **telp** Highly Voted 1 year, 3 months ago

**Selected Answer: A**

A is correct. This is the most flexible way to scale, allowing the authentication and audit services to be sized independently according to load.

B is incorrect. This will cause messages to be duplicated, one copy per subscription.

C is incorrect. This will allow the system to scale, but push subscriptions are less suited to handle large volumes of messages.

D is incorrect. This will allow the system to scale, however each audit service will listen to all subscriptions.

E. is incorrect. This will allow the system to scale, however it will require each audit service to listen to all subscriptions. Also push subscriptions are less suited to handle large volumes of messages.

upvoted 5 times

✉ **Aeglas** Most Recent 5 months, 1 week ago

**Selected Answer: A**

Most simple and efficient one is A

upvoted 1 times

✉ **braska** 5 months, 1 week ago

**Selected Answer: E**

Option E is a more scalable and efficient solution for handling a large volume of messages and scaling efficiently.

upvoted 1 times

✉ **\_rajan\_** 7 months, 1 week ago

**Selected Answer: A**

I would go with A.

upvoted 1 times

✉ **Yochen** 7 months, 3 weeks ago

In my opinion, Option C would be the most efficient way to handle the scenario. Here's why:

Single Topic: Having one Pub/Sub topic keeps things simpler and allows all authentication service instances to publish to the same topic.

Push Subscription with Load Balancer: This allows incoming messages to be distributed among all available audit service instances. The load balancer would handle distributing the load, making it easier for the audit service to scale out as needed.

Option C ensures both scalability and efficient handling of a large volume of messages.

upvoted 1 times

✉ **closer89** 11 months, 3 weeks ago

**Selected Answer: A**

i go for A + custom pubsub metric on autoscale

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Answer is E, in which there is one topic per authentication service and one push subscription per topic, with the endpoint pointing to one audit service, is a better option because it allows the audit services to scale horizontally to handle a large volume of messages, and it allows the messages to be processed in parallel. Each authentication service will send messages directly to its own topic, which will be handled by a specific audit service. This will ensure that the system can scale horizontally to handle a large volume of messages, and it will also allow the audit services to process the messages in parallel.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

A, in which there is only one topic and one pull subscription, would not allow the audit services to scale horizontally to handle a large volume of messages, as they would all be pulling messages from the same subscription. If the volume of messages increased, the audit services would not be able to process them all in a timely manner, as they would be competing for messages from the same subscription.

B, in which there is only one topic and one pull subscription per audit service, would also not allow the audit services to scale horizontally, as they would all be pulling messages from the same topic

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

C, in which there is only one topic and one push subscription with a load balancer endpoint, would not allow the audit services to scale horizontally to handle a large volume of messages. The messages would all be sent to the same endpoint, which would be handled by the load balancer. If the volume of messages increased, the load balancer would not be able to distribute the messages to the audit services in a timely manner, as it would have to process all of the messages itself before forwarding them to the audit services. This could lead to bottlenecks if the volume of messages increased.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

D, in which there is one topic per authentication service and one pull subscription per topic, you may encounter issues with scaling efficiency as the number of authentication service instances increases. This is because you would have to create a new topic for each new instance of the authentication service, and each audit service would have to pull messages from a different topic. This would not allow the audit services to process the messages in parallel, as each audit service would be pulling messages from a different topic and processing them sequentially. This could lead to bottlenecks if the volume of messages increased.

upvoted 1 times

 **zellck** 1 year, 4 months ago

**Selected Answer: A**

A is the answer.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: A**

A is correct I think

upvoted 2 times

 **Blueocean** 2 years, 3 months ago

While this can be between C and D, I would go with Option D considering the large volume mentioned in question

upvoted 1 times

 **scaenrui** 2 years, 3 months ago

I vote C

upvoted 2 times

 **ParagSanyashiv** 2 years, 3 months ago

Agree with D

upvoted 2 times

You are developing a marquee stateless web application that will run on Google Cloud. The rate of the incoming user traffic is expected to be unpredictable, with no traffic on some days and large spikes on other days. You need the application to automatically scale up and down, and you need to minimize the cost associated with running the application. What should you do?

- A. Build the application in Python with Firestore as the database. Deploy the application to Cloud Run.
- B. Build the application in C# with Firestore as the database. Deploy the application to App Engine flexible environment.
- C. Build the application in Python with CloudSQL as the database. Deploy the application to App Engine standard environment.
- D. Build the application in Python with Firestore as the database. Deploy the application to a Compute Engine managed instance group with autoscaling.

**Correct Answer: C***Community vote distribution*

A (100%)

 **p4** Highly Voted 2 years, 3 months ago

Why C? I chose option A because of the DB option.

both Cloud run (A) and App Engine Standard (C) can scale to zero, so we need to find out the correct DB Firestore vs CloudSQL since we don't know any details if data structures require relational or noSQL, I'd go for Firestore because it is more flexible in scalability than CloudSQL, and also you only pay per storage usage + operations

upvoted 11 times

 **closer89** 1 year ago

"you need to minimize the cost associated with running the application"

cloud run is cheaper, with 0.10 time granularity

upvoted 1 times

 **GCPCloudArchitectUser** Highly Voted 2 years, 2 months agoSelected Answer: A

I agree with A as it is the only one fits for scale up and down =

upvoted 6 times

 **alpha\_canary** Most Recent 1 week, 4 days agoSelected Answer: A

A: Building the application in Python with Firestore as the database and deploying the application to Cloud Run is a good approach. Cloud Run is designed to scale up and down automatically, even down to zero, which can help minimize costs when there's no traffic. Firestore is a serverless NoSQL document database that can scale automatically to meet your application's needs.

Why C is rejected?

C: While App Engine standard environment can scale down to zero instances, CloudSQL is not serverless and you are billed for the time that the database instance is running, which could increase costs when compared to Firestore.

upvoted 1 times

 **Aeglas** 5 months, 1 week agoSelected Answer: A

Also Firestore has a free tier quota

upvoted 1 times

 **braska** 5 months, 1 week agoSelected Answer: A

Option A is a suitable choice for building a stateless web application with unpredictable traffic, aiming to automatically scale up and down while minimizing costs

upvoted 1 times

👤 **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: A**

A is best suited here.

upvoted 1 times

👤 **[Removed]** 1 year, 2 months ago

**Selected Answer: A**

Both Cloud Run and App Engine Standard Environment allow scaling to zero (which minimize the cost), but Cloud SQL can't be minimized to zero while firestore is measured based on CPU usage.

So from the cost point of view, A is the answer

upvoted 1 times

👤 **omermahgoub** 1 year, 3 months ago

Answer is A: To minimize the cost of running the application and to allow it to automatically scale up and down based on incoming traffic, you should build the application in Python with Firestore as the database, and deploy it to Cloud Run.

B and C, which involve deploying the application to App Engine, may also allow the application to automatically scale, but they may not be as cost-effective as Cloud Run. Option D, which involves deploying the application to a Compute Engine managed instance group, would allow the application to automatically scale, but it would not be as cost-effective as Cloud Run, as you would have to pay for the resources that you use even when there is no traffic.

upvoted 2 times

👤 **zellck** 1 year, 4 months ago

**Selected Answer: A**

A is the answer.

upvoted 1 times

👤 **tomato123** 1 year, 8 months ago

**Selected Answer: A**

A is correct

upvoted 2 times

👤 **kinoko1330** 1 year, 8 months ago

**Selected Answer: A**

A because of "stateless web app"

upvoted 1 times

👤 **htakami** 2 years, 1 month ago

It's simple, we need a stateless web app (not relational DB as Cloud SQL), and sometimes it scales down to zero utilization (only GAE flex & Cloud Run can do this). I'll go with option A as well.

upvoted 1 times

👤 **htakami** 2 years, 1 month ago

And if you were wondering why not B, C# is not a supported language for GAE

upvoted 1 times

👤 **Kadhem** 5 months, 2 weeks ago

GAE flex don't scale to zero

upvoted 1 times

👤 **ESP\_SAP** 2 years, 1 month ago

Correct Answer is A;

They are talking about minimize cost, with Cloud SQL isn't cheaper than Firestore.

upvoted 1 times

👤 **Blueocean** 2 years, 3 months ago

Agree with Option C

upvoted 2 times

👤 **scaenruy** 2 years, 3 months ago

I vote C

upvoted 1 times

You have written a Cloud Function that accesses other Google Cloud resources. You want to secure the environment using the principle of least privilege. What should you do?

- A. Create a new service account that has Editor authority to access the resources. The deployer is given permission to get the access token.
- B. Create a new service account that has a custom IAM role to access the resources. The deployer is given permission to get the access token.
- C. Create a new service account that has Editor authority to access the resources. The deployer is given permission to act as the new service account.
- D. Create a new service account that has a custom IAM role to access the resources. The deployer is given permission to act as the new service account.

**Correct Answer: D**

Reference:

<https://cloud.google.com/blog/products/application-development/least-privilege-for-cloud-functions-using-cloud-iam>

*Community vote distribution*

D (89%)

11%

 **ParagSanyashiv** Highly Voted 2 years, 3 months ago

Agree with D

upvoted 7 times

 **alpha\_canary** Most Recent 1 week, 4 days ago

**Selected Answer: D**

<https://cloud.google.com/functions/docs/securing/function-identity#individual>  
upvoted 1 times

 **Xoxoo** 4 months ago

**Selected Answer: D**

Quoted from <https://cloud.google.com/functions/docs/securing/function-identity#individual>  
"In order to deploy a function with a user-managed service account, the deployer must have the iam.serviceAccounts.actAs permission on the service account being deployed"

upvoted 2 times

 **wanrltw** 5 months, 1 week ago

**Selected Answer: D**

<https://cloud.google.com/functions/docs/securing/function-identity#individual>  
upvoted 1 times

 **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: B**

This approach allows you to create a service account with a custom IAM role that provides only the necessary permissions required by your Cloud Function. By granting the deployer permission to get the access token, you ensure that they can obtain the necessary credentials to deploy and manage the Cloud Function.

upvoted 1 times

 **zellick** 1 year, 4 months ago

**Selected Answer: D**

D is the answer.

[https://cloud.google.com/functions/docs/securing/function-identity#per-function\\_identity](https://cloud.google.com/functions/docs/securing/function-identity#per-function_identity)

upvoted 2 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: D**

D is correct

upvoted 2 times

 **akshaychavan7** 1 year, 8 months ago

D should be the correct choice here.

In Google Cloud, the resource(which can be a Cloud Function, a VM, etc.) always acts as a service account while accessing other resources.

upvoted 1 times

 **[Removed]** 1 year, 11 months ago

What 'deployer' means here? The function itself? or the user who set up the function?

upvoted 1 times

 **[Removed]** 1 year, 11 months ago

B.

<https://cloud.google.com/functions/docs/securing/authenticating>

upvoted 1 times

 **[Removed]** 1 year, 11 months ago

Changed the mind to D. (the note above is when you \*invoke\* the function, not to access other GCP services).

<https://cloud.google.com/functions/docs/securing/function-identity>

"While IAM-defined service accounts are the preferred method for managing access in Google Cloud, some services might require other modes, such as an API key, OAuth 2.0 client, or service account key."

and

"Note: In order to deploy a function with a user-managed service account, the deployer must have the iam.serviceAccounts.actAs permission on the service account being deployed."

upvoted 4 times

Question #97

Topic 1

You are a SaaS provider deploying dedicated blogging software to customers in your Google Kubernetes Engine (GKE) cluster. You want to configure a secure multi-tenant platform to ensure that each customer has access to only their own blog and can't affect the workloads of other customers. What should you do?

- A. Enable Application-layer Secrets on the GKE cluster to protect the cluster.
- B. Deploy a namespace per tenant and use Network Policies in each blog deployment.
- C. Use GKE Audit Logging to identify malicious containers and delete them on discovery.
- D. Build a custom image of the blogging software and use Binary Authorization to prevent untrusted image deployments.

**Correct Answer: B**

Reference:

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

Community vote distribution

B (100%)

✉️  **Blueocean** Highly Voted 2 years, 3 months ago

Option B is correct  
<https://cloud.google.com/kubernetes-engine/docs/concepts/multitenancy-overview>  
upvoted 7 times

✉️  **\_rajan\_** Most Recent 7 months, 1 week ago

**Selected Answer: B**

This approach involves creating a separate namespace for each customer (tenant) and using Network Policies to enforce isolation between the namespaces. By deploying a namespace per tenant, you can ensure that each customer has access only to their own blog and cannot affect workloads of other customers.

upvoted 2 times

✉️  **maxdanny** 8 months ago

**Selected Answer: B**

<https://cloud.google.com/kubernetes-engine/docs/concepts/multitenancy-overview>  
upvoted 1 times

✉️  **zellick** 1 year, 4 months ago

**Selected Answer: B**

B is the answer.

[https://cloud.google.com/kubernetes-engine/docs/concepts/multitenancy-overview#what\\_is\\_multi-tenancy](https://cloud.google.com/kubernetes-engine/docs/concepts/multitenancy-overview#what_is_multi-tenancy)

Although Kubernetes cannot guarantee perfectly secure isolation between tenants, it does offer features that may be sufficient for specific use cases. You can separate each tenant and their Kubernetes resources into their own namespaces. You can then use policies to enforce tenant isolation. Policies are usually scoped by namespace and can be used to restrict API access, to constrain resource usage, and to restrict what containers are allowed to do.

upvoted 1 times

✉️  **ash\_meharun** 1 year, 5 months ago

<https://cloud.google.com/kubernetes-engine/docs/concepts/multitenancy-overview#:~:text=For%20example%2C%20a,the%20cluster%20operates.>  
upvoted 1 times

✉️  **TNT87** 1 year, 5 months ago

[https://cloud.google.com/kubernetes-engine/docs/concepts/multitenancy-overview#network\\_policies](https://cloud.google.com/kubernetes-engine/docs/concepts/multitenancy-overview#network_policies)  
Answer B  
upvoted 1 times

✉️  **tomato123** 1 year, 8 months ago

**Selected Answer: B**

B is correct  
upvoted 2 times

✉️  **szl0144** 1 year, 11 months ago

B is correct  
upvoted 1 times

Question #98

Topic 1

You have decided to migrate your Compute Engine application to Google Kubernetes Engine. You need to build a container image and push it to Artifact Registry using Cloud Build. What should you do? (Choose two.)

- A. Run gcloud builds submit in the directory that contains the application source code.
- B. Run gcloud run deploy app-name --image gcr.io/\$PROJECT\_ID/app-name in the directory that contains the application source code.
- C. Run gcloud container images add-tag gcr.io/\$PROJECT\_ID/app-name gcr.io/\$PROJECT\_ID/app-name:latest in the directory that contains the application source code.

D. In the application source directory, create a file named cloudbuild.yaml that contains the following contents:

```
steps:  
- name: 'gcr.io/cloud-builders/docker'  
  args: ['build', '-t', 'gcr.io/$PROJECT_ID/app-name', '.']  
- name: 'gcr.io/cloud-builders/docker'  
  args: ['push', 'gcr.io/$PROJECT_ID/app-name']
```

E. In the application source directory, create a file named cloudbuild.yaml that contains the following contents:

```
steps:  
- name: 'gcr.io/cloud-builders/gcloud'  
  args: ['app', 'deploy']  
  timeout: '1600s'
```

**Correct Answer: BD**

*Community vote distribution*

AD (100%)

 **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: AD**

I will go with AD.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

To build a container image and push it to Artifact Registry using Cloud Build, you should:

Run gcloud builds submit in the directory that contains the application source code. This command will trigger Cloud Build to build the container image and push it to Artifact Registry.

In the application source directory, create a file named cloudbuild.yaml that contains the instructions for building and pushing the container image. The file should contain the following steps:

steps:

```
-name: 'gcr.io/cloud-builders/docker'  
args: ['build', '-t', 'gcr.io/$PROJECT_ID/app-name', '.']  
-name: 'gcr.io/cloud-builders/docker'  
args: ['push', 'gcr.io/$PROJECT_ID/app-name']
```

This file will be used by Cloud Build to build and push the container image.

upvoted 2 times

 **omermahgoub** 1 year, 3 months ago

B is incorrect because it uses the gcloud run deploy command, which is used to deploy a container image to Cloud Run, not to Artifact Registry.

C is incorrect because it uses the gcloud container images add-tag command, which is used to add a tag to an existing container image in Container Registry, not to build and push a new container image to Artifact Registry.

E is incorrect because it uses the gcloud app deploy command, which is used to deploy an application to App Engine, not to build and push a container image to Artifact Registry.

upvoted 2 times

 **zellck** 1 year, 4 months ago

**Selected Answer: AD**

AD is the answer.

<https://cloud.google.com/build/docs/building/build-containers#store-images>

upvoted 2 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: AD**

AD are correct

upvoted 2 times

✉  **kinoko1330** 1 year, 8 months ago

**Selected Answer: AD**

<https://cloud.google.com/build/docs/building/build-containers>

upvoted 2 times

✉  **akshaychavan7** 1 year, 8 months ago

**Selected Answer: AD**

Yup, it's A and D

upvoted 1 times

✉  **GoReplyGCPExam** 1 year, 11 months ago

**Selected Answer: AD**

agree with AD

upvoted 2 times

✉  **p4** 2 years, 3 months ago

**Selected Answer: AD**

A to submit cloud build <https://cloud.google.com/sdk/gcloud/reference/builds/submit>

D describes the cloud build steps (docker build + push)

upvoted 3 times

✉  **p4** 2 years, 3 months ago

did anybody notice that D has container URLs "gcr.io", which is container registry, not artifact registry?  
not saying that there isn't a better alternative though

upvoted 1 times

✉  **p4** 2 years, 3 months ago

ok seems it is now possible to use such domains (preview feature)

<https://cloud.google.com/artifact-registry/docs/transition/setup-gcr-repo>

upvoted 1 times

✉  **Blueocean** 2 years, 3 months ago

Agree with Option B and D

upvoted 1 times

✉  **Blueocean** 2 years, 3 months ago

On further analysis Option A seems better than B as per this site . Correct options are A and D.

<https://cloud.google.com/artifact-registry/docs/configure-cloud-build>

upvoted 2 times

✉  **scaenrui** 2 years, 3 months ago

I vote A, D

upvoted 3 times

✉  **ParagSanyashiv** 2 years, 3 months ago

D is correct, but I am confused between B and C, because question says about creating the container using cloud build, while option B states about the cloud run deployment.

upvoted 1 times

✉  **ParagSanyashiv** 2 years, 3 months ago

B seems more correct. B and D are more suitable

upvoted 1 times

You are developing an internal application that will allow employees to organize community events within your company. You deployed your application on a single Compute Engine instance. Your company uses Google Workspace (formerly G Suite), and you need to ensure that the company employees can authenticate to the application from anywhere. What should you do?

- A. Add a public IP address to your instance, and restrict access to the instance using firewall rules. Allow your company's proxy as the only source IP address.
- B. Add an HTTP(S) load balancer in front of the instance, and set up Identity-Aware Proxy (IAP). Configure the IAP settings to allow your company domain to access the website.
- C. Set up a VPN tunnel between your company network and your instance's VPC location on Google Cloud. Configure the required firewall rules and routing information to both the on-premises and Google Cloud networks.
- D. Add a public IP address to your instance, and allow traffic from the internet. Generate a random hash, and create a subdomain that includes this hash and points to your instance. Distribute this DNS address to your company's employees.

**Correct Answer: C**

*Community vote distribution*

B (100%)

 **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: B**

B is correct.

upvoted 1 times

 **zelliCK** 1 year, 4 months ago

**Selected Answer: B**

B is the answer.

[https://cloud.google.com/iap/docs/concepts-overview#how\\_iap\\_works](https://cloud.google.com/iap/docs/concepts-overview#how_iap_works)

When an application or resource is protected by IAP, it can only be accessed through the proxy by principals, also known as users, who have correct Identity and Access Management (IAM) roles. When you grant a user access to an application or resources by IAP, they're subject to the

Question #100

Topic 1

Your development team is using Cloud Build to promote a Node.js application built on App Engine from your staging environment to production. The application relies on several directories of photos stored in a Cloud Storage bucket named webphotos-staging in the staging environment. After the promotion, these photos must be available in a Cloud Storage bucket named webphotos-prod in the production environment. You want to automate the process where possible. What should you do?

- A. Manually copy the photos to webphotos-prod.
- B. Add a startup script in the application's app.yaml file to move the photos from webphotos-staging to webphotos-prod.
- C. Add a build step in the cloudbuild.yaml file before the promotion step with the arguments:  

```
- name: gcr.io/cloud-builders/gsutil
  args: ['cp', '-r', 'gs://webphotos-staging',
         'gs://webphotos-prod']
  waitFor: ['-']
```
- D. Add a build step in the cloudbuild.yaml file before the promotion step with the arguments:  

```
- name: gcr.io/cloud-builders/gcloud
  args: ['cp', '-A', 'gs://webphotos-staging',
         'gs://webphotos-prod']
  waitFor: ['-']
```

**Correct Answer: C**

*Community vote distribution*

C (100%)

 **omermahgoub** 1 year, 3 months ago

C.Add a build step in the cloudbuild.yaml file before the promotion step with the arguments:

```
-name: gcr.io/cloud-builders/gsutil  
args: ['cp','-r','gs://webphotos-staging','gs://webphotos-prod']  
waitFor: ['-']
```

You should add a build step in the cloudbuild.yaml file before the promotion step with the arguments shown above. This build step will use the gsutil tool to copy the photos from the webphotos-staging bucket to the webphotos-prod bucket. The -r flag tells gsutil to copy all files in the bucket recursively, and the waitFor parameter tells Cloud Build to wait for this step to complete before continuing with the promotion step.

upvoted 3 times

 **zelick** 1 year, 4 months ago

**Selected Answer: C**

C is the answer.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: C**

C is correct

upvoted 2 times

 **nehaxlpb** 1 year, 9 months ago

**Selected Answer: C**

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

upvoted 1 times

 **Blueocean** 2 years, 3 months ago

Agree with Option C

upvoted 3 times

 **ParagSanyashiv** 2 years, 3 months ago

Agree with C

upvoted 2 times

Question #101

Topic 1

You are developing a web application that will be accessible over both HTTP and HTTPS and will run on Compute Engine instances. On occasion, you will need to SSH from your remote laptop into one of the Compute Engine instances to conduct maintenance on the app. How should you configure the instances while following Google-recommended best practices?

- A. Set up a backend with Compute Engine web server instances with a private IP address behind a TCP proxy load balancer.
- B. Configure the firewall rules to allow all ingress traffic to connect to the Compute Engine web servers, with each server having a unique external IP address.
- C. Configure Cloud Identity-Aware Proxy API for SSH access. Then configure the Compute Engine servers with private IP addresses behind an HTTP(s) load balancer for the application web traffic.
- D. Set up a backend with Compute Engine web server instances with a private IP address behind an HTTP(S) load balancer. Set up a bastion host with a public IP address and open firewall ports. Connect to the web instances using the bastion host.

**Correct Answer: C**

Reference:

[https://cloud.google.com/compute/docs/instances/connecting-advanced#cloud\\_iap](https://cloud.google.com/compute/docs/instances/connecting-advanced#cloud_iap)

*Community vote distribution*

C (90%)

10%

✉  **kostol** 7 months, 1 week ago

**Selected Answer: D**

VM can only connect through IAM with public IP so C wouldn't work  
bastion host is one of options instead - <https://cloud.google.com/compute/docs/connect/ssh-internal-ip>  
upvoted 1 times

✉  **wanrltw** 5 months, 1 week ago

"This document describes how to connect to a virtual machine (VM) instance through its internal IP address, using Identity-Aware Proxy (IAP) TCP forwarding."  
<https://cloud.google.com/compute/docs/connect/ssh-using-iap>  
upvoted 1 times

✉  **\_rajan\_** 7 months, 1 week ago

**Selected Answer: C**

C is correct  
upvoted 1 times

✉  **closer89** 1 year ago

i go for C  
<https://cloud.google.com/compute/docs/connect/ssh-using-iap>

IAP TCP forwarding enables you to establish an encrypted tunnel over which you can forward SSH connections to VMs. When you connect to a VM that uses IAP, IAP wraps the SSH connection inside HTTPS before forwarding the connection to the VM. Then, IAP checks if the user has the required IAM permissions and if they do, grants access to the VM.

If you need to connect to a VM that doesn't have external IP addresses and you can't use IAP, review the other methods listed in Connection options for internal-only VMs.

upvoted 1 times

✉  **closer89** 1 year ago

D is wrong.  
Bastion host VMs You have a specific use case, like session recording, and you can't use IAP  
upvoted 1 times

✉  **Pime13** 1 year, 2 months ago

**Selected Answer: C**

i would choose C: [https://medium.com/@larry\\_nguyen/use-identity-aware-proxy-iap-instead-of-bastion-host-to-connect-to-private-virtual-machines-in-9885bc7c12dd](https://medium.com/@larry_nguyen/use-identity-aware-proxy-iap-instead-of-bastion-host-to-connect-to-private-virtual-machines-in-9885bc7c12dd)  
upvoted 1 times

✉  **omermahgoub** 1 year, 3 months ago

D. is a recommended way to configure the instances while following Google-recommended best practices.

This approach provides several benefits:

The web server instances are only accessible through the load balancer and not directly via their private IP addresses, which improves security. The bastion host acts as a secure jump box that allows you to SSH into the web server instances, while only allowing incoming SSH connections on a specific IP address (the bastion host's public IP).

The firewall rules on the web server instances can be configured to only allow connections from the bastion host's IP, further reducing the attack surface.

It is a more recommended to have a bastion host that is authorized by your organization to connect to private instances this way it can provide better security to your instances. And also in terms of compliance, it will also follow the best practices of your organization.

upvoted 3 times

✉  **omermahgoub** 1 year, 3 months ago

C is a valid approach, but it may not be the best option for all use cases.

Cloud IAP allows you to control access to resources in your project by using identity and access management (IAM) roles, which is a good way to secure SSH access. However, this option does not address the issue of securing incoming web traffic, which is a separate concern. Configuring the servers with private IP addresses behind an HTTP(s) load balancer would help with securing the web traffic, but it does not provide an additional layer of security for SSH access. Additionally, it does not have the concept of secure jump host, which is a security best practice in protecting your instances from unwanted incoming connections.

upvoted 3 times

👤 **zelick** 1 year, 4 months ago

Selected Answer: C

C is the answer.

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

upvoted 1 times

👤 **TNT87** 1 year, 5 months ago

Selected Answer: C

[https://cloud.google.com/solutions/connecting-securely#storing\\_host\\_keys\\_by\\_enabling\\_guest\\_attributes](https://cloud.google.com/solutions/connecting-securely#storing_host_keys_by_enabling_guest_attributes)

Answer C

upvoted 2 times

👤 **tomato123** 1 year, 8 months ago

Selected Answer: C

C is correct

upvoted 2 times

👤 **akshaychavan7** 1 year, 8 months ago

Selected Answer: C

I feel both C and D are correct for this scenario.

The only reason I would go with option C is that it would be easier to set up than setting up a bastion host.

upvoted 1 times

👤 **nehaxlpb** 1 year, 9 months ago

Selected Answer: C

With TCP forwarding, IAP can protect SSH and RDP access to your VMs hosted on Google Cloud. Your VM instances don't even need public addresses.

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

upvoted 1 times

👤 **szl0144** 1 year, 11 months ago

C is my answer, guys

upvoted 2 times

👤 **s7an** 1 year, 11 months ago

D should be the answer (<https://cloud.google.com/solutions/connecting-securely#external>) But the bastion host should also be protected by I

upvoted 2 times

👤 **GoReplyGCPExam** 1 year, 11 months ago

C should be correct ([https://cloud.google.com/iap/docs/using-tcp-forwarding#tunneling\\_ssh\\_connections](https://cloud.google.com/iap/docs/using-tcp-forwarding#tunneling_ssh_connections))

upvoted 1 times

👤 **dishum** 2 years ago

Ans is D

upvoted 2 times

👤 **dishum** 1 year, 11 months ago

<https://cloud.google.com/solutions/connecting-securely#external>

upvoted 1 times

👤 **scaenrui** 2 years, 3 months ago

I vote C

upvoted 4 times

You have a mixture of packaged and internally developed applications hosted on a Compute Engine instance that is running Linux. These applications write log records as text in local files. You want the logs to be written to Cloud Logging. What should you do?

- A. Pipe the content of the files to the Linux Syslog daemon.
- B. Install a Google version of fluentd on the Compute Engine instance.
- C. Install a Google version of collectd on the Compute Engine instance.
- D. Using cron, schedule a job to copy the log files to Cloud Storage once a day.

**Correct Answer: B**

Reference:

<https://cloud.google.com/logging/docs/agent/logging/configuration>

*Community vote distribution*

B (100%)

 **GCPCloudArchitectUser** Highly Voted 2 years, 2 months ago

**Selected Answer: B**

Collectd is used for Monitoring agents

Fluentd is for cloud logging agent

upvoted 8 times

 **ParagSanyashiv** Highly Voted 2 years, 3 months ago

Agree with B

upvoted 7 times

 **zelick** Most Recent 1 year, 4 months ago

**Selected Answer: B**

B is the answer.

<https://cloud.google.com/stackdriver/docs/solutions/agents/ops-agent>

The Ops Agent is the primary agent for collecting telemetry from your Compute Engine instances. Combining logging and metrics into a single agent, the Ops Agent uses Fluent Bit for logs, which supports high-throughput logging, and the OpenTelemetry Collector for metrics.

You can configure the Ops Agent to support parsing of log files from third-party applications.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: B**

B is correct

upvoted 4 times

You want to create `fully baked` or `golden` Compute Engine images for your application. You need to bootstrap your application to connect to the appropriate database according to the environment the application is running on (test, staging, production). What should you do?

- A. Embed the appropriate database connection string in the image. Create a different image for each environment.
- B. When creating the Compute Engine instance, add a tag with the name of the database to be connected. In your application, query the Compute Engine API to pull the tags for the current instance, and use the tag to construct the appropriate database connection string.
- C. When creating the Compute Engine instance, create a metadata item with a key of `DATABASE` and a value for the appropriate database connection string. In your application, read the `DATABASE` environment variable, and use the value to connect to the appropriate database.
- D. When creating the Compute Engine instance, create a metadata item with a key of `DATABASE` and a value for the appropriate database connection string. In your application, query the metadata server for the `DATABASE` value, and use the value to connect to the appropriate database.

**Correct Answer: C**

*Community vote distribution*

D (100%)

✉  **HotSpa27** Highly Voted 2 years, 3 months ago

I vote D.

<https://cloud.google.com/compute/docs/metadata/querying-metadata>

upvoted 6 times

✉  **omermahgoub** Most Recent 1 year, 3 months ago

D. When creating the Compute Engine instance, create a metadata item with a key of "DATABASE" and a value for the appropriate database connection string. In your application, query the metadata server for the "DATABASE" value, and use the value to connect to the appropriate database.

This approach allows you to create a single golden image that is agnostic to the environment it is running in, while still allowing the appropriate database connection to be set at runtime. The metadata item is stored with the instance, so it can be read by your application at any time. Th

Question #104

Topic 1

th

You are developing a microservice-based application that will be deployed on a Google Kubernetes Engine cluster. The application needs to read and write to a

Spanner database. You want to follow security best practices while minimizing code changes. How should you configure your application to retrieve Spanner credentials?

- A. Configure the appropriate service accounts, and use Workload Identity to run the pods.
- B. Store the application credentials as Kubernetes Secrets, and expose them as environment variables.
- C. Configure the appropriate routing rules, and use a VPC-native cluster to directly connect to the database.
- D. Store the application credentials using Cloud Key Management Service, and retrieve them whenever a database connection is made.

**Correct Answer: B**

Reference:

<https://cloud.google.com/sql/docs/mysql/connect-kubernetes-engine>

*Community vote distribution*

A (77%)

B (23%)

✉  **kinoko1330** Highly Voted 1 year, 8 months ago

**Selected Answer: A**

<https://cloud.google.com/blog/products/containers-kubernetes/introducing-workload-identity-better-authentication-for-your-gke-applications>

A Cloud IAM service account is an identity that an application can use to make requests to Google APIs. As an application developer, you can generate individual IAM service accounts for each application, and then download and store the keys as a Kubernetes secret that you manually rotate. Not only is this process burdensome, but service account keys only expire every 10 years (or until you manually rotate them). In the case of a breach or compromise, an unaccounted-for key could mean prolonged access for an attacker. This potential blind spot, plus the management overhead of key inventory and rotation, makes using service account keys as secrets a less than ideal method for authenticating GKE workloads.

upvoted 8 times

✉  **alex8081** 1 year, 8 months ago

Exact...

and it's a recent alternative to secrets ... why would google want you to ignore it? :)

upvoted 2 times

✉  **htakami** Highly Voted 2 years, 1 month ago

I assume that nobody read through the official docs and GCP Best practices for K8s and Cloud SQL.

<https://cloud.google.com/sql/docs/mysql/connect-kubernetes-engine#secrets>

"A database credentials Secret includes the name of the database user you are connecting as, and the user's database password."

The best answer here is B, having K8s Secrets is the go-to method to configure and store sensitive information within a cluster such as Spanner credentials

upvoted 5 times

 **braska** Most Recent 5 months, 1 week ago

**Selected Answer: A**

Option A is the recommended approach for securely configuring your microservice-based application to retrieve Spanner credentials on Google Kubernetes Engine (GKE)

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: A**

This approach involves configuring service accounts with the necessary permissions to access the Spanner database. By using Workload Identity, you can associate these service accounts with your Kubernetes Engine pods, allowing them to authenticate and retrieve Spanner credentials automatically.

upvoted 2 times

 **closer89** 1 year ago

**Selected Answer: B**

i go for B

question is about how to RETRIEVE db creds

<https://cloud.google.com/sql/docs/mysql/connect-kubernetes-engine#secrets>

A is about how to connect to spanner

upvoted 1 times

 **[Removed]** 1 year, 2 months ago

**Selected Answer: A**

Google recommends using service accounts and work load identity whenever possible

upvoted 2 times

 **felipeschossler** 1 year ago

Exactly!

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

A. Configure the appropriate service accounts, and use Workload Identity to run the pods.

Workload Identity is a way to associate Kubernetes service accounts with Google Cloud IAM service accounts, allowing your pods to authenticate to Google Cloud services using their IAM identity. This means that you don't have to store application credentials in your code or Kubernetes Secrets, and you can manage the permissions of your application in Google Cloud IAM.

You would need to create service account in cloud IAM and a Kubernetes service account and then map them to use Workload Identity. You can also use gcloud command line to map the Kubernetes service account to the desired IAM service account. Then in your application, can use the Kubernetes service account to authenticate to Spanner, which will authenticate as the mapped IAM service account.

This way you don't have to hardcode credentials in your code, and you can easily manage the permissions of your application using Google Cloud IAM.

upvoted 1 times

 **zellick** 1 year, 4 months ago

**Selected Answer: A**

A is the answer.

[https://cloud.google.com/kubernetes-engine/docs/concepts/workload-identity#what\\_is](https://cloud.google.com/kubernetes-engine/docs/concepts/workload-identity#what_is)

Applications running on GKE might need access to Google Cloud APIs such as Compute Engine API, BigQuery Storage API, or Machine Learning APIs.

Workload Identity allows a Kubernetes service account in your GKE cluster to act as an IAM service account. Pods that use the configured Kubernetes service account automatically authenticate as the IAM service account when accessing Google Cloud APIs. Using Workload Identity allows you to assign distinct, fine-grained identities and authorization for each application in your cluster.

upvoted 1 times

 **TNT87** 1 year, 5 months ago

**Selected Answer: A**

Answer is A

Store the application credentials as Kubernetes Secrets, and expose them as environment variables

upvoted 2 times

 **TNT87** 1 year, 5 months ago

Sorry i dwant to paste the link to A, not answer B. B is wrong.

<https://kubernetes.io/docs/concepts/configuration/secret/#alternatives-to-secrets>

Answer A

upvoted 1 times

 **TNT87** 1 year, 5 months ago

It cant be B because

Because Secrets can be created independently of the Pods that use them, there is less risk of the Secret (and its data) being exposed during the workflow of creating, viewing, and editing Pods. Kubernetes, and applications that run in your cluster, can also take additional precautions with Secrets, such as avoiding writing secret data to nonvolatile storage.

Secrets are similar to ConfigMaps but are specifically intended to hold confidential data.

Caution:

Kubernetes Secrets are, by default, stored unencrypted in the API server's underlying data store (etcd). Anyone with API access can retrieve or modify a Secret, and so can anyone with access to etcd. Additionally, anyone who is authorized to create a Pod in a namespace can use that access to read any Secret in that namespace; this includes indirect access such as the ability to create a Deployment.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: A**

I think A is correct

upvoted 4 times

 **nehaxlpb** 1 year, 9 months ago

**Selected Answer: A**

A and B ,both are correct. Currenly in my project we are using A for allowing pods to query Bigquery. So A and B both seems to be correct.

upvoted 1 times

 **akshaychavan7** 1 year, 8 months ago

A service account will only allow you to establish your workload identity(basically authenticate the identity of your cluster pods). But, in order to establish a database connection, you would need to connect it using the DB credentials( like host, user id, password, and database name to connect to). To securely store such credentials, Google recommends using a Secret Manager. So the answer would be l

upvoted 1 times

 **[Removed]** 1 year, 11 months ago

**Selected Answer: B**

B.

The question is not about how to connect/access Cloud Spanner, but is how to "retrieve Spanner \*credentials\*".

upvoted 3 times

 **brewpike** 1 year, 11 months ago

A and B -> It should be select 2 best options question.

upvoted 1 times

 **americoleonardo** 1 year, 11 months ago

**Selected Answer: B**

I think B is more suitable in this situation

upvoted 3 times

 **GCPCloudArchitectUser** 2 years, 2 months ago

**Selected Answer: A**

Yes A is the option

upvoted 2 times

 **scaenruy** 2 years, 3 months ago

I vote A

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

upvoted 4 times

 **Blueocean** 2 years, 3 months ago

Yes could be Option A , also Option B could work, not sure if Option B is not right considering the question states minimum code changes  
upvoted 1 times

 **juancambb** 2 years, 1 month ago

yes is better b

upvoted 1 times

Question #105

*Topic 1*

You are deploying your application on a Compute Engine instance that communicates with Cloud SQL. You will use Cloud SQL Proxy to allow your application to communicate to the database using the service account associated with the application's instance. You want to follow the Google-recommended best practice of providing minimum access for the role assigned to the service account. What should you do?

- A. Assign the Project Editor role.
- B. Assign the Project Owner role.
- C. Assign the Cloud SQL Client role.
- D. Assign the Cloud SQL Editor role.

**Correct Answer: C**

Reference:

<https://cloud.google.com/sql/docs/mysql/sql-proxy>

*Community vote distribution*

C (100%)

 **scaenruy** Highly Voted 2 years, 3 months ago

I vote C

<https://cloud.google.com/sql/docs/mysql/roles-and-permissions>

upvoted 6 times

 **alpha\_canary** Most Recent 1 week, 4 days ago

**Selected Answer: C**

[https://cloud.google.com/sql/docs/mysql/roles-and-permissions#:~:text=When%20you%20use%20an%20account%20to%20connect%20to%20a%20Cloud%20SQL%20instance%2C%20the%20account%20must%20have%20the%20Cloud%20SQL%20%3E%20Client%20role%20\(roles/cloudsql.client\)%2C%20which%20includes%20permissions%20required%20for%20connecting.](https://cloud.google.com/sql/docs/mysql/roles-and-permissions#:~:text=When%20you%20use%20an%20account%20to%20connect%20to%20a%20Cloud%20SQL%20instance%2C%20the%20account%20must%20have%20the%20Cloud%20SQL%20%3E%20Client%20role%20(roles/cloudsql.client)%2C%20which%20includes%20permissions%20required%20for%20connecting.)

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: C**

Cloud SQL Client role: This role provides the necessary permissions to interact with Cloud SQL while minimizing access to other resources.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

C. Assign the Cloud SQL Client role.

The Cloud SQL Client role has the minimal set of permissions required to access Cloud SQL instances. This role includes permissions to connect to and use a Cloud SQL instance, but it doesn't include permissions to create, delete or manage the instance itself. This role should be granted to the service account associated with your Compute Engine instance, in order to allow your application to connect to the Cloud SQL instance using the Cloud SQL Proxy.

You can assign the Cloud SQL Client role to a service account by using the Cloud Console, the gcloud command-line tool, or the Cloud Identity and Access Management (IAM) API. Once the role is assigned, your application will be able to authenticate to Cloud SQL using the service account and the Cloud SQL Proxy.

Question #106

Topic 1

Your team develops stateless services that run on Google Kubernetes Engine (GKE). You need to deploy a new service that will only be accessed by other services running in the GKE cluster. The service will need to scale as quickly as possible to respond to changing load. What should you do?

- A. Use a Vertical Pod Autoscaler to scale the containers, and expose them via a ClusterIP Service.
- B. Use a Vertical Pod Autoscaler to scale the containers, and expose them via a NodePort Service.
- C. Use a Horizontal Pod Autoscaler to scale the containers, and expose them via a ClusterIP Service.
- D. Use a Horizontal Pod Autoscaler to scale the containers, and expose them via a NodePort Service.

**Correct Answer: C**

*Community vote distribution*

C (100%)

 **plutonians123** 5 months ago

**Selected Answer: C**

Horizontal Pod Autoscaler (HPA) scales the number of pod replicas based on CPU usage or other select metrics, which is suitable for quick scaling with load changes. ClusterIP is appropriate for services only accessible within the cluster. This combination seems to meet all the requirements.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: C**

HPA automatically scales the number of pods in a deployment based on CPU utilization or other custom metrics. By using HPA, you can ensure that your service scales quickly to respond to changing load while minimizing manual intervention. Exposing the service via a ClusterIP Service allows other services running in the GKE cluster to access it securely without exposing it to the public internet.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

C. Use a Horizontal Pod Autoscaler to scale the containers, and expose them via a ClusterIP Service.

When dealing with services that are only accessed by other services in the same GKE cluster, it's usually best to use a ClusterIP Service. This type of service allows pods to be accessed by other pods within the cluster using their IP address, but doesn't expose them to the outside world.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

A Horizontal Pod Autoscaler is used to automatically scale the number of replicas of a deployment based on certain metrics. This is useful for scaling based on CPU utilization, memory usage, or custom metrics. By using a Horizontal Pod Autoscaler, you can respond quickly to changes in load by automatically creating or deleting replicas of your pods, so the service can handle the traffic.

You can expose the service via a ClusterIP Service by creating one in Kubernetes and configuring the selector to match the replicas running in your deployment. This allows other services to discover and communicate with your new service by its ClusterIP.

upvoted 1 times

 **zellick** 1 year, 4 months ago

**Selected Answer: C**

C is the answer.

[https://cloud.google.com/kubernetes-engine/docs/concepts/service#services\\_of\\_type\\_clusterip](https://cloud.google.com/kubernetes-engine/docs/concepts/service#services_of_type_clusterip)

When you create a Service of type ClusterIP, Kubernetes creates a stable IP address that is accessible from nodes in the cluster.

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

The Horizontal Pod Autoscaler changes the shape of your Kubernetes workload by automatically increasing or decreasing the number of Pod replicas in response to the workload's CPU or memory consumption, or in response to custom metrics reported from within Kubernetes or external monitoring sources outside of your cluster.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: C**

C is correct

upvoted 2 times

 **scaenrui** 2 years, 3 months ago

I vote C

unvoted 3 times

Question #107

Topic 1

You recently migrated a monolithic application to Google Cloud by breaking it down into microservices. One of the microservices is deployed using Cloud Functions. As you modernize the application, you make a change to the API of the service that is backward-incompatible. You need to support both existing callers who use the original API and new callers who use the new API. What should you do?

- A. Leave the original Cloud Function as-is and deploy a second Cloud Function with the new API. Use a load balancer to distribute calls between the versions.
- B. Leave the original Cloud Function as-is and deploy a second Cloud Function that includes only the changed API. Calls are automatically routed to the correct function.

- C. Leave the original Cloud Function as-is and deploy a second Cloud Function with the new API. Use Cloud Endpoints to provide an API gateway that exposes a versioned API.
- D. Re-deploy the Cloud Function after making code changes to support the new API. Requests for both versions of the API are fulfilled based on a version identifier included in the call.

**Correct Answer:** C

Reference:

<https://cloud.google.com/endpoints/docs/openapi/get-started-cloud-functions>

*Community vote distribution*

C (93%)

7%

👤 GCPCloudArchitectUser Highly Voted 2 years, 2 months ago

Selected Answer: C

Based on the link ... where it says for backward incompatible strategy use two separate deployments/instances v1 and v2 and only C option is inline with the link

upvoted 7 times

👤 omermahgoub Most Recent 1 year, 3 months ago

Answer is C

When making backward-incompatible changes to an API, it's important to provide a way for existing callers to continue using the old API while

Question #108

Topic 1

You are developing an application that will allow users to read and post comments on news articles. You want to configure your application to store and display user-submitted comments using Firestore. How should you design the schema to support an unknown number of comments and articles?

- A. Store each comment in a subcollection of the article.
- B. Add each comment to an array property on the article.
- C. Store each comment in a document, and add the comment's key to an array property on the article.
- D. Store each comment in a document, and add the comment's key to an array property on the user profile.

Correct Answer: D

Community vote distribution

A (49%)

D (34%)

C (17%)

👤 p4 Highly Voted 2 years, 3 months ago

Selected: A

Firestore has a "hierarchical structure": collection contains documents, document can contain (sub)collections

D does not make sense bc why do you want to link comments to the user profile instead of the article?

<https://stackoverflow.com/questions/48634227/limitation-to-number-of-documents-under-one-collection-in-firebase-firestore>

"There is no documented limit to the number of documents that can be stored in a Cloud Firestore collection. The system is designed to scale huge data sets."

upvoted 21 times

👤 juancambb 2 years, 1 month ago

the subcollection has a limit of 1Mb of data, so for unknown number of comments is not valid, the answer is D

upvoted 1 times

👤 GoReplyGCPExam 1 year, 11 months ago

That's wrong, the 1MB limit it's on the document inside the subcollection (not on the subcollection itself).

"Document size - Cloud Firestore is optimized for small documents and enforces a 1MB size limit on documents. If your array can expand arbitrarily, it is better to use a subcollection, which has better scaling performance."

Check out also the example in the subcollections documentation, showing a rooms-messages hierarchy example.  
<https://firebase.google.com/docs/firestore/data-model#subcollections>

upvoted 6 times

👤 htakami Highly Voted 2 years, 1 month ago

Why D and not C? For my understanding, we need to keep a relation between the articles and their comments. I don't see how the user profile could come in handy... but please let me know if I misunderstood something. For me, Ans C makes more sense.

upvoted 9 times

 **alpha\_canary** Most Recent 1 week, 4 days ago

**Selected Answer: A**

It can't be D because:

Storing each comment in a document and adding the comment's key to an array property on the user profile wouldn't efficiently link comments to articles.

upvoted 1 times

 **Kadhem** 4 months, 1 week ago

**Selected Answer: D**

Answer is D in my opinion for "display user-submitted comments" and "unknown number of comments and articles"

upvoted 1 times

 **Aeglas** 5 months, 1 week ago

**Selected Answer: A**

Answer is A

upvoted 3 times

 **Aeglas** 5 months, 1 week ago

**Selected Answer: A**

As per previous comments also appointed, there is not such a limitation on size for a Subcollection, and it does not make sense to store the relation with User profile like answer D

upvoted 3 times

 **braska** 5 months, 1 week ago

**Selected Answer: A**

Option A is the recommended approach for structuring data in Firestore to support an unknown number of comments and articles. Firestore is a NoSQL document-oriented database, and using subcollections provides a flexible and scalable way to organize related data

upvoted 2 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: C**

I would go with C.

upvoted 1 times

 **sota\_hi\_there** 10 months ago

**Selected Answer: A**

the correct answer is A. reference: <https://firebase.google.com/docs/firestore/data-model>

upvoted 2 times

 **gc\_exam2022** 10 months, 3 weeks ago

Answer is D

upvoted 1 times

 **efrenpq** 11 months, 2 weeks ago

**Selected Answer: A**

Firestore has a "hierarchical structure"

upvoted 1 times

 **mrvergara** 1 year, 2 months ago

**Selected Answer: C**

It is recommended to add the comment document IDs to an array property on the corresponding article document, rather than on a user profile. This approach allows you to easily retrieve all comments for a specific article by querying the comments collection using the article ID and then filtering the results based on the IDs in the article's comments array.

Storing the comment IDs in the article document also avoids the need to make multiple read operations to retrieve the comments for a given article, which can be slow and increase latency.

For example, you could create an array property named "comments" in the article document and add the comment document IDs to this array every time a user submits a new comment for the article. This allows you to efficiently retrieve all comments for a given article by querying the comments collection and filtering based on the IDs in the article's "comments" array.

upvoted 1 times

 **chunker** 1 year, 3 months ago

**Selected Answer: A**

Close to this example: <https://firebase.google.com/docs/firestore/data-model#subcollections>

upvoted 2 times

 **felipeschossler** 1 year ago

Exactly this, thanks for sharing the docs here, I change my answer because of you!

upvoted 2 times

 **omermahgoub** 1 year, 3 months ago

Answer is A. Store each comment in a subcollection of the article, because it allows for easy scaling and querying of the comments as the data increases. With this approach, you can easily fetch the comments associated with an article by querying the subcollection of that article, instead of querying all the comments in a single collection. It also allows you to query specific comments and articles easily, since you have the reference to the specific article they are associated with.

upvoted 3 times

 **omermahgoub** 1 year, 3 months ago

Storing each comment in a document, and adding the comment's key to an array property on the user profile (Option D) would make it more difficult to fetch all the comments associated with a specific article. Additionally, it would also make it more difficult to query the comments and articles since you would have to go through the user profile to find the comment's key and then use that to find the comment's information. The subcollection approach allows for better organization and querying of the data, making it a better choice in this scenario.

upvoted 2 times

 **omermahgoub** 1 year, 3 months ago

C. Store each comment in a document, and add the comment's key to an array property on the article would work, but it may not be the best solution for this use case. While it would allow you to query for all the comments associated with an article by finding the document with the article and reading the array property of its key.

However, this approach would make it more difficult to scale the data as the number of comments grows, because it would require you to retrieve all the comment keys in the array of the article and then perform additional queries to retrieve the actual comment information one by one. This could slow down the application as the number of comments increase, and make it more difficult to handle high-load situations.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Another reason for not choosing C is that, it might also pose an issue for data consistency as comments can change over time and updating the comment document would not automatically update the array property on the article, creating inconsistencies in the data.

upvoted 1 times

 **TNT87** 1 year, 4 months ago

[https://firebase.google.com/docs/firestore/best-practices#high\\_read\\_write\\_and\\_delete\\_rates\\_to\\_a\\_narrow\\_document\\_range](https://firebase.google.com/docs/firestore/best-practices#high_read_write_and_delete_rates_to_a_narrow_document_range)

upvoted 1 times

 **zellck** 1 year, 4 months ago

**Selected Answer: D**

D is the answer.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: D**

D is correct I think

upvoted 2 times

Engine instance that doesn't have a public IP address. What should you do?

- A. Use Carrier Peering
- B. Use VPC Network Peering
- C. Use Shared VPC networks
- D. Use Private Google Access

**Correct Answer: C**

Reference:

<https://cloud.google.com/compute/docs/ip-addresses>

*Community vote distribution*

D (100%)

 **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: D**

Private Google Access allows your Compute Engine instances to access Google Cloud APIs and services without requiring a public IP address. It enables outbound connectivity to Google APIs and services using internal IP addresses.

upvoted 2 times

 **telp** 1 year, 3 months ago

**Selected Answer: D**

A is not correct because Carrier Peering enables you to access Google applications, such as Google Workspace, by using a service provider to obtain enterprise-grade network services that connect your infrastructure to Google.

B is not correct because VPC Network Peering enables you to peer VPC networks so that workloads in different VPC networks can communicate in a private RFC 1918 space. Traffic stays within Google's network and doesn't traverse the public internet.

C is not correct because Shared VPC allows an organization to connect resources from multiple projects to a common VPC network so that they can communicate with each other securely and efficiently using internal IPs from that network.

D is correct because Private Google Access is an option available for each subnetwork. When it is enabled, instances in the subnetwork can communicate with public Google API endpoints even if the instances don't have external IP addresses.

upvoted 4 times

 **omermahgoub** 1 year, 3 months ago

D. Use Private Google Access

Private Google Access is a feature that enables access to Google Cloud APIs and services for instances that don't have a public IP address. With this feature, you can allow your Compute Engine instances in a VPC network to access Google services over the private IP addresses, without the need for a NAT gateway or VPN.

This feature is especially useful when you want to access Google APIs and services from an instance that doesn't have internet access or a public IP address. In this case, you can enable Private Google Access on the VPC network that your Compute Engine instances belong to, and they will be able to call the Cloud Storage API using the private IP address.

To enable Private Google Access, you can use the gcloud command-line tool, the Cloud Console, or the REST API. This feature is also available for other services like BigQuery and Cloud SQL as well, to access them from instances without a public IP address.

upvoted 1 times

 **zelliCK** 1 year, 4 months ago

**Selected Answer: D**

D is the answer.

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

VM instances that only have internal IP addresses (no external IP addresses) can use Private Google Access. They can reach the external IP addresses of Google APIs and services. The source IP address of the packet can be the primary internal IP address of the network interface or an alias IP range that is assigned to the interface. If you disable Private Google Access, the VM instances can no longer reach Google APIs and services; they can only send traffic within the VPC network.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: D**

D is correct

upvoted 2 times

✉️  **akshaychavan7** 1 year, 8 months ago

**Selected Answer: D**

Yup, it's D.

upvoted 1 times

✉️  **GCPCloudArchitectUser** 2 years, 2 months ago

**Selected Answer: D**

I vote for D as well

upvoted 4 times

✉️  **scaenruiy** 2 years, 3 months ago

I vote D

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

upvoted 4 times

✉️  **Blueocean** 2 years, 3 months ago

Yes agree should be Option D

upvoted 1 times

Question #110

Topic 1

You are a developer working with the CI/CD team to troubleshoot a new feature that your team introduced. The CI/CD team used HashiCorp Packer to create a new Compute Engine image from your development branch. The image was successfully built, but is not booting up. You need to investigate the issue with the CI/CD team. What should you do?

- A. Create a new feature branch, and ask the build team to rebuild the image.
- B. Shut down the deployed virtual machine, export the disk, and then mount the disk locally to access the boot logs.
- C. Install Packer locally, build the Compute Engine image locally, and then run it in your personal Google Cloud project.
- D. Check Compute Engine OS logs using the serial port, and check the Cloud Logging logs to confirm access to the serial port.

**Correct Answer: C**

Reference:

<https://cloud.google.com/architecture/automated-build-images-with-jenkins-kubernetes>

*Community vote distribution*

D (100%)

✉️  **scaenruiy**  2 years, 3 months ago

I vote D

<https://cloud.google.com/compute/docs/troubleshooting/troubleshooting-using-serial-console>

upvoted 9 times

✉️  **Blueocean** 2 years, 3 months ago

Agree with Option D

upvoted 4 times

 **jnas** [Most Recent] 9 months, 1 week ago

**Selected Answer: D**

D is the answer - the other are too long.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: D**

Answer is D

If the Compute Engine image is not booting up, one of the first steps to troubleshoot the issue would be to check the OS logs to see what might be causing the problem. Compute Engine provides access to the serial console logs of a virtual machine, which can be accessed through the Cloud Console or the gcloud command-line tool. This will allow you to see the output of the virtual machine's boot process and identify any errors or issues that might be preventing it from starting up.

Additionally, you should also check the Cloud Logging logs to confirm that you have access to the serial port. It may be possible that the firewall rules or IAM permissions are blocking access to the serial port and causing the image not to boot. So, you should check the logs for any errors related to access or firewall rules.

By checking the OS logs and the Cloud Logging logs, you and the CI/CD team can get a better understanding of what might be causing the issue and take steps to fix it.

upvoted 2 times

 **zellck** 1 year, 4 months ago

**Selected Answer: D**

D is the answer.

[https://cloud.google.com/compute/docs/troubleshooting/vm-startup#identify\\_the\\_reason\\_why\\_the\\_boot\\_disk\\_isnt\\_booting](https://cloud.google.com/compute/docs/troubleshooting/vm-startup#identify_the_reason_why_the_boot_disk_isnt_booting)

Identify the reason why the boot disk isn't booting

- Examine your virtual machine instance's serial port output.

An instance's BIOS, bootloader, and kernel prints their debug messages into the instance's serial port output, providing valuable information about any errors or issues that the instance experienced. If you enable serial port output logging to Cloud Logging, you can access this information even when your instance is not running.

upvoted 1 times

 **ash\_meharun** 1 year, 4 months ago

In option D, what does it mean by "confirm access to the serial port"?

If I need to see the boot logs, then how the checking the access to serial port gonna help?

upvoted 1 times

 **TNT87** 1 year, 5 months ago

[https://cloud.google.com/compute/docs/troubleshooting/troubleshooting-using-serial-console#connecting\\_to\\_a\\_serial\\_console\\_with\\_a\\_login\\_prompt](https://cloud.google.com/compute/docs/troubleshooting/troubleshooting-using-serial-console#connecting_to_a_serial_console_with_a_login_prompt)

Answer D

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: D**

D is correct

upvoted 3 times

 **ParagSanyashiv** 2 years, 3 months ago

**Selected Answer: D**

D is more suitable

upvoted 3 times

 **GCPCloudArchitectUser** 2 years, 2 months ago

This is interesting to learn that if a compute engine isn't bootable and you can connect still

upvoted 4 times

You manage an application that runs in a Compute Engine instance. You also have multiple backend services executing in stand-alone Docker containers running in Compute Engine instances. The Compute Engine instances supporting the backend services are scaled by managed instance groups in multiple regions. You want your calling application to be loosely coupled. You need to be able to invoke distinct service implementations that are chosen based on the value of an HTTP header found in the request. Which Google Cloud feature should you use to invoke the backend services?

- A. Traffic Director
- B. Service Directory
- C. Anthos Service Mesh
- D. Internal HTTP(S) Load Balancing

**Correct Answer: D**

*Community vote distribution*

A (79%)

14%

7%

✉️  GoReplyGCPExam Highly Voted 1 year, 11 months ago

"the backend services are scaled by managed instance groups in multiple regions", the Internal load balancer is a regional service, so It's A in opinion.

- "An internal HTTP(S) load balancer routes internal traffic to the service running on the VM. Traffic Director works with Cloud Load Balancing provide a managed ingress experience. You set up an external or internal load balancer, and then configure that load balancer to send traffic to your microservices."

upvoted 9 times

✉️  alpha\_canary Most Recent 1 week, 4 days ago

**Selected Answer: A**

[https://cloud.google.com/traffic-director/docs/overview#traffic\\_management](https://cloud.google.com/traffic-director/docs/overview#traffic_management):~:text=Advanced%20traffic%20management%2C%20including%20routing%20and%20request%20manipulation%20(based%20on%20hostname%2C%20path%2C%20headers%2C%20cookies%2C%20and%20more)%2C%20enables%20you%20to%20determine%20how%20traffic%20flows%20between%20your%20services

upvoted 1 times

✉️  braska 5 months, 1 week ago

**Selected Answer: C**

Anthos Service Mesh is a service mesh solution that can be used to invoke distinct service implementations based on the value of an HTTP header in the request. It provides a platform-agnostic way to connect, manage, and secure microservices running on Google Cloud or other environments

upvoted 1 times

✉️  \_\_rajan\_\_ 7 months, 1 week ago

**Selected Answer: A**

Traffic Director is a Google Cloud feature that provides a global traffic management control plane for service mesh architectures. It allows you to configure and manage traffic routing across multiple services and environments.

upvoted 1 times

✉️  purushi 8 months, 3 weeks ago

I go for A: Traffic director is used to direct the traffic to services running in the different regions or within a region based on the HTTP header values.

upvoted 2 times

✉️  jnas 9 months, 1 week ago

**Selected Answer: A**

A as it's the only one that lets you route based on headers

upvoted 1 times

 closer89 1 year ago

**Selected Answer: A**

[https://cloud.google.com/traffic-director/docs/overview#traffic\\_management](https://cloud.google.com/traffic-director/docs/overview#traffic_management)

Advanced traffic management, including routing and request manipulation (based on hostname, path, headers, cookies, and more), enables you to determine how traffic flows between your services. You can also apply actions like retries, redirects, and weight-based traffic splitting for canary deployments. Advanced patterns like fault injection, traffic mirroring, and outlier detection enable DevOps use cases that improve your resiliency.

upvoted 1 times

 Pime13 1 year, 2 months ago

**Selected Answer: A**

A: <https://cloud.google.com/traffic-director/docs/set-up-gce-vms>

upvoted 1 times

 omermahgoub 1 year, 3 months ago

**Selected Answer: A**

Traffic Director provides global traffic management for service meshes and hybrid deployments. It allows you to configure routing rules based on the values of HTTP headers, so you can direct traffic to different service implementations based on the value of an HTTP header found in the request. With Traffic Director, you can route traffic to different services running in different regions, and it also supports automatic failover, so you can ensure high availability for your backend services.

In your case, you can configure Traffic Director to inspect the value of an HTTP header in the request, and then route the traffic to the appropriate service implementation running in different regions. This allows your application to invoke the backend services in a loosely coupled way, and ensures that the backend services can scale independently of the calling application.

upvoted 1 times

 omermahgoub 1 year, 3 months ago

It also works with MIGs to allow you to manage the scaling of the backend services in different regions, and the combination of Traffic Director and MIG allow you to provide service availability in multiple regions.

upvoted 1 times

 omermahgoub 1 year, 3 months ago

Option D, Internal HTTP(S) Load Balancing, is a feature that allows you to distribute incoming traffic to a group of instances in a Virtual Private Cloud (VPC) network. It works by creating a load balancer, and configuring it to forward traffic to the instances that you specify. This feature is useful for situations where you want to distribute traffic to multiple instances running in the same region.

However, in this scenario where you want to invoke distinct service implementations that are chosen based on the value of an HTTP header found in the request. The Internal HTTP(S) Load Balancer doesn't offer this type of feature. It typically directs traffic based on the IP or hostname and port, but it's not capable of inspecting the value of an HTTP header like Traffic Director does.

upvoted 1 times

 omermahgoub 1 year, 3 months ago

Therefore, Traffic Director would be a better choice for this scenario as it allows for more complex and fine-grained traffic management, with the capability to inspect the value of an HTTP header and route the traffic to the appropriate service implementation.

upvoted 1 times

 closer89 1 year ago

do not post chatgpt answers!

upvoted 2 times

 zellick 1 year, 4 months ago

**Selected Answer: D**

D is the answer.

<https://cloud.google.com/load-balancing/docs/l7-internal/traffic-management>

Internal HTTP(S) Load Balancing supports advanced traffic management functionality that enables you to use the following features:

- Traffic steering. Intelligently route traffic based on HTTP(S) parameters (for example, host, path, headers, and other request parameters).

upvoted 2 times

 tomato123 1 year, 8 months ago

**Selected Answer: A**

I think A is correct

upvoted 2 times

 **akshaychavan7** 1 year, 8 months ago

**Selected Answer: A**

I believe, it should be A.

upvoted 3 times

 **akshaychavan7** 1 year, 8 months ago

I went through the link shared by Blueocean, and also the Google documentation for Traffic Director, and I feel the correct answer should be option A.

Here's my take on this -

HTTP(s) load balancer does allow the option of Traffic Steering which identifies the header values and based on that it directs the traffic. But here it is important to note that the traffic is directed to the specific Compute Engine instance and not to the service endpoint!

On the other hand, Traffic Director also allows Traffic Steering which directs the traffic based on header values to the specific service endpoint which is what is needed in the above scenario. It also supports the point of loosely coupled services.

Sources -

<https://cloud.google.com/traffic-director>

<https://cloud.google.com/traffic-director/docs/features>

upvoted 1 times

 **akshaychavan7** 1 year, 8 months ago

Here's what the documentation says, 'Traffic Director supports advanced request routing features like traffic splitting, enabling use cases like canarying, url rewrites/redirects, fault injection, traffic mirroring, and advanced routing capabilities based on various header values, including cookies. Traffic Director also supports many advanced traffic policies with the inclusion of many load-balancing schemes, circuit breaking, and backend outlier detections.'

Also, in the above question, there's a statement specifying the need for the application to be loosely coupled. To support this point, I found out one line on the Traffic Director's documentation which goes like this, 'This separation of application logic from networking logic lets you improve your development velocity, increase service availability, and introduce modern DevOps practices to your organization.'

upvoted 1 times

 **Blueocean** 2 years, 3 months ago

Agree with Option D

<https://cloud.google.com/load-balancing/docs/l7-internal/traffic-management>

upvoted 2 times

 **ParagSanyashiv** 2 years, 3 months ago

Agree with D

upvoted 3 times

Your team is developing an ecommerce platform for your company. Users will log in to the website and add items to their shopping cart. Users will be automatically logged out after 30 minutes of inactivity. When users log back in, their shopping cart should be saved. How should you store users' session and shopping cart information while following Google-recommended best practices?

- A. Store the session information in Pub/Sub, and store the shopping cart information in Cloud SQL.
- B. Store the shopping cart information in a file on Cloud Storage where the filename is the SESSION ID.
- C. Store the session and shopping cart information in a MySQL database running on multiple Compute Engine instances.
- D. Store the session information in Memorystore for Redis or Memorystore for Memcached, and store the shopping cart information in Firestore.

**Correct Answer: A***Community vote distribution*

D (100%)

**✉️**  **ParagSanyashiv**  2 years, 3 months ago**Selected Answer: D**

Should be D definitely

upvoted 9 times

**✉️**  **\_rajan\_**  7 months, 1 week ago**Selected Answer: D**

D is correct.

upvoted 1 times

**✉️**  **telp** 1 year, 3 months ago**Selected Answer: D**

A is not correct because local memory is lost on process termination, so you would lose the cart information.

B is not correct because accessing a Cloud Storage bucket is slow and expensive for session information. This is not a Google Cloud best practice.

C is not correct because BigQuery wouldn't be able to handle the frequent updates made to carts and sessions.

D is correct because Memorystore is fast and a standard solution to store session information, and Firestore is ideal for small structured data such as a shopping cart. The user will be mapped to the shopping cart with a new session, if required.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: D**

Answer is D

When storing session and shopping cart information for an ecommerce platform, it's important to consider scalability, reliability, and security. A solution that follows Google-recommended best practices would be to use Memorystore for Redis or Memorystore for Memcached to store session information and Firestore to store shopping cart information.

Memorystore can store session information and easily handle a large number of concurrent connections, which is crucial for an ecommerce platform where users are logged in and adding items to their shopping cart frequently.

Firestore can easily handle large amounts of semi-structured data, such as a shopping cart's item. Firestore is also a scalable and reliable solution, and it supports automatic scaling and replication.

By separating the session information and shopping cart information into different services, you can also increase security and avoid any potential data breaches. Using different services will also allow you to scale them independently.

upvoted 1 times

 **zellck** 1 year, 4 months ago

**Selected Answer: D**

D is the answer.

upvoted 1 times

 **N8dagr8** 1 year, 5 months ago

anyone actually seen this on a test? is A actually correct?

upvoted 1 times

 **TNT87** 1 year, 5 months ago

D is correct

<https://cloud.google.com/memorystore/docs/redis/redis-overview>

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: D**

D is correct

upvoted 3 times

 **akshaychavan7** 1 year, 8 months ago

**Selected Answer: D**

Agree with D

upvoted 1 times

 **nqthien041292** 2 years ago

**Selected Answer: D**

Vote D

upvoted 1 times

Question #113

Topic 1

You are designing a resource-sharing policy for applications used by different teams in a Google Kubernetes Engine cluster. You need to ensure that all applications can access the resources needed to run. What should you do? (Choose two.)

- A. Specify the resource limits and requests in the object specifications.
- B. Create a namespace for each team, and attach resource quotas to each namespace.
- C. Create a LimitRange to specify the default compute resource requirements for each namespace.
- D. Create a Kubernetes service account (KSA) for each application, and assign each KSA to the namespace.
- E. Use the Anthos Policy Controller to enforce label annotations on all namespaces. Use taints and tolerations to allow resource sharing for namespaces.

**Correct Answer: AB**

*Community vote distribution*

✉  **scaenruy** Highly Voted 2 years, 3 months ago

I vote B, C  
<https://kubernetes.io/docs/concepts/policy/resource-quotas/>  
<https://kubernetes.io/docs/concepts/policy/limit-range/>  
upvoted 13 times

✉  **Blueocean** 2 years, 3 months ago

Yes agree B, C  
<https://cloud.google.com/blog/products/containers-kubernetes/kubernetes-best-practices-resource-requests-and-limits>  
upvoted 6 times

✉  **plutonian123** Most Recent 5 months ago

**Selected Answer: AC**

When it comes to Google's recommended best practices for Kubernetes, especially in the context of Google Kubernetes Engine (GKE), the emphasis is generally placed on setting specific resource requests and limits for each pod and container (Option A). This approach aligns with Kubernetes best practices, as it ensures efficient and reliable operation of applications by maximizing infrastructure utilization and guaranteeing smooth application performance.

This granular level of configuration, where resource requests and limits are explicitly set for each workload, is key to operating applications as efficiently and reliably as possible in Kubernetes clusters. It allows for the classification of pods into different Quality of Service (QoS) classes, such as 'Guaranteed' and 'Burstable', which further aids in resource management and scheduling decisions.

upvoted 1 times

✉  **\_rajan\_** 7 months, 1 week ago

**Selected Answer: AB**

Specify the resource limits and requests in the object specifications. This will ensure that each application is allocated the resources it needs to run, and that no application can consume more resources than it was allocated.

Create a namespace for each team, and attach resource quotas to each namespace. This will allow you to isolate each team's applications from each other, and to ensure that each team's applications are not consuming more resources than they were allocated.

upvoted 1 times

✉  **purushi** 8 months, 3 weeks ago

I go with B and C. Defining namespaces and Limiting resource quotas for each team in order to avoid resource collisions and hunger.  
upvoted 2 times

✉  **omermahgoub** 1 year, 3 months ago

**Selected Answer: BC**

In the context of the problem statement, B and C are appropriate solution for ensuring that all applications can access the resources needed to run:

B. Create a namespace for each team, and attach resource quotas to each namespace. This way, you can set limits on the resources that a team can consume, so that one team does not consume all the resources of the cluster, and that resources are shared among all teams in a fair way.

C. Create a LimitRange to specify the default compute resource requirements for each namespace. LimitRanges allow you to set default limits and requests for all the pods in a specific namespace, it also ensure that pods in that namespace can never consume more resources than the LimitRange defined.

You can use a combination of resource limits, quotas, and limit ranges to prevent a single team or application from consuming too many resources, as well as to ensure that all teams and applications have access to the resources they need to run.

upvoted 1 times

✉  **omermahgoub** 1 year, 3 months ago

Option A: Specify the resource limits and requests in the object specifications, is a valid method for controlling the resources that a pod or container needs, but it may not be sufficient by itself to fully manage the resources in a multi-tenant cluster where multiple teams and applications need to share resources.

When you set resource limits and requests on the pod or container level, you have a fine-grained control over the resources that a specific pod or container needs, but it doesn't provide a way to set limits or quotas on the level of a whole team or namespace. It also doesn't provide a default configuration for all pods created in a namespace.

By itself, this method does not give you the visibility and control you need over the overall resource usage across multiple teams and applications. With creating a namespace per team and attaching quotas, you can limit the resources each team can use, and with LimitRanges you can ensure that no pod created in the namespace can go beyond specific limits.

upvoted 1 times

 **zellick** 1 year, 4 months ago

**Selected Answer: BC**

BC is the answer.

<https://kubernetes.io/docs/concepts/policy/resource-quotas/>

A resource quota, defined by a ResourceQuota object, provides constraints that limit aggregate resource consumption per namespace. It can limit the quantity of objects that can be created in a namespace by type, as well as the total amount of compute resources that may be consumed by resources in that namespace.

<https://kubernetes.io/docs/concepts/policy/limit-range/>

A LimitRange is a policy to constrain the resource allocations (limits and requests) that you can specify for each applicable object kind (such as Pod or PersistentVolumeClaim) in a namespace.

upvoted 2 times

 **TNT87** 1 year, 5 months ago

**Selected Answer: BC**

<https://cloud.google.com/blog/products/containers-kubernetes/kubernetes-best-practices-resource-requests-and-limits>

Ans B,C

upvoted 3 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: BC**

BC are correct

upvoted 4 times

 **bk7** 1 year, 8 months ago

**Selected Answer: AB**

A&B as obvious !

upvoted 3 times

 **alex8081** 1 year, 8 months ago

why A&B?

upvoted 1 times

 **akshaychavan7** 1 year, 8 months ago

**Selected Answer: BC**

I will go with B and C.

upvoted 1 times

 **jdx000** 1 year, 9 months ago

**Selected Answer: BC**

B,C are the right options

upvoted 2 times

 **[Removed]** 2 years ago

A, B

LimitRanges are great and all, but they don't actually guarantee that running containers have the resources available that they need, since the not object-specific.

upvoted 1 times

Question #114

Topic 1

You are developing a new application that has the following design requirements:

- ⇒ Creation and changes to the application infrastructure are versioned and auditable.
- ⇒ The application and deployment infrastructure uses Google-managed services as much as possible.
- ⇒ The application runs on a serverless compute platform.

How should you design the application's architecture?

- A. 1. Store the application and infrastructure source code in a Git repository. 2. Use Cloud Build to deploy the application infrastructure with Terraform. 3. Deploy the application to a Cloud Function as a pipeline step.
- B. 1. Deploy Jenkins from the Google Cloud Marketplace, and define a continuous integration pipeline in Jenkins. 2. Configure a pipeline step to pull the application source code from a Git repository. 3. Deploy the application source code to App Engine as a pipeline step.
- C. 1. Create a continuous integration pipeline on Cloud Build, and configure the pipeline to deploy the application infrastructure using Deployment Manager templates. 2. Configure a pipeline step to create a container with the latest application source code. 3. Deploy the container to a Compute Engine instance as a pipeline step.
- D. 1. Deploy the application infrastructure using gcloud commands. 2. Use Cloud Build to define a continuous integration pipeline for changes to the application source code. 3. Configure a pipeline step to pull the application source code from a Git repository, and create a containerized application. 4. Deploy the new container on Cloud Run as a pipeline step.

**Correct Answer: D**

Reference:

<https://cloud.google.com/docs/ci-cd>

*Community vote distribution*

A (69%)

D (31%)

 **morenocasado**  2 years ago

**Selected Answer: A**

A is the correct choice.

B - use Jenkins as the deployment tool instead of Cloud Build (The application and deployment infrastructure uses Google-managed services much as possible).

C - uses Compute Engine to run containers. CE is not serverless.

D - we can't version gcloud commands

upvoted 6 times

👤 **wanrltw** 5 months ago

Cloud Functions are intended for single-purpose functions, not an entire app.

D is a far better fit here and nobody is talking about "versioning gcloud commands" - Cloud Run has revisions (=versions), which meets the task's criteria.

upvoted 1 times

👤 **alpha\_canary** Most Recent ⓘ 1 week, 4 days ago

**Selected Answer: A**

D would be true if & only it didn't mention using gcloud commands to deploy application infrastructure

upvoted 1 times

👤 **wanrltw** 5 months ago

**Selected Answer: D**

I vote D:

- gcloud, Cloud Build, Cloud Run - are Google-managed services
- Cloud Run has revisions (=versions)
- Cloud Run is serverless

A is wrong, as Cloud Functions are intended for single-purpose functions - not an entire app.

upvoted 2 times

👤 **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: A**

A is correct

upvoted 1 times

👤 **purushi** 8 months, 3 weeks ago

**Selected Answer: A**

My answer is A:

Version and auditable: GIT

GCP managed deployment infrastructure: Cloud build, Cloud Deployment Manager, Terraform

Serverless: Cloud Functions

upvoted 2 times

👤 **NewComer200** 12 months ago

**Selected Answer: A**

It is definitely A vs. B, though.

I still think the deciding factor is "Creation and changes to the application infrastructure are versioned and auditable".

Whether to deploy to Cloud Run or Cloud Functions is irrelevant because we don't know the contents of the application.

Both are serverless.

upvoted 1 times

👤 **AscendedCrow** 1 year, 1 month ago

**Selected Answer: D**

What put me off A is that at the end there is deploy to `Cloud Function` and it should be all serverless applications and not just a cloud function that is what Cloud Run should do.

upvoted 2 times

✉  **omermahgoub** 1 year, 3 months ago

**Selected Answer: D**

Option D is the best fit for designing the architecture of the new application as it satisfies all the design requirements of versioning and auditing the infrastructure changes, using Google-managed services and deploying the application on a serverless compute platform. The approach includes:

- Deploy the application infrastructure using gcloud commands.
- Use Cloud Build to define a continuous integration pipeline for changes to the application source code.
- Configure a pipeline step to pull the application source code from a Git repository, and create a containerized application.
- Deploy the new container on Cloud Run as a pipeline step.

It's worth noting that all options could potentially satisfy the requirements, as long as they use Google-managed services and track infrastructure creation and changes, the choice of different services, platform and tools depend on the specific requirements of your application and development preferences.

upvoted 4 times

✉  **AscendedCrow** 1 year, 1 month ago

What about the versioning aspect?

upvoted 1 times

✉  **omermahgoub** 1 year, 3 months ago

Option A: 1. Store the application and infrastructure source code in a Git repository. 2. Use Cloud Build to deploy the application infrastructure with Terraform. 3. Deploy the application to a Cloud Function as a pipeline step, can potentially satisfy the requirement of versioning and auditing the infrastructure changes, but it may not meet the other two requirements of using Google-managed services and deploying the application on a serverless compute platform:

- By using Terraform, which is a third-party infrastructure as code tool, it is not a Google-managed service and it may not have the same level of integration as Google-managed services.
- Cloud Functions are a serverless compute platform, but it's mainly used to run event-driven, short-lived functions, while it's not a suitable choice for running long running processes, web servers and so on.

upvoted 2 times

✉  **omermahgoub** 1 year, 3 months ago

In addition, deploying the infrastructure using Terraform, which is not fully integrated with the Google Cloud, may lead to additional cost management effort.

Also, deploying the application on Cloud Functions may not be able to meet some of the requirements like long running processes, static workloads and other requirements that Cloud Run can fulfill.

upvoted 1 times

✉  **omermahgoub** 1 year, 3 months ago

Although, all of the options may have their own merits and depending on the specific requirement of the application any of them can be suitable, but considering all the requirements stated in the question option D could be the best fit.

upvoted 1 times

✉  **zelick** 1 year, 4 months ago

**Selected Answer: A**

A is the answer.

upvoted 1 times

✉  **TNT87** 1 year, 5 months ago

Ans A

<https://cloud.google.com/docs/ci-cd/products#featured-products-for-ci-cd>

upvoted 1 times

✉  **[Removed]** 1 year, 7 months ago

D is correct, applications should not be deployed on cloud functions.

upvoted 2 times

✉  **tomato123** 1 year, 8 months ago

**Selected Answer: A**

A is correct

upvoted 4 times

 **dishum** 1 year, 11 months ago

B and C are not correct (we cant use jenkins in option B, and cant use compute engine as it is not serverless in option C)

So in A and D option -

option A is not right becoz we can deploy on cloud function not suitable as serverless compute

So i think Answer is D

upvoted 1 times

 **dishum** 1 year, 11 months ago

Changing my answer to A, becoz of versioning. can't use gcloud commands in versioning in option D

upvoted 2 times

 **nqthien041292** 2 years ago

**Selected Answer: A**

Vote A

Question #115

Topic 1

You are creating and running containers across different projects in Google Cloud. The application you are developing needs to access Google Cloud services from within Google Kubernetes Engine (GKE). What should you do?

- A. Assign a Google service account to the GKE nodes.
- B. Use a Google service account to run the Pod with Workload Identity.
- C. Store the Google service account credentials as a Kubernetes Secret.
- D. Use a Google service account with GKE role-based access control (RBAC).

**Correct Answer: A**

*Community vote distribution*

B (100%)

 **Blueocean**  2 years, 3 months ago

Option B

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

upvoted 7 times

 **alpha\_canary**  1 week, 4 days ago

**Selected Answer: B**

[https://cloud.google.com/kubernetes-engine/docs/concepts/workload-identity#:~:text=Workload%20Identity%20Federation%20for%20GKE%20is%20the%20recommended%20way%20for%20your%20workload%20running%20on%20Google%20Kubernetes%20Engine%20\(GKE\)%20to%20access%20Google%20Cloud%20services%20in%20a%20ure%20and%20manageable%20way](https://cloud.google.com/kubernetes-engine/docs/concepts/workload-identity#:~:text=Workload%20Identity%20Federation%20for%20GKE%20is%20the%20recommended%20way%20for%20your%20workload%20running%20on%20Google%20Kubernetes%20Engine%20(GKE)%20to%20access%20Google%20Cloud%20services%20in%20a%20ure%20and%20manageable%20way)

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: B**

The best way to access Google Cloud services from within Google Kubernetes Engine (GKE) is to use a Google service account to run the Pod with Workload Identity.

Workload Identity allows your pods to authenticate to Google Cloud services using their Kubernetes service account credentials, without you having to expose any sensitive credentials in your code.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: B**

Application images runs as a container within a POD as a process. So Pod should be identified as a principle here and it should have a service account to access other services within GKE cluster.

upvoted 2 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: B**

In summary, using Workload Identity allows you to authenticate your application to Google Cloud services using the same identity that runs the application, this makes it simple to manage the access and permissions to resources, and also ensures that your application only has the necessary permissions to access the services.

upvoted 2 times

 **omermahgoub** 1 year, 3 months ago

The correct answer is B: Use a Google service account to run the Pod with Workload Identity.

Workload Identity allows you to authenticate to Google Cloud services using the same identity that runs your application, instead of creating and managing a separate service account. This simplifies the process of granting permissions to your application, and ensures that it only has the necessary access to resources.

When you assign a Google service account to GKE nodes (Option A), it can be difficult to manage the permissions needed by the application and also could be a security issue since it grants access to all the services that the service account has permissions to.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

When you assign a Google service account to GKE nodes (Option A), it can be difficult to manage the permissions needed by the application and also could be a security issue since it grants access to all the services that the service account has permissions to.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Storing the Google service account credentials as a Kubernetes Secret (Option C) can be a security concern, since the credentials may be easily accessed by unauthorized parties.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Use a Google service account with GKE role-based access control (RBAC) (Option D) is not the recommended approach, while RBAC is good to restrict and manage access to resources, it's not the best fit for authenticating the workloads to access the Google Cloud services.

upvoted 1 times

 **zellck** 1 year, 4 months ago

**Selected Answer: B**

B is the answer.

[https://cloud.google.com/kubernetes-engine/docs/concepts/workload-identity#what\\_is](https://cloud.google.com/kubernetes-engine/docs/concepts/workload-identity#what_is)

Applications running on GKE might need access to Google Cloud APIs such as Compute Engine API, BigQuery Storage API, or Machine Learning APIs.

Workload Identity allows a Kubernetes service account in your GKE cluster to act as an IAM service account. Pods that use the configured Kubernetes service account automatically authenticate as the IAM service account when accessing Google Cloud APIs. Using Workload Identity allows you to assign distinct, fine-grained identities and authorization for each application in your cluster.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: B**

B is correct

upvoted 2 times

 **akshaychavan7** 1 year, 8 months ago

**Selected Answer: B**

I will go with option B.

upvoted 1 times

 **nqthien041292** 2 years ago

**Selected Answer: B**

Vote B

upvoted 1 times

 **jitu028** 2 years ago

Correct answer is B

upvoted 1 times

👤 **assuf** 2 years, 3 months ago

vote B

upvoted 4 times

Question #116

Topic 1

You have containerized a legacy application that stores its configuration on an NFS share. You need to deploy this application to Google Kubernetes Engine (GKE) and do not want the application serving traffic until after the configuration has been retrieved. What should you do?

- A. Use the gsutil utility to copy files from within the Docker container at startup, and start the service using an ENTRYPOINT script.
- B. Create a PersistentVolumeClaim on the GKE cluster. Access the configuration files from the volume, and start the service using an ENTRYPOINT script.
- C. Use the COPY statement in the Dockerfile to load the configuration into the container image. Verify that the configuration is available, and start the service using an ENTRYPOINT script.
- D. Add a startup script to the GKE instance group to mount the NFS share at node startup. Copy the configuration files into the container, and start the service using an ENTRYPOINT script.

**Correct Answer:** D

Reference:

<https://cloud.google.com/compute/docs/instances/startup-scripts/linux>

*Community vote distribution*

B (100%)

👤 **Ksamilosb** Highly Voted 2 years, 2 months ago

It's not necessary to mount NFS to each node in GKE. Just create PVC point to shared NFS, mount to container, and use configuration in ENTRYPOINT. Vote B

upvoted 8 times

👤 **GCPCloudArchitectUser** 2 years, 2 months ago

I am not convinced but it does seem to be best option among all options

upvoted 1 times

👤 **\_rajan\_** Most Recent 7 months, 1 week ago

**Selected Answer: B**

B is correct.

upvoted 1 times

👤 **purushi** 8 months, 3 weeks ago

**Selected Answer: B**

B is more formal and standardized way to mount NFS onto the worker node compared to A where it asks us to create a startup script to mount the volume.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: B**

With PersistentVolumeClaim object, we can claim the volume what we need dynamically. The storage class will be defined by network administrator. Container/Pod needs to wait until it reads configuration from the mounted volume before serving traffic to its clients.

upvoted 1 times

 **jnas** 9 months, 1 week ago

**Selected Answer: B**

<https://cloud.google.com/kubernetes-engine/docs/concepts/persistent-volumes>. PersistentVolume resources are used to manage durable storage in a cluster. In GKE, a PersistentVolume is typically backed by a persistent disk. You can also use other storage solutions like NFS. Filestore is a NFS solution on Google Cloud

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: B**

B and D are the main candidate answers

Option B: allows the application to be stateless and have no dependencies on the filesystem of the host.

D: is a good solution since it allows the application to access its configuration as soon as the application starts, without having to copy the configuration files into the container.

But the best option is B, because it allows the application to be stateless and have no dependencies on the filesystem of the host. This approach is more flexible, makes it easy to update the configuration files, and reduces the size of the container image.

upvoted 1 times

 **telp** 1 year, 3 months ago

**Selected Answer: B**

B is correct using default tools

upvoted 1 times

 **TNT87** 1 year, 4 months ago

<https://kubernetes.io/docs/concepts/storage/persistent-volumes/#access-modes>

<https://cloud.google.com/filestore/docs/accessing-fileshares>

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

upvoted 1 times

 **zellck** 1 year, 4 months ago

**Selected Answer: B**

B is the answer.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: B**

B is correct

upvoted 3 times

 **americoleonardo** 1 year, 11 months ago

**Selected Answer: B**

I think B is more suitable in this situation

upvoted 2 times

 **juancambb** 2 years, 1 month ago

B and C are valid, but B use native tools of Kubernetes, so is a best practice and easy to implement.

upvoted 2 times

 **juancambb** 2 years, 1 month ago

answer is B

upvoted 1 times

 **assuf** 2 years, 3 months ago

vote C

upvoted 4 times

Your team is developing a new application using a PostgreSQL database and Cloud Run. You are responsible for ensuring that all traffic is kept private on Google

Cloud. You want to use managed services and follow Google-recommended best practices. What should you do?

- A. 1. Enable Cloud SQL and Cloud Run in the same project. 2. Configure a private IP address for Cloud SQL. Enable private services access. 3. Create a Serverless VPC Access connector. 4. Configure Cloud Run to use the connector to connect to Cloud SQL.
- B. 1. Install PostgreSQL on a Compute Engine virtual machine (VM), and enable Cloud Run in the same project. 2. Configure a private IP address for the VM. Enable private services access. 3. Create a Serverless VPC Access connector. 4. Configure Cloud Run to use the connector to connect to the VM hosting PostgreSQL.
- C. 1. Use Cloud SQL and Cloud Run in different projects. 2. Configure a private IP address for Cloud SQL. Enable private services access. 3. Create a Serverless VPC Access connector. 4. Set up a VPN connection between the two projects. Configure Cloud Run to use the connector to connect to Cloud SQL.
- D. 1. Install PostgreSQL on a Compute Engine VM, and enable Cloud Run in different projects. 2. Configure a private IP address for the VM. Enable private services access. 3. Create a Serverless VPC Access connector. 4. Set up a VPN connection between the two projects. Configure Cloud Run to use the connector to access the VM hosting PostgreSQL

**Correct Answer: B**

*Community vote distribution*

A (100%)

 **alpha\_canary** 1 week, 4 days ago

**Selected Answer: A**

A is correct.

B & D is rejected easily

C: its adding unnecessary complexity by putting them in different project. Why would be even do that  
upvoted 1 times

 **darkblade60** 3 months, 2 weeks ago

Should be B, your app is PostgreSQL + Cloud Run, uses Cloud SQL is change the premise  
upvoted 1 times

 **darkblade60** 3 months, 2 weeks ago

mmmm well, I think its A because CloudSQL can be postgresql  
upvoted 1 times

 **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: A**

I would go with A.  
upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: A**

The key here is, Google Managed services and follow Google-recommended best practices: Definitely Cloud SQL instead of PostgreSQL th almost an unmanaged service managed by custom configurations set by customers.

upvoted 2 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: A**

The answer would be A. By using Cloud SQL and Cloud Run in the same project, you can take advantage of the built-in security features and managed services provided by Google Cloud. By configuring a private IP address for Cloud SQL and enabling private services access, you can ensure that all traffic is kept private. You can also create a Serverless VPC Access connector and configure Cloud Run to use this connector to connect to Cloud SQL. This configuration will allow your application to connect to the database securely and privately, following Google-recommended best practices.

upvoted 1 times

 **zelick** 1 year, 4 months ago

**Selected Answer: A**

A is the answer.

<https://cloud.google.com/vpc/docs/serverless-vpc-access>

Serverless VPC Access makes it possible for you to connect directly to your Virtual Private Cloud network from serverless environments such as Cloud Run, App Engine, or Cloud Functions. Configuring Serverless VPC Access allows your serverless environment to send requests to your VPC network using internal DNS and internal IP addresses (as defined by RFC 1918 and RFC 6598). The responses to these requests also use your internal network.

upvoted 1 times

 **TNT87** 1 year, 5 months ago

**Selected Answer: A**

<https://cloud.google.com/sql/docs/postgres/connect-run#configure>

<https://cloud.google.com/sql/docs/postgres/connect-run#private-ip>

Answer A

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: A**

A is correct

upvoted 2 times

 **akshaychavan7** 1 year, 8 months ago

**Selected Answer: A**

Options C and D are crossed out as they suggest using different projects.

To choose between option A and B, why should we install PostgreSQL explicitly, if it is already present in CloudSQL. So, I will go with CloudSQL.

upvoted 1 times

 **nqthien041292** 2 years ago

**Selected Answer: A**

Vote A

upvoted 2 times

 **Blueocean** 2 years, 3 months ago

Option A is best option

upvoted 3 times

 **scaenruy** 2 years, 3 months ago

I vote A

<https://cloud.google.com/sql/docs/postgres/connect-run#private-ip>

upvoted 1 times

 **ParagSanyashiv** 2 years, 3 months ago

**Selected Answer: A**

Correct option is A

upvoted 2 times

 **ParagSanyashiv** 2 years, 3 months ago

I will go for option A, as mentioned in the question, managed services to be used, in this case using a Cloud SQL would be correct. If a PostgreSQL is installed in a compute engine, then it will be customer managed rather google service managed.

upvoted 2 times

You are developing an application that will allow clients to download a file from your website for a specific period of time. How should you design the application to complete this task while following Google-recommended best practices?

- A. Configure the application to send the file to the client as an email attachment.
- B. Generate and assign a Cloud Storage-signed URL for the file. Make the URL available for the client to download.
- C. Create a temporary Cloud Storage bucket with time expiration specified, and give download permissions to the bucket. Copy the file, and send it to the client.
- D. Generate the HTTP cookies with time expiration specified. If the time is valid, copy the file from the Cloud Storage bucket, and make the file available for the client to download.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **Blueocean** Highly Voted 2 years, 3 months ago

Agree with Option B

upvoted 7 times

 **scaenruy** Highly Voted 2 years, 3 months ago

Yes, I vote B

upvoted 5 times

 **alpha\_canary** Most Recent 1 week, 4 days ago

**Selected Answer: B**

[https://cloud.google.com/storage/docs/access-control/signed-urls#:~:text=X%2DGoog%2DDate%3A%20The,604800%20seconds%20\(7%20days\)](https://cloud.google.com/storage/docs/access-control/signed-urls#:~:text=X%2DGoog%2DDate%3A%20The,604800%20seconds%20(7%20days))

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

Question #119

Topic 1

Your development team has been asked to refactor an existing monolithic application into a set of composable microservices. Which design aspects should you implement for the new application? (Choose two.)

- A. Develop the microservice code in the same programming language used by the microservice caller.
- B. Create an API contract agreement between the microservice implementation and microservice caller.
- C. Require asynchronous communications between all microservice implementations and microservice callers.
- D. Ensure that sufficient instances of the microservice are running to accommodate the performance requirements.
- E. Implement a versioning scheme to permit future changes that could be incompatible with the current interface.

**Correct Answer: B**

*Community vote distribution*

B (72%)

E (28%)

 **nqthien041292** Highly Voted 2 years ago

**Selected Answer: B**

Vote BE

upvoted 8 times

 **alpha\_canary** Most Recent 1 week, 4 days ago

**Selected Answer: B**

B & E is the answer

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: B**

BD : is the correct one here.

Create an API contract agreement between the microservice implementation and microservice caller. This will help to ensure that the microservices are decoupled from each other, and that the caller can be updated without having to update the implementation.

Ensure that sufficient instances of the microservice are running to accommodate the performance requirements. This is important because microservices are often scaled independently, and you need to make sure that each microservice can handle the expected load.

upvoted 2 times

 **purush** 8 months, 3 weeks ago

**Selected Answer: E**

Versioning schema is the evolutionary process in API development.

For eg:

/v1/users/1234

/v2/users/1234

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: B**

API contract design is the first step in design-first approach while creating APIs (REST). We can also follow code-first approach while providing solution via public APIs. Design first approach is more flexible and provides sufficient amount of time for the dev team to gather requirements to understand what customer really wants.

upvoted 1 times

 **edward\_zhang** 1 year, 2 months ago

D & E,  
B and E are same thing. D is considering capacity of micro service.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: B**

B. Guarantees that the two parties are communicating in a well-defined way, which makes the microservices more flexible, composable, and easy to understand.

E. Allows to make changes to the service's API while still maintaining backward compatibility. With versioning, new and old consumers can continue to use the service without interruption as new features are added.

On the other hand, developing the microservice code in the same programming language as the microservice caller does not promote loose coupling, and it may also increase the complexity of the system as it will depend on language-specific features. Asynchronous communication are also not always necessary and depend on the use case and requirement. Ensuring sufficient instances of the microservice are running can be done by using a scalability strategy such as Auto-scaling, and this is not a specific design aspect.

upvoted 1 times

 **telp** 1 year, 3 months ago

BE with the recommendation on <https://cloud.google.com/architecture/migrating-a-monolithic-app-to-microservices-gke>

upvoted 1 times

 **zellck** 1 year, 4 months ago

**Selected Answer: B**

BE is the answer.

[https://cloud.google.com/architecture/migrating-a-monolithic-app-to-microservices-gke#api\\_contracts](https://cloud.google.com/architecture/migrating-a-monolithic-app-to-microservices-gke#api_contracts)

Each microservice should be invoked only from a set of interfaces. Each interface should in turn be clearly defined by a contract that can be implemented using an API definition language like the OpenAPI Initiative specification or RAML. Having well-defined API contracts and interfaces allows you to develop tests as a main component of your solution (for example, by applying test-driven development) against these API interfaces.

<https://cloud.google.com/architecture/migrating-a-monolithic-app-to-microservices-gke#versioning>

To give you flexibility in managing updates that might break existing clients, you should implement a versioning scheme for your microservice. Versioning lets you deploy updated versions of a microservice without affecting the clients that are using an existing version.

upvoted 2 times

 **TNT87** 1 year, 5 months ago

1. When you incrementally migrate services, configure communication between services and monolith to go through well-defined API contracts  
Answer B

2. [https://cloud.google.com/architecture/microservices-architecture-refactoring-monoliths#design\\_interservice\\_communication](https://cloud.google.com/architecture/microservices-architecture-refactoring-monoliths#design_interservice_communication) Ans C  
Ans B,C

upvoted 1 times

 **TNT87** 1 year, 5 months ago

To support C

[https://cloud.google.com/architecture/microservices-architecture-interservice-communication#logical\\_separation\\_of\\_service](https://cloud.google.com/architecture/microservices-architecture-interservice-communication#logical_separation_of_service)  
In this document, you isolate the payment service from the rest of the application. All flows in the original Online Boutique application are synchronous. "In the refactored application, the payment process is converted to an asynchronous flow. Therefore, when you receive a purchase request, instead of processing it immediately, you provide a "request received" confirmation to the user. In the background, an asynchronous request is triggered to the payment service to process the payment."

upvoted 1 times

 **TNT87** 1 year, 5 months ago

To support B

\*When you incrementally migrate services, configure communication between services and monolith to go through well-defined API contracts  
<https://cloud.google.com/architecture/microservices-architecture-refactoring-monoliths>

upvoted 1 times

 **TNT87** 1 year, 5 months ago

I personally do not see or find anything supporting E at all...

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: E**

BE are correct

upvoted 4 times

 **jdx000** 1 year, 9 months ago

Note to admin: change this question's answer to reflect a 2 answer selection

upvoted 4 times

 **jdx000** 1 year, 9 months ago

**Selected Answer: B**

B & E seems best

upvoted 3 times

 **hitmax87** 2 years ago

B and D

upvoted 2 times

 **GoReplyGCPExam** 1 year, 11 months ago

For me to ensure that sufficient instances of the microservice are running to accommodate the performance requirements is not needed because of the big variety of services that provide autoscaling.

BE

upvoted 1 times

 **fabiam93** 2 years, 1 month ago

Agree with B and E.

[https://cloud.google.com/appengine/docs/standard/java/designing-microservice-api#using\\_strong\\_contracts](https://cloud.google.com/appengine/docs/standard/java/designing-microservice-api#using_strong_contracts)

upvoted 2 times

 **GCPCloudArchitectUser** 2 years, 2 months ago

This one is tricky one as C and E could be better option as well but there was no mention about reliability...

upvoted 2 times

 **GCPCloudArchitectUser** 2 years, 2 months ago

I will agree with B and E

upvoted 4 times

You deployed a new application to Google Kubernetes Engine and are experiencing some performance degradation. Your logs are being written to Cloud

Logging, and you are using a Prometheus sidecar model for capturing metrics. You need to correlate the metrics and data from the logs to troubleshoot the performance issue and send real-time alerts while minimizing costs. What should you do?

- A. Create custom metrics from the Cloud Logging logs, and use Prometheus to import the results using the Cloud Monitoring REST API.
- B. Export the Cloud Logging logs and the Prometheus metrics to Cloud Bigtable. Run a query to join the results, and analyze in Google Data Studio.
- C. Export the Cloud Logging logs and stream the Prometheus metrics to BigQuery. Run a recurring query to join the results, and send notifications using Cloud Tasks.
- D. Export the Prometheus metrics and use Cloud Monitoring to view them as external metrics. Configure Cloud Monitoring to create log-based metrics from the logs, and correlate them with the Prometheus data.

**Correct Answer:** D

Reference:

<https://cloud.google.com/blog/products/operations/troubleshoot-gke-faster-with-monitoring-data-in-your-logs>

*Community vote distribution*

D (100%)

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: D**

This option is the most cost-effective because it does not require you to export any data to Bigtable or BigQuery. It is also the most efficient option because it allows you to correlate the metrics and logs in real time.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: D**

Correlate Prometheus metrics and Cloud logging logs: We need to compare these two logs. Prometheus is an external metrics which can be a library dependency used in the application. To compare Apple vs apple, we need to bring Prometheus metrics to GCP and should configure Cloud monitoring to treat them as an external metric.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: D**

This option allows you to use Cloud Monitoring to view the Prometheus metrics and create log-based metrics from the logs. This allows you to correlate the metrics and logs in one place. By using Cloud Monitoring, you can also set up alerting rules and dashboards which can help you identify and troubleshoot the performance issues in real-time and with low costs.

It's not necessary to export the data to another storage to perform the correlation and to set up notifications, it can all be done directly in the Cloud Monitoring, taking advantage of its features.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

D. Export the Prometheus metrics and use Cloud Monitoring to view them as external metrics. Configure Cloud Monitoring to create log-based metrics from the logs, and correlate them with the Prometheus data.

upvoted 1 times

 **zellck** 1 year, 4 months ago

**Selected Answer: D**

D is the answer.

[https://cloud.google.com/stackdriver/docs/solutions/gke/prometheus#viewing\\_metrics](https://cloud.google.com/stackdriver/docs/solutions/gke/prometheus#viewing_metrics)

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: D**

D is correct

Question #121

Topic 1

You have been tasked with planning the migration of your company's application from on-premises to Google Cloud. Your company's monolithic application is an ecommerce website. The application will be migrated to microservices deployed on Google Cloud in stages. The majority of your company's revenue is generated through online sales, so it is important to minimize risk during the migration. You need to prioritize features and select the first functionality to migrate. What should you do?

- A. Migrate the Product catalog, which has integrations to the frontend and product database.
- B. Migrate Payment processing, which has integrations to the frontend, order database, and third-party payment vendor.
- C. Migrate Order fulfillment, which has integrations to the order database, inventory system, and third-party shipping vendor.
- D. Migrate the Shopping cart, which has integrations to the frontend, cart database, inventory system, and payment processing system.

**Correct Answer: A**

*Community vote distribution*

A (91%)

9%

 **GCPCloudArchitectUser**  2 years, 2 months ago

**Selected Answer: A**

I agree with Option A, as the question states "first one"

upvoted 5 times

✉  **\_\_rajan\_\_** (Most Recent) 7 months, 1 week ago

**Selected Answer: A**

I will go with A as it has less dependencies.

upvoted 1 times

✉  **purushi** 8 months, 3 weeks ago

**Selected Answer: A**

A should be the first MVP item in the list.

Key is to avoid risks in the initial stages of transition.

upvoted 1 times

✉  **omermahgoub** 1 year, 3 months ago

**Selected Answer: D**

[https://cloud.google.com/architecture/migrating-a-monolithic-app-to-microservices-gke#example\\_migrating\\_a\\_shopping\\_cart](https://cloud.google.com/architecture/migrating-a-monolithic-app-to-microservices-gke#example_migrating_a_shopping_cart)

Based on the guide referenced, the answer would be D. Migrate the Shopping cart, which has integrations to the frontend, cart database, inventory system, and payment processing system. The guide recommends migrating functionality with the least dependencies and level of complexity first, which the shopping cart functionality has fewer dependencies and less complexity than the other options presented. This will minimize risk while still providing value to the business and allowing further migration of more complex functionality.

upvoted 1 times

✉  **omermahgoub** 1 year, 3 months ago

Migrating the product catalog first may be a good option if the product catalog is a separate service that doesn't rely on other services and can be deployed independently. However, if it is closely tied to other services such as the frontend or product database, migrating it first may introduce complexity and increase the risk of the migration, as the other dependent services would need to be migrated or integrated with new product catalog service in parallel.

upvoted 1 times

✉  **zellick** 1 year, 4 months ago

**Selected Answer: A**

A is the answer.

[https://cloud.google.com/architecture/migrating-a-monolithic-app-to-microservices-gke#choosing\\_an\\_initial\\_migration\\_effort](https://cloud.google.com/architecture/migrating-a-monolithic-app-to-microservices-gke#choosing_an_initial_migration_effort)

upvoted 1 times

✉  **TNT87** 1 year, 5 months ago

[https://cloud.google.com/architecture/migrating-a-monolithic-app-to-microservices-gke#example\\_migrating\\_a\\_shopping\\_cart](https://cloud.google.com/architecture/migrating-a-monolithic-app-to-microservices-gke#example_migrating_a_shopping_cart)

Answer A

upvoted 2 times

 **[Removed]** 1 year, 7 months ago

I don't agree with option A. Google docs says:

"When you plan your migration, it's tempting to start with features that are trivial to migrate. This might represent a quick win, but might not be the best learning experience for your team. Instead of going straight to the migration, you should spend time evaluating all of the features and create plans for their migration."

"According to this evaluation framework, the ideal candidate for the initial migration effort should be challenging enough to be meaningful, but simple enough to minimize the risk of failure. The initial migration process should also:

Require little refactoring, considering both the feature itself and the related business processes.

Be stateless—that is, have no external data requirements.

Have few or no dependencies."

I think it's between options B & C since the third-party vendors already have a microservices architecture going on.

<https://cloud.google.com/architecture/migrating-a-monolithic-app-to-microservices-gke#:~:text=When%20you%20plan,for%20their%20migration>.

upvoted 2 times

 **ajipeggy** 1 year, 5 months ago

as it says in your link:

A migration plan example

The following list shows an example of a migration order:

Platform frontend; that is, the user interface

Stateless features, such as a currency-conversion service

Features with independent datasets (datasets that have no dependencies on other datasets), such as a service to list your brick-and-mortar stores

Features with shared datasets—the business logic of the ecommerce platform

so the first one should be the user interface = product catalogue

upvoted 2 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: A**

A is correct

upvoted 2 times

 **szl0144** 1 year, 11 months ago

A is correct.

upvoted 1 times

 **BackendBoi** 2 years ago

I will vote C. It is the only service where a temporary disruption will not impact all sales on the website (because it is not embedded in the frontend).

upvoted 2 times

 **Blueocean** 2 years, 3 months ago

Agree Option A , in order to keep the disruption as minimum as possible by migrating minimum features

Question #122

Topic 1

Your team develops services that run on Google Kubernetes Engine. Your team's code is stored in Cloud Source Repositories. You need to quickly identify bugs in the code before it is deployed to production. You want to invest in automation to improve developer feedback and make the process as efficient as possible.

What should you do?

- A. Use Spinnaker to automate building container images from code based on Git tags.
- B. Use Cloud Build to automate building container images from code based on Git tags.
- C. Use Spinnaker to automate deploying container images to the production environment.
- D. Use Cloud Build to automate building container images from code based on forked versions.

**Correct Answer: A**

Reference:

<https://spinnaker.io/docs/guides/tutorials/codelabs/kubernetes-v2-source-to-prod/>*Community vote distribution*

B (87%)

13%

**rajan** 7 months, 1 week ago**Selected Answer: B**

B is correct.

upvoted 1 times

**purushti** 8 months, 3 weeks ago**Selected Answer: B**

We need to have the following steps in Cloud Build to identify bugs"

- 1) Static code analysis
- 2) Code Vulnerability scanning
- 3) Docker Image vulnerability scanning

Using Grype is one such example.

upvoted 1 times

**eddoasso** 9 months, 4 weeks ago**Selected Answer: D**

I say D.

Both B and D could work. However why not use traditional git workflows and keep separate branches for separate tasks. This way each image can be tested independently.

upvoted 1 times

**omermahgoub** 1 year, 3 months ago**Selected Answer: B**

Option B is appropriate because it uses Cloud Build, a service that can automatically build container images from code stored in Cloud Source Repositories based on Git tags. This allows developers to quickly identify bugs in their code before it is deployed to production, by automating the building process and improving developer feedback.

Option A uses Spinnaker, which is a multi-cloud continuous delivery platform that can automate building, testing, and deploying container images. However, it does not specifically mention using git tags to trigger builds, thus for this particular use case it might not be the best fit.

upvoted 1 times

**omermahgoub** 1 year, 3 months ago

Option C also uses Spinnaker, and is similar to A, Spinnaker can automate deploying container images to the production environment, but not specific to building and identifying bugs before deploying, so it might not be the best fit for this use case.

Option D uses Cloud Build, but it's not specific to building images based on git tags, it's more general and focuses on building images based on forked versions, which might not be needed in this case.

upvoted 1 times

**zellck** 1 year, 4 months ago**Selected Answer: B**

B is the answer.

upvoted 1 times

**GCP001** 1 year, 5 months ago

D ) You need to quickly identify bugs in the code before it is deployed to production. So it's for developer to fork the code and test the build. Later they can push the changes using PR to the master repo/branch.

upvoted 2 times

**[Removed]** 1 year, 7 months ago**Selected Answer: B**

cloud build is the google service so it stands to reason to use that.

upvoted 2 times

✉️ 🚑 **tomato123** 1 year, 8 months ago

**Selected Answer: B**

I think b is correct

upvoted 3 times

✉️ 🚑 **hitmax87** 2 years ago

**Selected Answer: D**

I vote D. Because every developer before merge to the master should test build in his branch. It will expose bugs. Once branch merged to the master, master build pipeline comes up.

upvoted 1 times

✉️ 🚑 **GCPCloudArchitectUser** 2 years, 2 months ago

**Selected Answer: B**

I would disagree with A as Spinnaker is for deployment not for building images

So either B or C : C is stating to deploy to production but the question is to give feedback to developer before it goes to production

So the only close answer is B but it is half answer

Perhaps choice A was poorly written instead deploy build then it could be A

upvoted 4 times

✉️ 🚑 **GCPCloudArchitectUser** 2 years, 2 months ago

I mean instead of deploy it was typed incorrect as build for A

upvoted 1 times

✉️ 🚑 **scaenruy** 2 years, 3 months ago

I vote B

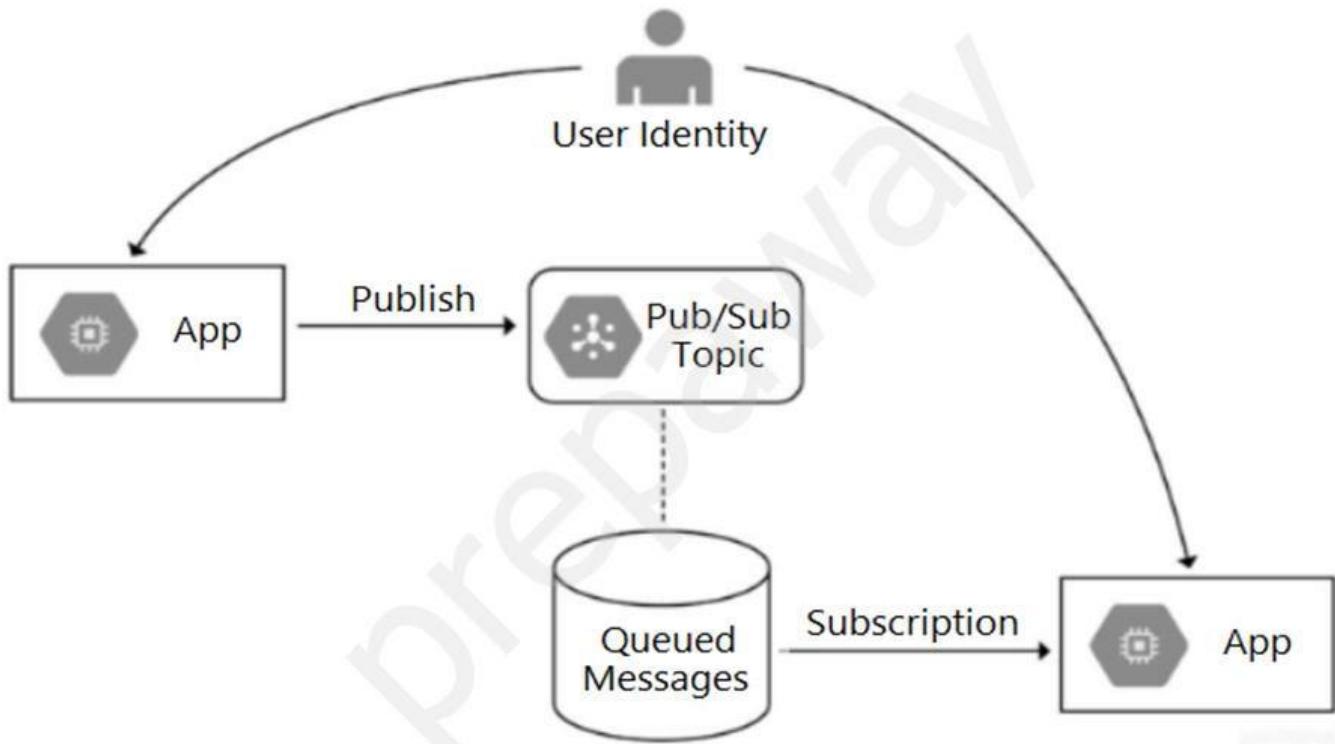
upvoted 3 times

Question #123

*Topic 1*

Your team is developing an application in Google Cloud that executes with user identities maintained by Cloud Identity. Each of your application's users will have an associated Pub/Sub topic to which messages are published, and a Pub/Sub subscription where the same user will retrieve published messages. You need to ensure that only authorized users can publish and subscribe to their own specific Pub/Sub topic and

subscription. What should you do?



- A. Bind the user identity to the pubsub.publisher and pubsub.subscriber roles at the resource level.
- B. Grant the user identity the pubsub.publisher and pubsub.subscriber roles at the project level.
- C. Grant the user identity a custom role that contains the pubsub.topics.create and pubsub.subscriptions.create permissions.
- D. Configure the application to run as a service account that has the pubsub.publisher and pubsub.subscriber roles.

**Correct Answer: C**

*Community vote distribution*

A (100%)

\_\_rajan\_\_ 7 months, 1 week ago

**Selected Answer: A**

A is correct.

upvoted 1 times

purushi 8 months, 3 weeks ago

**Selected Answer: A**

Granting IAM at resource level is enough.

If project level permission is given then user will be having publisher and subscriber roles for all the pub-sub topics created within the project. this should be avoided according to the question asked.

upvoted 1 times

Pime13 1 year, 2 months ago

**Selected Answer: A**

A -> resource level

upvoted 1 times

✉️  **omermahgoub** 1 year, 3 months ago

**Selected Answer: A**

A. Bind the user identity to the pubsub.publisher and pubsub.subscriber roles at the resource level.

By binding the user identity to the pubsub.publisher and pubsub.subscriber roles at the resource level, you can ensure that each user can only publish and subscribe to their specific Pub/Sub topic and subscription. This allows for granular permissions management and ensures that each user can only access the resources they are authorized to.

The other options are not suitable in this case because,

upvoted 2 times

✉️  **omermahgoub** 1 year, 3 months ago

B. Granting the user identity the pubsub.publisher and pubsub.subscriber roles at the project level would give the user access to all topics and subscriptions within the project and not specific to a user.

C. Granting the user identity a custom role that contains the pubsub.topics.create and pubsub.subscriptions.create permissions would allow the user to create topics and subscriptions but not access to their specific topic or subscription.

D. Configuring the application to run as a service account that has the pubsub.publisher and pubsub.subscriber roles would not provide granular permissions management for the user.

upvoted 2 times

✉️  **TNT87** 1 year, 2 months ago

why do you write all these compositions , you write unnecessary paragraphs always, as if we don't have documents and often times you will be giving wrong explanations. I believe just pasting a link to support your answer is enough as well have access to the documentation

upvoted 2 times

✉️  **TNT87** 1 year, 2 months ago

believe

upvoted 1 times

✉️  **zellick** 1 year, 4 months ago

**Selected Answer: A**

A is the answer.

upvoted 1 times

✉️  **tomato123** 1 year, 8 months ago

**Selected Answer: A**

Question #124

Topic 1

You are evaluating developer tools to help drive Google Kubernetes Engine adoption and integration with your development environment, which includes VS Code and IntelliJ. What should you do?

- A. Use Cloud Code to develop applications.
- B. Use the Cloud Shell integrated Code Editor to edit code and configuration files.
- C. Use a Cloud Notebook instance to ingest and process data and deploy models.
- D. Use Cloud Shell to manage your infrastructure and applications from the command line.

**Correct Answer: A**

Reference:

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

*Community vote distribution*

A (100%)

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: A**

A is correct.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: A**

Google Cloud code plugin can be installed on IntelliJ and VS code IDEs.

This provides very flexibility for developer to work with GKE platform.

upvoted 2 times

 **Oleksii\_ki** 9 months, 4 weeks ago

**Selected Answer: A**

Cloud Code is a set of plugins for VS Code and IntelliJ that provides an integrated development experience for working with Kubernetes and Google Cloud

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: A**

A. Use Cloud Code to develop applications.

Cloud Code is a set of plugins for VS Code and IntelliJ that provides an integrated development experience for working with Kubernetes and Google Cloud. The plugins include features such as interactive cluster and resource management, one-click Kubernetes cluster creation, and built-in debugging and diagnostics. It also supports to quickly deploy and debug applications using the Kubernetes and Google Cloud SDKs. Also, it allows developers to easily perform tasks like deploying and debugging applications, managing resources, and running local development environments. Cloud Code is a great tool for teams looking to streamline their development process for Kubernetes and Google Cloud.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

The Cloud Shell integrated Code Editor is a command-line text editor that you can use to edit code and configuration files within the Cloud Shell environment. While it can be useful for small changes or quick tests, it may not provide the same level of functionality or convenience as a dedicated development environment such as VS Code or IntelliJ. Additionally, Cloud Shell is primarily intended for managing infrastructure and applications from the command line, and may not offer the best workflow or experience for developing applications. For these reasons, it may be more beneficial to use a more robust development environment like VS Code or IntelliJ to develop and manage your applications on the Google Kubernetes Engine.

upvoted 1 times

 **zelick** 1 year, 4 months ago

**Selected Answer: A**

A is the answer.

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

Cloud Code provides IDE support for the full development cycle of Kubernetes and Cloud Run applications, from creating and customizing a new application from sample templates to running your finished application. Cloud Code supports you along the way with run-ready samples, out-of-the-box configuration snippets, and a tailored debugging experience — making developing with Kubernetes and Cloud Run a whole lot easier.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: A**

A is correct

upvoted 3 times

 **GCPCloudArchitectUser** 2 years, 2 months ago

**Selected Answer: A**

Agreed with Option A ... referred link

upvoted 3 times

 **Blueocean** 2 years, 3 months ago

Agree with Option A

upvoted 3 times

the app, the application caches the user's information (e.g., session, name, address, preferences), which is stored for quick retrieval during checkout.

While testing your application in a browser, you get a 502 Bad Gateway error. You have determined that the application is not connecting to Memorystore. What is the reason for this error?

- A. Your Memorystore for Redis instance was deployed without a public IP address.
- B. You configured your Serverless VPC Access connector in a different region than your App Engine instance.
- C. The firewall rule allowing a connection between App Engine and Memorystore was removed during an infrastructure update by the DevOps team.
- D. You configured your application to use a Serverless VPC Access connector on a different subnet in a different availability zone than your App Engine instance.

**Correct Answer: A**

Reference:

<https://cloud.google.com/endpoints/docs/openapi/troubleshoot-response-errors>

*Community vote distribution*

B (67%)	C (19%)	14%
---------	---------	-----

 **ParagSanyashiv** Highly Voted 2 years, 3 months ago

**Selected Answer: B**

B is the correct answer in this case, A is wrong because according to the best practice and security purpose gcp doesn't allow public ip for re server.

upvoted 6 times

 **alpha\_canary** Most Recent 1 week, 4 days ago

**Selected Answer: B**

B: If you configured your Serverless VPC Access connector in a different region than your App Engine instance, this could cause connectivity issues. Serverless VPC Access connectors and the resources they connect to must be in the same region.

upvoted 1 times

 **theshant** 1 month, 1 week ago

C. The firewall rule allowing a connection between App Engine and Memorystore was removed during an infrastructure update by the DevOps team.

Here's why this scenario aligns with the error:

502 Bad Gateway: This error typically indicates that a server (in this case, App Engine) is unable to communicate with an upstream server (Memorystore for Redis) due to a configuration issue.

Firewall Rule Removal: If a firewall rule previously allowed App Engine to connect to Memorystore, removing it would block communication and cause the connection failure.

upvoted 1 times

 **kldn** 7 months, 1 week ago

**Selected Answer: B**

<https://cloud.google.com/vpc/docs/configure-serverless-vpc-access>

In the Region field, select a region for your connector. This must match the region of your serverless service.

If your service or job is in the region us-central or europe-west, use us-central1 or europe-west1.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: C**

1

1

The most likely reason for the 502 Bad Gateway error is that the firewall rule allowing a connection between App Engine and Memorystore was removed during an infrastructure update by the DevOps team.

This is because App Engine needs to be able to connect to Memorystore in order to retrieve the cached user information. If the firewall rule is removed, App Engine will not be able to connect to Memorystore and the application will fail.

upvoted 2 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: D**

502 Bad gateway issue is common more in App Engine Flexible environments than Std due to memory issues. Here I go with option D since pointing connector to a different subnet than App engine instance could cause Bad Gateway issue. A is not correct, because even with the different region with the same subnet, App engine instance do not get issues while connecting to Memeorystore.

upvoted 1 times

 **zanhsieh** 10 months, 2 weeks ago

**Selected Answer: C**

C.

A: No. The public IP is not mandatory.

B: No. App Engine instance region can be different with Serverless VPC Access connector.

Link here: <https://support.google.com/a/answer/10620692?hl=en> .

"We support VPC access connectors in 6 regions (us-central, us-west1, us-east1, asia-southeast1, asia-east1, and europe-west1). .... Note: Support for additional regions is coming soon." Although the document didn't mention directly, what if an app in App Engine in southamerica-east1-a would like to connect to Cloud SQL in us region? Note that the diagram here is REALLY mis-leading:

[https://cloud.google.com/vpc/docs/serverless-vpc-access#example\\_2](https://cloud.google.com/vpc/docs/serverless-vpc-access#example_2)

C: Yes. This is the only possible answer.

D: No. Serverless VPC Access connector shall be configured with a different subnet. See:

<https://cloud.google.com/vpc/docs/configure-serverless-vpc-access#console>

"Every connector requires its own /28 subnet to place connector instances on. A subnet cannot be used by other resources such as VMs, Private Service Connect, or load balancers."

upvoted 2 times

 **telp** 1 year, 3 months ago

**Selected Answer: B**

A is not correct because Cloud Run connects to Memorystore via the Serverless VPC Connector. Connections are over private networks. Public addresses are not required.

B is correct. All of the components must be in the same region.

C is not correct because for connectivity between Cloud Run and Memorystore all that is required is a Serverless VPN Connector.

D is not correct. The Serverless VPC Connector is configured with a non-overlapping subnet that is not associated with the VPC.

upvoted 2 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: D**

While both B and D refer to the configuration of the Serverless VPC Access connector and could potentially cause issues with the application's ability to connect to Memorystore, they are slightly different.

For B:

Having the connector in a different region than the App Engine instance could result in increased latency and potential connectivity issues, but would not necessarily prevent the App Engine instance from connecting to Memorystore.

For D:

This option is more specific and is indicating that if the connector is on a different subnet or availability zone from the App Engine instance, it could cause issues with the application's ability to connect to Memorystore. It is less likely for this situation to cause latency or performance issues, as it will affect the connectivity of the App Engine to Memorystore.

Both B and D refer to misconfiguration of the Serverless VPC Access connector, but option D is more specific and directly relates to connectivity issues and is more likely to be the root cause of the 502 Bad Gateway error encountered.

upvoted 2 times

👤 **zellick** 1 year, 4 months ago

**Selected Answer: B**

B is the answer.

[https://cloud.google.com/vpc/docs/serverless-vpc-access#how\\_it\\_works](https://cloud.google.com/vpc/docs/serverless-vpc-access#how_it_works)

Serverless VPC Access is based on a resource called a connector. A connector handles traffic between your serverless environment and your VPC network. When you create a connector in your Google Cloud project, you attach it to a specific VPC network and region. You can then configure your serverless services to use the connector for outbound network traffic.

upvoted 1 times

👤 **tomato123** 1 year, 8 months ago

**Selected Answer: B**

B is correct

upvoted 2 times

👤 **akshaychavan7** 1 year, 8 months ago

**Selected Answer: B**

Yes! This should be B

upvoted 1 times

Question #126

Topic 1

Your team develops services that run on Google Cloud. You need to build a data processing service and will use Cloud Functions. The data to be processed by the function is sensitive. You need to ensure that invocations can only happen from authorized services and follow Google-recommended best practices for securing functions. What should you do?

- A. Enable Identity-Aware Proxy in your project. Secure function access using its permissions.
- B. Create a service account with the Cloud Functions Viewer role. Use that service account to invoke the function.
- C. Create a service account with the Cloud Functions Invoker role. Use that service account to invoke the function.
- D. Create an OAuth 2.0 client ID for your calling service in the same project as the function you want to secure. Use those credentials to invoke the function.

**Correct Answer: C**

Reference:

<https://medium.com/google-cloud/how-to-securelyInvoke-a-cloud-function-from-google-kubernetes-engine-running-on-another-gcp-79797ec2b2c6>

*Community vote distribution*

C (67%)

A (17%)

D (17%)

👤 **fabiam93**  2 years, 1 month ago

**Selected Answer: C**

For me C. In link1 we can see how google suggests to use service accounts and in link2 we can see that the invoker role exists.  
Link1: <https://cloud.google.com/functions/docs/securing#authentication> Link2:

<https://cloud.google.com/functions/docs/reference/iam/roles#cloud-functions-roles>

upvoted 5 times

👤 **Aeglas**  5 months, 1 week ago

**Selected Answer: C**

IAP is not available for Cloud Functions, so the only possible option is C

upvoted 1 times

👤 **Aeglas** 5 months, 1 week ago

IAP is not available for Cloud Functions, so the only possible answer is C

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: A**

1

The best way to ensure that invocations of a Cloud Function that processes sensitive data can only happen from authorized services and follow Google-recommended best practices is to enable Identity-Aware Proxy in your project and secure function access using its permissions.

upvoted 1 times

 **Aeglas** 5 months, 1 week ago

IAP is not available for Cloud Functions

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: C**

Since this is service to service communication, cloud function invoker role should be provided to the service that wants to invoke cloud functions in the data processing pipeline.

upvoted 1 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: C**

vote c

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: A**

The best approach is to use a combination of authn, authz, and encryption

1. Enable IAP to ensure that only authenticated and authorized users or services can access Cloud Function
2. Set up an appropriate level of access control using IAM roles and policies, such as roles/cloudfunctions.invoker, to ensure that only authorized services can invoke your Cloud Function. This can be done by creating a service account for the calling function, assign the appropriate invoker role to the service account on the data processing function and use the service account credentials in the calling function
3. Use Google-provided libraries or resources, such as KMS or Cloud Storage, to encrypt and store sensitive data
4. Apply security best practices such as limiting the scope of the service account, and using Cloud IAP to protect access to your Cloud Function
5. consider using Cloud Event that ensure your function is triggered only by authorized events, you can use Cloud Event to ensure that your function is invoked only by specific event types that you have configured

upvoted 2 times

 **omermahgoub** 1 year, 3 months ago

Options B and D are not correct. The Cloud Functions Viewer role does not have the necessary permissions to invoke a Cloud Function and creating an OAuth 2.0 client ID for your calling service is not enough to secure a Cloud Function.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Option C is correct that creating a service account with the appropriate invoker role is one step in securing your Cloud Function, however it should be used in conjunction with other security measures.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Option A is correct in that it's important to enable IAP to ensure that only authenticated and authorized users or services can access your Cloud Function, but it's not enough by itself to secure your function.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

By following the above steps, you can ensure that your Cloud Function is secure and can only be invoked by authorized services.

upvoted 1 times

 **Aeglas** 5 months, 1 week ago

IAP is not available for Cloud Functions, so the correct answer is C

upvoted 1 times

 **zellck** 1 year, 4 months ago

**Selected Answer: C**

C is the answer.

<https://cloud.google.com/functions/docs/securing/authenticating>

upvoted 1 times

✉  **jcataluna** 1 year, 4 months ago

**Selected Answer: C**

C is correct

upvoted 1 times

✉  **TNT87** 1 year, 5 months ago

ANSWER C

<https://medium.com/google-cloud/how-to-securely-invoke-a-cloud-function-from-google-kubernetes-engine-running-on-another-gcp-79797ec2b2c6>

upvoted 4 times

✉  **tomato123** 1 year, 8 months ago

**Selected Answer: D**

I think D is correct

upvoted 1 times

✉  **akshaychavan7** 1 year, 8 months ago

**Selected Answer: C**

I will go with option C.

upvoted 1 times

✉  **mbenhassine1986** 1 year, 11 months ago

C :

[https://cloud.google.com/functions/docs/securing/authenticating#authenticating\\_function\\_to\\_function\\_calls](https://cloud.google.com/functions/docs/securing/authenticating#authenticating_function_to_function_calls)

upvoted 2 times

✉  **nqthien041292** 2 years ago

**Selected Answer: C**

Vote C

upvoted 1 times

✉  **KillerGoogle** 2 years, 1 month ago

I believe this is C

upvoted 1 times

✉  **GCPCloudArchitectUser** 2 years, 2 months ago

**Selected Answer: D**

Agreed D ...

From link reference below

The tokens themselves are created using the OAuth 2 framework, and its extension, Open Identity Connect, but the sequence is complex and error-prone, and the use of Cloud Client Libraries to manage the process is highly recommended.

upvoted 2 times

✉  **fabiam93** 2 years, 1 month ago

Why not C?

In link1 we can see how google suggests to use service accounts and in link2 we can see that the invoker role exists.

Link1: <https://cloud.google.com/functions/docs/securing#authentication>

Link2: <https://cloud.google.com/functions/docs/reference/iam/roles#cloud-functions-roles>

upvoted 2 times

✉  **ZOZOKOU** 2 years, 2 months ago

Option D.

<https://cloud.google.com/functions/docs/securing>

upvoted 2 times

Question #127

Topic 1

You are deploying your applications on Compute Engine. One of your Compute Engine instances failed to launch. What should you do? (Choose two.)

- A. Determine whether your file system is corrupted.
- B. Access Compute Engine as a different SSH user.
- C. Troubleshoot firewall rules or routes on an instance.
- D. Check whether your instance boot disk is completely full.
- E. Check whether network traffic to or from your instance is being dropped.

**Correct Answer:** DE

Reference:

<https://cloudacademy.com/course/deploying-applications-on-gcp-compute/deploying-applications-and-services-on-compute-engine/>

*Community vote distribution*

AD (100%)

 **alpha\_canary** 1 week, 4 days ago

**Selected Answer:** AD

A & D

[https://cloud.google.com/compute/docs/troubleshooting/vm-startup#identify\\_the\\_reason\\_why\\_the\\_boot\\_disk\\_isnt\\_booting](https://cloud.google.com/compute/docs/troubleshooting/vm-startup#identify_the_reason_why_the_boot_disk_isnt_booting)

Network issues shouldn't stop a compute engine from booting up so C & E are out.

B cant be true because how can u SSH if it doesnt boot

upvoted 1 times

 **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: AD**

I will go with AD.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: AD**

Compute engine will not launch when either of these happens.

- 1) When its file system is corrupted.
- 2) When its boot disk is full.

upvoted 1 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: AD**

[https://cloud.google.com/compute/docs/troubleshooting/vm-startup#identify\\_the\\_reason\\_why\\_the\\_boot\\_disk\\_isnt\\_booting](https://cloud.google.com/compute/docs/troubleshooting/vm-startup#identify_the_reason_why_the_boot_disk_isnt_booting)

- Verify that your boot disk is not full.

If your boot disk is completely full and your operating system does not support automatic resizing, you won't be able to connect to your instance. You must create a new instance and recreate the boot disk.

- Verify that your disk has a valid file system.

If your file system is corrupted or otherwise invalid, you won't be able to launch your instance.

upvoted 3 times

 **zellick** 1 year, 4 months ago

**Selected Answer: AD**

AD is the answer.

[https://cloud.google.com/compute/docs/troubleshooting/vm-startup#identify\\_the\\_reason\\_why\\_the\\_boot\\_disk\\_isnt\\_booting](https://cloud.google.com/compute/docs/troubleshooting/vm-startup#identify_the_reason_why_the_boot_disk_isnt_booting)

- Verify that your boot disk is not full.

If your boot disk is completely full and your operating system does not support automatic resizing, you won't be able to connect to your instance. You must create a new instance and recreate the boot disk.

- Verify that your disk has a valid file system.

If your file system is corrupted or otherwise invalid, you won't be able to launch your instance.

upvoted 3 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: AD**

AD are correct

upvoted 4 times

 **akshaychavan7** 1 year, 8 months ago

**Selected Answer: AD**

A and D seem right here.

upvoted 2 times

 **nqthien041292** 2 years ago

**Selected Answer: AD**

Vote AD

upvoted 3 times

 **Blueocean** 2 years, 3 months ago

Options D for sure , in the rest Option A seems the nearest one as one of the troubleshooting steps is to check the file system

upvoted 2 times

 **Ers0** 2 years, 3 months ago

A & D!

If the failure is on the launch changing the SSH user will not help. Network traffic, Network routes, Firewall rules...are not influencing the instance boot!

upvoted 2 times

✉️  **ParagSanyashiv** 2 years, 3 months ago

AD should be the correct one, because launching VM failure does not depends on network connectivity of that VM. Network comes into the picture when vm boots.

upvoted 3 times

✉️  **HotSpa27** 2 years, 3 months ago

I vote AD.

<https://cloud.google.com/compute/docs/troubleshooting/vm-startup>

Verify that your disk has a valid file system.

Verify that your boot disk is not full.

Question #128

Topic 1

Your web application is deployed to the corporate intranet. You need to migrate the web application to Google Cloud. The web application must be available only to company employees and accessible to employees as they travel. You need to ensure the security and accessibility of the web application while minimizing application changes. What should you do?

- A. Configure the application to check authentication credentials for each HTTP(S) request to the application.
- B. Configure Identity-Aware Proxy to allow employees to access the application through its public IP address.
- C. Configure a Compute Engine instance that requests users to log in to their corporate account. Change the web application DNS to point to the proxy Compute Engine instance. After authenticating, the Compute Engine instance forwards requests to and from the web application.
- D. Configure a Compute Engine instance that requests users to log in to their corporate account. Change the web application DNS to point to the proxy Compute Engine instance. After authenticating, the Compute Engine issues an HTTP redirect to a public IP address hosting the web application.

**Correct Answer: B**

*Community vote distribution*

B (63%)

C (37%)

✉️  **Blueocean**  2 years, 3 months ago

Agree with Option B

upvoted 9 times

✉️  **TNT87** 1 year, 5 months ago

why public IP yet it must only be accessible to the employees only? B is wrong

upvoted 2 times

✉️  **tuanbo91** 1 year, 4 months ago

it's Google public IP, <https://cloud.google.com/iap/docs/managing-access>

upvoted 1 times

✉️  **TNT87** 1 year, 4 months ago

If its B, it must not use public IP, That makes B wrong. the answer is C. its already in coorporate intranet, why use public IP?

upvoted 1 times

✉️  **mrvergara** 1 year, 2 months ago

How the users are going to authenticate to Compute Engine?

upvoted 1 times

✉️  **alpha\_canary**  1 week, 4 days ago

**Selected Answer: B**

B is the answer. IAP is the solution in these kind of scenarios.

Don't be alerted by mention of public IP. It's completely fine to deploy an internal app on public IP as long as u have proper authentication. Si the question mentions "accessible to employees as they travel", this is how many companies deploy such internal tools.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: B**

I will go with B.

upvoted 1 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: B**

i'd choose b: <https://cloud.google.com/blog/topics/developers-practitioners/control-access-your-web-sites-identity-aware-proxy>

upvoted 2 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: C**

This approach allows you to use Google Cloud infrastructure to authenticate users against the corporate intranet before providing access to the web application, without making major changes to the web application. By configuring a Compute Engine instance as a proxy and changing the web application's DNS to point to this proxy, you can ensure that only employees who have been authenticated against the corporate intranet are able to access the web application. This approach also allows the employees to access the web application while they are traveling, as long as they have internet access.

upvoted 2 times

 **omermahgoub** 1 year, 3 months ago

Identity-Aware Proxy (IAP) is a feature of Google Cloud Platform that allows you to secure access to resources by using identity and context-based access control. IAP allows you to restrict access to a resource (such as a web application) to only authenticated and authorized users or service accounts.

However, in this scenario, since the web application is hosted on the corporate intranet, it will not have a public IP address and it will not be accessible from the internet. And it's not possible to use IAP to restrict access to an intranet-hosted application by its IP address.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Additionally, IAP is designed to work with resources that are hosted on Google Cloud, and it may not be possible to configure it to work with an intranet-hosted application without making significant changes to the application and the intranet infrastructure.

That's why the best solution would be to use a VPN connection or a reverse proxy to allow employees to access the application as if they were on the intranet while they are traveling or to secure the access to the intranet-hosted web application from the internet.

upvoted 1 times

 **tuanbo91** 1 year, 4 months ago

**Selected Answer: B**

B is correct.

upvoted 3 times

 **zellick** 1 year, 4 months ago

**Selected Answer: B**

B is the answer.

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

IAP lets you establish a central authorization layer for applications accessed by HTTPS, so you can use an application-level access control model instead of relying on network-level firewalls.

IAP policies scale across your organization. You can define access policies centrally and apply them to all of your applications and resources. When you assign a dedicated team to create and enforce policies, you protect your project from incorrect policy definition or implementation in any application.

upvoted 2 times

 **micoams** 1 year, 4 months ago

**Selected Answer: B**

B, while employees are traveling, they don't have access to the intranet, so they need to use the public IP. IAP secures the public endpoint.

upvoted 3 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: C**

C seems right

upvoted 3 times

✉️  **akshaychavan7** 1 year, 8 months ago

**Selected Answer: C**

I would completely agree with BackendBoi's comment. I would have picked option B only if it would have not been said to access through public IP. Out of all the options, option C seems the best pick. I had read somewhere that the proxy compute engine is used for securing access to the compute engine instance hosting application.

upvoted 2 times

✉️  **BackendBoi** 2 years ago

I tend to C. A is bad because sending the credentials in each HTTP(s) request is bad and inefficient. B requires each user to have a Google Workspace account, which is not a given for the corporate intranet. On top of that there is no mention that the application checks for the token header, so a public IP would still expose the application. C would work, but it's ineffective. D is useless if the application is still exposed through the public IP. None of these solutions are great, but C is the least bad of the bunch.

upvoted 3 times

✉️  **dishum** 1 year, 11 months ago

You couldn't opt anyone? I suggest you to skip this in exam :)

upvoted 1 times

Question #129

*Topic 1*

You have an application that uses an HTTP Cloud Function to process user activity from both desktop browser and mobile application clients. This function will serve as the endpoint for all metric submissions using HTTP POST.

Due to legacy restrictions, the function must be mapped to a domain that is separate from the domain requested by users on web or mobile sessions. The domain for the Cloud Function is <https://fn.example.com>. Desktop and mobile clients use the domain <https://www.example.com>. You need to add a header to the function's

HTTP response so that only those browser and mobile sessions can submit metrics to the Cloud Function. Which response header should you add?

- A. Access-Control-Allow-Origin: \*
- B. Access-Control-Allow-Origin: [https://\\*.example.com](https://*.example.com)
- C. Access-Control-Allow-Origin: <https://fn.example.com>
- D. Access-Control-Allow-origin: <https://www.example.com>

**Correct Answer: A**

*Community vote distribution*

D (100%)

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: D**

D is correct.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: D**

It is like requesting service from front end to back-end service. Here front-end service domain is <https://www.example.com> and back-end service domain where cloud function runs is <https://fn.example.com>

upvoted 1 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: D**

vote d

upvoted 2 times

 **zellck** 1 year, 4 months ago

**Selected Answer: D**

D is the answer.

<https://cloud.google.com/functions/docs/samples/functions-http-cors>

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: D**

D is correct

upvoted 2 times

 **htakami** 2 years, 1 month ago

I agree with D but just a little detail (idk if it was a typo) ... the word "origin" must be "Origin"... besides that seems correct

upvoted 3 times

 **GCPCloudArchitectUser** 2 years, 2 months ago

**Selected Answer: D**

I agree it should be D

upvoted 4 times

 **Blueocean** 2 years, 3 months ago

Should be Option D, Option A will allow all and not only specific as requested in the question

upvoted 3 times

 **scaenruy** 2 years, 3 months ago

I vote D

upvoted 2 times

Question #130

Topic 1

You have an HTTP Cloud Function that is called via POST. Each submission's request body has a flat, unnested JSON structure containing numeric and text data. After the Cloud Function completes, the collected data should be immediately available for ongoing and complex analytics by many users in parallel. How should you persist the submissions?

- A. Directly persist each POST request's JSON data into Datastore.
- B. Transform the POST request's JSON data, and stream it into BigQuery.

C. Transform the POST request's JSON data, and store it in a regional Cloud SQL cluster.

D. Persist each POST request's JSON data as an individual file within Cloud Storage, with the file name containing the request identifier.

**Correct Answer: D**

*Community vote distribution*

B (100%)

✉  **ParagSanyashiv** Highly Voted 2 years, 3 months ago

**Selected Answer: B**

B should be the correct one because question has mentioned for analytics of the data.  
upvoted 15 times

✉  **\_rajan\_** Most Recent 7 months, 1 week ago

**Selected Answer: B**

B is correct since we need to do complex analytics.  
upvoted 1 times

✉  **purushi** 8 months, 3 weeks ago

**Selected Answer: B**

The key here is "Collected data should be IMMEDIATELY available for ongoing and complex analytics", and hence option B is correct.  
upvoted 1 times

✉  **Pime13** 1 year, 2 months ago

**Selected Answer: B**

"data should be immediately available for ongoing and complex analytics" -> B  
upvoted 1 times

✉  **omermahgoub** 1 year, 3 months ago

**Selected Answer: B**

B. Transform the POST request's JSON data, and stream it into BigQuery.

BigQuery is a highly scalable data warehouse that is well suited for handling large amounts of data and complex analytics in near real-time. By streaming the JSON data from your Cloud Function directly into BigQuery, you can make the collected data immediately available for analytic many users in parallel. BigQuery support various data types including json, so you can store your request body without any transformation.

A. Directly persist each POST request's JSON data into Datastore.

Datastore is a NoSQL document database that can be used to store structured data, but it's not designed to handle the high volume of data t you need to analyze in near real-time. And it would require additional processing to be available for analysis.

upvoted 1 times

✉  **omermahgoub** 1 year, 3 months ago

C. Transform the POST request's JSON data, and store it in a regional Cloud SQL cluster.

Cloud SQL is a fully-managed MySQL, PostgreSQL, and SQL Server database service, which is more suited for transactional workloads, rather than for storing large amounts of data for analytics purposes.

upvoted 1 times

✉  **omermahgoub** 1 year, 3 months ago

Storing the data as individual files in Cloud Storage may not be the best approach for immediate and parallel analytics as it would require additional processing and data manipulation to make it available for analytics purposes.

upvoted 1 times

✉  **omermahgoub** 1 year, 3 months ago

D. Persist each POST request's JSON data as an individual file within Cloud Storage, with the file name containing the request identifier

upvoted 1 times

✉  **omermahgoub** 1 year, 3 months ago

A. Directly persist each POST request's JSON data into Datastore.

Datastore is a NoSQL document database that can be used to store structured data, but it's not designed to handle the high volume of da that you need to analyze in near real-time. And it would require additional processing to be available for analysis.

upvoted 1 times

 **zellick** 1 year, 4 months ago

**Selected Answer: B**

B is the answer.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: B**

B is correct

upvoted 2 times

 **GCPCloudArchitectUser** 2 years, 2 months ago

Option B... can't disagree enough Analytics = BigQuery

upvoted 2 times

 **Blueocean** 2 years, 3 months ago

Is between Option B and D. Option B talks about transforming JSON data but no where in question we get to understand this need. So even though is BigQuery for analytics purposes Option D is more suitable.

upvoted 2 times

Question #131

*Topic 1*

Your security team is auditing all deployed applications running in Google Kubernetes Engine. After completing the audit, your team discovers that some of the applications send traffic within the cluster in clear text. You need to ensure that all application traffic is encrypted as quickly as possible while minimizing changes to your applications and maintaining support from Google. What should you do?

- A. Use Network Policies to block traffic between applications.
- B. Install Istio, enable proxy injection on your application namespace, and then enable mTLS.
- C. Define Trusted Network ranges within the application, and configure the applications to allow traffic only from those networks.
- D. Use an automated process to request SSL Certificates for your applications from Let's Encrypt and add them to your applications.

**Correct Answer: A**

*Community vote distribution*

B (100%)

 **scaenruy** Highly Voted  2 years, 3 months ago

I vote B

<https://cloud.google.com/istio/docs/istio-on-gke/installing>  
(deprecated)

upvoted 8 times

 **Blueocean** 2 years, 3 months ago

<https://cloud.google.com/service-mesh/docs/by-example/mtls> option B

upvoted 6 times

 **Xoxoo** Most Recent  4 months ago

**Selected Answer: B**

Answer: B

Istio enhances the security of microservices by providing features such as mutual TLS (Transport Layer Security) authentication between services, access controls, and encryption of communication channels.

upvoted 2 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: B**

Istio is a service mesh that can be used to encrypt traffic between applications in a GKE cluster. It does this by injecting a sidecar proxy into each pod. The sidecar proxy intercepts all traffic to and from the pod and encrypts it using mTLS (mutual TLS).

upvoted 2 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: B**

Istio is suitable for providing cutting edge concerns to the services running in the GKE cluster. Istio provides security, fault tolerance and resiliency out of the box.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: B**

B. Install Istio, enable proxy injection on your application namespace, and then enable mTLS.

Istio is a service mesh that runs within your Kubernetes cluster and provides a set of features, such as traffic management, service discovery, automatic encryption of traffic between services using mutual Transport Layer Security (mTLS). By installing Istio and enabling proxy injection in your application namespace, you can quickly and easily enable mTLS for all traffic within the cluster without making changes to your applications. Once the proxy injection is enabled, Istio automatically adds the necessary sidecar proxies to each pod in the namespace and configures them to encrypt traffic.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

C. Define Trusted Network ranges within the application, and configure the applications to allow traffic only from those networks.  
It does not provide any encryption for the traffic, it only allows traffic from specific IP ranges.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

D. Use an automated process to request SSL Certificates for your applications from Let's Encrypt and add them to your applications.  
It can encrypt the traffic between the client and the application but it doesn't cover the traffic inside the cluster.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

A. Use Network Policies to block traffic between applications  
Network policies are used to control traffic between pods in the cluster, it can help to secure the communication but it doesn't provide any encryption

upvoted 1 times

 **zelliCK** 1 year, 4 months ago

**Selected Answer: B**

B is the answer.

<https://cloud.google.com/istio/docs/istio-on-gke/overview>

Istio gives you the following benefits:

- Secure service-to-service communication in a cluster with strong identity-based authentication and authorization.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: B**

B is correct

upvoted 3 times

 **jdx000** 1 year, 9 months ago

**Selected Answer: B**

B should work. It's the only answer with a solution without blocking or restricting the cluster traffic

upvoted 2 times

 **szl0144** 1 year, 11 months ago

B is correct

upvoted 2 times

 **yogi\_508** 2 years ago

will go with D. A,C are nowhere in context( traffic should be encrypted)  
if there is Anthos Service Mesh instead of Istio in B then it is definitely B.

upvoted 1 times

 **htakami** 2 years, 1 month ago

This question/answers are outdated... Google stopped supporting Istio implementations and suggest to migrate to ASM. Option B seems more reasonable, but depends on the date it was written.

upvoted 2 times

 **ParagSanyashiv** 2 years, 3 months ago

The question is not about blocking the traffic. D is the correct answer.

upvoted 2 times

Question #132

Topic 1

You migrated some of your applications to Google Cloud. You are using a legacy monitoring platform deployed on-premises for both on-premises and cloud-deployed applications. You discover that your notification system is responding slowly to time-critical problems in the cloud applications. What should you do?

- A. Replace your monitoring platform with Cloud Monitoring.
- B. Install the Cloud Monitoring agent on your Compute Engine instances.
- C. Migrate some traffic back to your old platform. Perform A/B testing on the two platforms concurrently.
- D. Use Cloud Logging and Cloud Monitoring to capture logs, monitor, and send alerts. Send them to your existing platform.

**Correct Answer: D**

*Community vote distribution*

D (89%)

11%

 **KillerGoogle**  2 years, 1 month ago

**Selected Answer: D**

He migrated only 'some' of applications, not all of them to GCP.

upvoted 8 times

 **\_rajan\_**  7 months, 1 week ago

**Selected Answer: D**

I will go with D.

upvoted 1 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: D**

D, but if solution used is GCE logging and monitoring wouldn't be there since GCE do not have direct integration.

i feel this question might be "incomplete"

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: D**

D. Use Cloud Logging and Cloud Monitoring to capture logs, monitor, and send alerts. Send them to your existing platform. is a valid option if your aim to integrate the on-premise monitoring platform with the cloud monitoring platform, this way you can have a holistic view of all your application performance.

You can also use Google Cloud's Stackdriver service to integrate the monitoring, logging and tracing across both on-premise and cloud. Stackdriver can be used to get unified view of all your application performance and trace the root cause of an issue.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

not all of the applications have been migrated, in this scenario, a hybrid monitoring solution would be a good approach. You can keep using the legacy on-premises monitoring platform for the on-premises applications, and use Google Cloud Monitoring for the cloud-deployed applications. This approach would allow you to maintain visibility into both on-premises and cloud-deployed applications in a single monitoring interface, and send alerts to a centralized notification system.

You can use Cloud Monitoring to discover resources running in your on-premises infrastructure by using the Cloud Monitoring Agent that can be installed on the machines running on-premises. It will help you to monitor on-premise machines with Cloud Monitoring.

upvoted 1 times

 **zellick** 1 year, 4 months ago

**Selected Answer: D**

D is the answer.

upvoted 1 times

 **[Removed]** 1 year, 7 months ago

**Selected Answer: D**

Not all applications were migrated

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: D**

D is correct

upvoted 2 times

 **nqthien041292** 2 years ago

**Selected Answer: D**

Vote D

upvoted 1 times

 **GCPCloudArchitectUser** 2 years, 2 months ago

**Selected Answer: A**

I vote for A

upvoted 2 times

 **Blueocean** 2 years, 3 months ago

Agree with Option D

upvoted 4 times

Question #133

Topic 1

You recently deployed your application in Google Kubernetes Engine, and now need to release a new version of your application. You need the ability to instantly roll back to the previous version in case there are issues with the new version. Which deployment model should you use?

- A. Perform a rolling deployment, and test your new application after the deployment is complete.
- B. Perform A/B testing, and test your application periodically after the new tests are implemented.
- C. Perform a blue/green deployment, and test your new application after the deployment is. complete.
- D. Perform a canary deployment, and test your new application periodically after the new version is deployed.

**Correct Answer: D**

*Community vote distribution*

C (100%)

 **Blueocean**  2 years, 3 months ago

Option C is correct

upvoted 8 times

 **\_rajan\_**  7 months, 1 week ago

**Selected Answer: C**

C is correct.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: C**

The key here is rolling back to the previous deployments if we find issues with the current(latest) deployment. With Canary, only certain portion of the traffic is allowed to newer version that does on the fly testing. With A/B, certain portion of the traffic is split to the dedicated testers to confirm everything is fine with the newer version.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: C**

C. Perform a blue/green deployment, and test your new application after the deployment is complete.

A Blue/Green deployment is a technique that allows you to release new versions of an application while maintaining the ability to roll back to the previous version if there are issues. It works by having two identical production environments: one, the "green" environment, that is serving traffic, and another, the "blue" environment, that is idle. When you want to release a new version of your application, you deploy it to the "blue" environment, test it to make sure it is working as expected and then switch traffic to the "blue" environment.

This way you can have zero-downtime deployment and if there's any issues with the new version you can easily roll back to the previous version by switching the traffic back to the green environment.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

B. Perform A/B testing, and test your application periodically after the new tests are implemented.

A/B testing is used to test different versions of an application; it doesn't provide an instant rollback in case of issues.

upvoted 2 times

 **omermahgoub** 1 year, 3 months ago

A. Perform a rolling deployment, and test your new application after the deployment is complete.

This model does not allow an instant rollback as it does not have a parallel environment to switch traffic to.

upvoted 2 times

 **omermahgoub** 1 year, 3 months ago

D. Perform a canary deployment, and test your new application periodically after the new version is deployed.

Canary deployment is similar to blue/green deployment but in this approach it's rolling out the new version of application gradually, it's used to test the new version with a small percentage of the traffic before rolling it out to the entire environment, if there are issues it's harder to roll back since it's already rolled out to some of the users.

upvoted 2 times

 **zellick** 1 year, 4 months ago

**Selected Answer: C**

C is the answer.

[https://cloud.google.com/architecture/application-deployment-and-testing-strategies#choosing\\_the\\_right\\_strategy](https://cloud.google.com/architecture/application-deployment-and-testing-strategies#choosing_the_right_strategy)

upvoted 1 times

 **tab02733** 1 year, 6 months ago

**Selected Answer: C**

ABCD can roll back.

C the answer becomes because the condition must be an immediate rollback.

[https://cloud.google.com/architecture/application-deployment-and-testing-strategies#choosing\\_the\\_right\\_strategy](https://cloud.google.com/architecture/application-deployment-and-testing-strategies#choosing_the_right_strategy)

upvoted 1 times

 **tab02733** 1 year, 6 months ago

immediate -> instant

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: C**

C seems correct

upvoted 2 times

 **americoleonardo** 1 year, 11 months ago

**Selected Answer: C**

Agree with b/g deployment

upvoted 1 times

✉  **nqthien041292** 2 years ago

**Selected Answer: C**

Vote C

upvoted 1 times

✉  **Ers0** 2 years, 3 months ago

In my opinion is C!

D could work but we do not have detailed information about the traffic (synthetic or not, if we want to move it gradually or not...) for this reason  
Blue/Green is probably enough

upvoted 3 times

✉  **scaenruy** 2 years, 3 months ago

I vote C

upvoted 2 times

Question #134

*Topic 1*

You developed a JavaScript web application that needs to access Google Drive's API and obtain permission from users to store files in their Google Drives. You need to select an authorization approach for your application. What should you do?

- A. Create an API key.
- B. Create a SAML token.
- C. Create a service account.
- D. Create an OAuth Client ID.

**Correct Answer: D**

Reference:

<https://developers.google.com/drive/api/v3/about-auth>

*Community vote distribution*

D (89%)

11%

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: C**

OAuth 2.0 is an authorization framework that enables applications to obtain limited access to user accounts on an HTTP service, such as Google Drive. OAuth 2.0 is the preferred authorization approach for JavaScript web applications because it provides a secure and user-friendly way to obtain permission from users to access their Google Drive accounts.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

Wrongly Selected C It should be D.

OAuth 2.0 is an authorization framework that enables applications to obtain limited access to user accounts on an HTTP service, such as Google Drive. OAuth 2.0 is the preferred authorization approach for JavaScript web applications because it provides a secure and user-friendly way to obtain permission from users to access their Google Drive accounts.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: D**

We need to have OAuth 2.0 flow. The client app should have client ID and secret key generated from Google Drive application. This way the user can log in to their Google Drive account and can perform CRUD operations. The best thing here is, the client app is not aware of the user credentials, and it is very secure. The most common way of getting access token is from authorization code flow with PKCE. PKCE, since it is a JS client app.

upvoted 2 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: D**

D. Create an OAuth Client ID.

OAuth is an authorization framework that allows third-party applications to access resources on behalf of a user, without having to handle the user's credentials. To use Google Drive's API, your application needs to obtain permission from the user to access their Google Drive, and the best way to do this is through OAuth.

You would need to create an OAuth 2.0 client ID and integrate it into your application. This will allow your application to redirect users to the Google OAuth 2.0 server, where they can grant permission to your application to access their Google Drive.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

- A. Create an API key is not secure enough to give the permission of the user Google Drive access
- B. Create a SAML token: SAML is used for identity and access management, it doesn't give access to user's Google Drive.
- C. Create a service account: Service account is used for server-to-server communication, it doesn't allow for user-level access to their Google Drive.

upvoted 1 times

 **zellck** 1 year, 4 months ago

**Selected Answer: D**

D is the answer.

<https://developers.google.com/drive/api/guides/api-specific-auth>

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: D**

D is correct

upvoted 3 times

 **akshaychavan7** 1 year, 8 months ago

**Selected Answer: D**

Yes! it's D.

upvoted 1 times

 **jitu028** 2 years ago

Correct answer - D

upvoted 1 times

 **Blueocean** 2 years, 3 months ago

Option D

<https://developers.google.com/drive/api/v3/about-auth>

upvoted 4 times

You manage an ecommerce application that processes purchases from customers who can subsequently cancel or change those purchases. You discover that order volumes are highly variable and the backend order-processing system can only process one request at a time. You want to ensure seamless performance for customers regardless of usage volume. It is crucial that customers' order update requests are performed in the sequence in which they were generated. What should you do?

- A. Send the purchase and change requests over WebSockets to the backend.
- B. Send the purchase and change requests as REST requests to the backend.
- C. Use a Pub/Sub subscriber in pull mode and use a data store to manage ordering.
- D. Use a Pub/Sub subscriber in push mode and use a data store to manage ordering.

**Correct Answer: B***Community vote distribution*

C (100%)

 **scaenruy** Highly Voted 2 years, 3 months ago

I vote C

<https://cloud.google.com/pubsub/docs/pull>

upvoted 9 times

 **Blueocean** 2 years, 3 months ago

Agreed considering only one request can be processed at a time

upvoted 2 times

 **Blueocean** 2 years, 3 months ago

And there are a large number of incoming requests Pub Sub is needed

upvoted 3 times

 **\_rajan\_** Most Recent 7 months, 1 week ago

**Selected Answer: C**

C is correct.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: C**

Pull model so that application handle the requests by pulling requests one by one. This is called event driven architecture where the response client from the app will happen asynchronously.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: C**

C. Use a Pub/Sub subscriber in pull mode and use a data store to manage ordering.

To ensure that customer order update requests are performed in the sequence in which they were generated, the recommended approach is to use a Pub/Sub subscriber in pull mode, together with a data store to manage ordering.

This approach allows the backend system to process requests one at a time, while maintaining the order of requests. By using a pull-based subscription, the backend system can control the rate at which messages are consumed from the Pub/Sub topic, and can ensure that requests are processed in the correct order. The data store can be used to maintain a queue of requests, where each request is added to the queue in order that it was generated, and then processed by the backend system.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

A. Send the purchase and change requests over WebSockets to the backend.

WebSockets are a protocol for bidirectional communication between a client and server, it may not ensure that requests are processed in the order they were generated.

B. Send the purchase and change requests as REST requests to the backend.

Sending the request as REST does not ensure that requests are processed in the order they were generated, it also would not allow controlling the rate at which requests are consumed.

D. Use a Pub/Sub subscriber in push mode and use a data store to manage ordering.

Push-based subscription doesn't allow controlling the rate at which requests are consumed, it also may not ensure that requests are processed in the order they were generated.

upvoted 1 times

 **zellck** 1 year, 4 months ago

**Selected Answer: C**

C is the answer.

upvoted 1 times

 **tomato123** 1 year, 8 months ago

**Selected Answer: C**

C is correct

upvoted 2 times

 **jdx000** 1 year, 9 months ago

**Selected Answer: C**

Correct answer C

upvoted 1 times

Question #136

Topic 1

Your company needs a database solution that stores customer purchase history and meets the following requirements:

- ⇒ Customers can query their purchase immediately after submission.
- ⇒ Purchases can be sorted on a variety of fields.
- ⇒ Distinct record formats can be stored at the same time.

Which storage option satisfies these requirements?

- A. Firestore in Native mode
- B. Cloud Storage using an object read
- C. Cloud SQL using a SQL SELECT statement
- D. Firestore in Datastore mode using a global query

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **Blueocean**  2 years, 3 months ago

Agree with Option A

<https://cloud.google.com/datastore/docs/firestore-or-datastore>

upvoted 5 times

✉  **\_\_rajan\_\_** Most Recent 7 months, 1 week ago

**Selected Answer: A**

The answer is A. Firestore in Native mode.

Firestore in Native mode is a NoSQL document database that is designed for scalability, performance, and ease of use. It is a good choice for storing customer purchase history because it meets all of the requirements

upvoted 1 times

✉  **purushi** 8 months, 3 weeks ago

**Selected Answer: A**

Firestore is for storing semi structured data. It is optimized for high reads and low writes. Since each document can store different collection types, ( MONGO DB ), fire store is suitable for the above requirements.

upvoted 2 times

✉  **omermahgoub** 1 year, 3 months ago

**Selected Answer: A**

A. Firestore in Native mode

Firestore in Native mode satisfies these requirements. It is a NoSQL document database, which means that it stores semi-structured data, and each document can have its own fields and structure. This allows for storing distinct record formats at the same time, which is a requirement. Firestore also has strong query performance and support, customers can query their purchase immediately after submission, and purchases can be sorted on a variety of fields, it is highly optimized to support real-time queries, you can retrieve data with low latency.

upvoted 1 times

✉  **omermahgoub** 1 year, 3 months ago

B. Cloud Storage using an object read

Cloud Storage is an object storage service and it is not optimized for real-time queries as it does not support secondary indexes or SQL-like queries.

C. Cloud SQL using a SQL SELECT statement

Cloud SQL is a relational database service that supports SQL statements and it would be possible to use SQL SELECT statements to sort purchase by different fields but it is not optimized for real-time queries and the distinct record formats may be challenging to implement.

D. Firestore in Datastore mode using a global query

Firestore in Datastore mode is a previous generation of Firestore and it does not support the same level of query support and performance as Firestore in Native mode, it may also face challenges to support real-time query and distinct record formats.

upvoted 1 times

✉  **zelliCK** 1 year, 4 months ago

**Selected Answer: A**

A is the answer.

upvoted 2 times

✉  **[Removed]** 1 year, 7 months ago

@megn they mean that each record can have a different shape, the data is not consistent.

upvoted 1 times

✉  **tomato123** 1 year, 8 months ago

**Selected Answer: A**

A is correct

upvoted 2 times

 **nehaxlpb** 1 year, 9 months ago

**Selected Answer: A**

Firestore is the next major version of Datastore and a re-branding of the product. Taking the best of Datastore and the Firebase Realtime Database, Firestore is a NoSQL document database built for automatic scaling, high performance, and ease of application development.

Firestore introduces new features such as:

A new, strongly consistent storage layer

A collection and document data model

Real-time updates

Mobile and Web client libraries

Firestore is backwards compatible with Datastore, but the new data model, real-time updates, and mobile and web client library features are r

To access all of the new Firestore features, you must use Firestore in Native mode.

upvoted 3 times

 **[Removed]** 1 year, 11 months ago

What do they mean by "Distinct record formats"?

upvoted 1 times

 **szl0144** 1 year, 11 months ago

firestore native mode:

A new, strongly consistent storage layer

A collection and document data model

Real-time updates

Mobile and Web client libraries

upvoted 3 times

Question #137

Topic 1

You recently developed a new service on Cloud Run. The new service authenticates using a custom service and then writes transactional information to a Cloud

Spanner database. You need to verify that your application can support up to 5,000 read and 1,000 write transactions per second while identifying any bottlenecks that occur. Your test infrastructure must be able to autoscale. What should you do?

- A. Build a test harness to generate requests and deploy it to Cloud Run. Analyze the VPC Flow Logs using Cloud Logging.
- B. Create a Google Kubernetes Engine cluster running the Locust or JMeter images to dynamically generate load tests. Analyze the results using Cloud Trace.
- C. Create a Cloud Task to generate a test load. Use Cloud Scheduler to run 60,000 Cloud Task transactions per minute for 10 minutes. Analyze the results using Cloud Monitoring.
- D. Create a Compute Engine instance that uses a LAMP stack image from the Marketplace, and use Apache Bench to generate load tests against the service. Analyze the results using Cloud Trace.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **scaenruy** Highly Voted  2 years, 3 months ago

I vote B

<https://cloud.google.com/architecture/distributed-load-testing-using-gke>

upvoted 6 times

 **\_rajan\_** Most Recent  7 months, 1 week ago

Selected Answer: B

B is correct.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

Selected Answer: B

The key here is "Your test infrastructure must be able to autoscale" and load testing.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Selected Answer: B

B. Create a Google Kubernetes Engine cluster running the Locust or JMeter images to dynamically generate load tests. Analyze the results us Cloud Trace.

To verify that your application can support up to 5,000 read and 1,000 write transactions per second and to identify any bottlenecks that occur you can use a load testing tool such as Locust or JMeter to generate load tests on your Cloud Run service. These tools allow you to simulate high number of concurrent requests and help you determine the maximum number of requests your service can handle.

You can run the load testing tool on a Google Kubernetes Engine (GKE) cluster which will support autoscale feature, this way you can handle high number of requests, and use Cloud Trace to analyze the results, which will give you insights into the performance and any bottlenecks.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

A. Build a test harness to generate requests and deploy it to Cloud Run. Analyze the VPC Flow Logs using Cloud Logging. VPC flow logs would not provide the transaction details, it's more useful to troubleshoot issues at the network level.

C. Create a Cloud Task to generate a test load. Use Cloud Scheduler to run 60,000 Cloud Task transactions per minute for 10 minutes. Analyze the results using Cloud Monitoring.

Although cloud task is a good solution for scheduling the test loads, it's not the best solution for load testing since it doesn't support dynamic loading and it would be hard to get the fine-grained details about the performance.

D. Create a Compute Engine instance that uses a LAMP stack image from the Marketplace, and use Apache Bench to

upvoted 1 times

 **zellck** 1 year, 4 months ago

Selected Answer: B

B is the answer.

<https://cloud.google.com/architecture/distributed-load-testing-using-gke>

upvoted 1 times

 **tomato123** 1 year, 8 months ago

Selected Answer: B

B is correct

upvoted 2 times

 **nehaxlpb** 1 year, 9 months ago

Selected Answer: B

This tutorial explains how to use Google Kubernetes Engine (GKE) to deploy a distributed load testing framework that uses multiple containers to create traffic for a simple REST-based API. This tutorial load-tests a web application deployed to App Engine that exposes REST-style endpoints to respond to incoming HTTP POST requests.

You can use this same pattern to create load testing frameworks for a variety of scenarios and applications, such as messaging systems, data stream management systems, and database systems.

upvoted 1 times

 **dishum** 2 years ago

Correct answer is B

upvoted 1 times

Question #138

Topic 1

You are using Cloud Build for your CI/CD pipeline to complete several tasks, including copying certain files to Compute Engine virtual machines. Your pipeline requires a flat file that is generated in one builder in the pipeline to be accessible by subsequent builders in the same pipeline. How should you store the file so that all the builders in the pipeline can access it?

- A. Store and retrieve the file contents using Compute Engine instance metadata.
- B. Output the file contents to a file in /workspace. Read from the same /workspace file in the subsequent build step.
- C. Use gsutil to output the file contents to a Cloud Storage object. Read from the same object in the subsequent build step.
- D. Add a build argument that runs an HTTP POST via curl to a separate web server to persist the value in one builder. Use an HTTP GET via curl from the subsequent build step to read the value.

**Correct Answer:** D

*Community vote distribution*

B (100%)

 **scaenruy** Highly Voted 2 years, 3 months ago

I vote B

<https://cloud.google.com/build/docs/build-config-file-schema>

upvoted 10 times

 **purush** Most Recent 8 months, 3 weeks ago

**Selected Answer: B**

Correct answer is B. Save your flat file under /workspace folder and hence the same file can be used for other build steps. Very simple and straight forward approach though. :)

upvoted 1 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: B**

I vote B

<https://cloud.google.com/build/docs/build-config-file-schema>

upvoted 1 times

👤 **omermahgoub** 1 year, 3 months ago

**Selected Answer: B**

The best approach is to output the file contents to a file in /workspace directory in one build step and read from the same /workspace file in the subsequent build step. This way, the file is easily accessible by all builders in the pipeline as they all run in the same environment and share the same file system. And it's the easiest and simplest way of sharing the file between the builds in the pipeline.

upvoted 1 times

👤 **zellick** 1 year, 4 months ago

**Selected Answer: B**

B is the answer.

[https://cloud.google.com/build/docs/configuring-builds/pass-data-between-steps#passing\\_data\\_using\\_workspaces](https://cloud.google.com/build/docs/configuring-builds/pass-data-between-steps#passing_data_using_workspaces)

To pass data between build steps, store the assets produced by the build step in /workspace and these assets will be available to any subsequent build steps.

upvoted 1 times

👤 **TNT87** 1 year, 5 months ago

[https://cloud.google.com/build/docs/configuring-builds/pass-data-between-steps#passing\\_data\\_using\\_workspaces](https://cloud.google.com/build/docs/configuring-builds/pass-data-between-steps#passing_data_using_workspaces)

<https://cloud.google.com/build/docs/configuring-builds/pass-data-between-steps>

upvoted 1 times

👤 **TNT87** 1 year, 5 months ago

Answer B

upvoted 1 times

👤 **cstempo** 1 year, 5 months ago

B is wrong

<https://cloud.google.com/build/docs/build-config-file-schema>

Use the dir field in a build step to set a working directory to use when running the step's container. If you set the dir field in the build step, the working directory is set to /workspace/<dir>. If this value is a relative path, it is relative to the build's working directory. If this value is absolute may be outside the build's working directory, in which case the contents of the path may NOT be persisted across build step executions

upvoted 1 times

👤 **TNT87** 1 year, 5 months ago

Ans B is correct

[https://cloud.google.com/build/docs/configuring-builds/pass-data-between-steps#passing\\_data\\_using\\_workspaces](https://cloud.google.com/build/docs/configuring-builds/pass-data-between-steps#passing_data_using_workspaces)

upvoted 1 times

👤 **TNT87** 1 year, 5 months ago

whatsa your answer then

upvoted 1 times

👤 **[Removed]** 1 year, 5 months ago

did you take the exam recently?

upvoted 1 times

👤 **tomato123** 1 year, 8 months ago

**Selected Answer: B**

B is correct

upvoted 2 times

👤 **nehaxlpb** 1 year, 9 months ago

**Selected Answer: B**

To pass data between build steps, store the assets produced by the build step in /workspace and these assets will be available to any subsequent build steps.

upvoted 1 times

👤 **americoleonardo** 1 year, 11 months ago

**Selected Answer: B**

agree with b

upvoted 1 times

 **mbenhassine1986** 1 year, 11 months ago

I Vote B

[https://cloud.google.com/build/docs/configuring-builds/pass-data-between-steps#passing\\_data\\_using\\_workspaces](https://cloud.google.com/build/docs/configuring-builds/pass-data-between-steps#passing_data_using_workspaces)

upvoted 1 times

Question #139

*Topic 1*

Your company's development teams want to use various open source operating systems in their Docker builds. When images are created in published containers in your company's environment, you need to scan them for Common Vulnerabilities and Exposures (CVEs). The scanning process must not impact software development agility. You want to use managed services where possible. What should you do?

- A. Enable the Vulnerability scanning setting in the Container Registry.
- B. Create a Cloud Function that is triggered on a code check-in and scan the code for CVEs.
- C. Disallow the use of non-commercially supported base images in your development environment.
- D. Use Cloud Monitoring to review the output of Cloud Build to determine whether a vulnerable version has been used.

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: A**

A is correct.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: A**

A is a very straight forward option. One more choice would be using vulnerability scanning tools like Grype ( open source ) in the build step its with cloud build.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: A**

A. Enable the Vulnerability scanning setting in the Container Registry would be the best solution in this case.

It would allow you to automatically scan images for known vulnerabilities and detect any issues as soon as they're pushed to the registry. This will help to identify vulnerabilities early in the development cycle, allowing the development teams to take action before images are deployed to production. This approach is automated, does not impact development agility and since it is a built-in feature of the Container Registry, it is a managed service and therefore, it does not require additional maintenance and management.

upvoted 2 times

 **omermahgoub** 1 year, 3 months ago

Option B, Create a Cloud Function that is triggered on a code check-in and scan the code for CVEs, would impact development agility as it would add an additional step to the development process which can slow down the development teams and impact the development process.

Option C, Disallow the use of non-commercially supported base images in the development environment, would limit the flexibility of the development teams, and they may not be able to use the best tools for the job which can negatively impact the quality of the end-product.

Option D, Use Cloud Monitoring to review the output of Cloud Build to determine whether a vulnerable version has been used, is a good practice to detect and alert on potential issues as soon as possible, but it is an additional step that needs to be set up and maintained. Additionally, it does not handle the vulnerability scanning on its own but rather acts as an additional layer of security.

upvoted 2 times

 **TNT87** 1 year, 4 months ago

<https://docs.docker.com/engine/scan/>

Answer A

upvoted 1 times

 **zellck** 1 year, 4 months ago

**Selected Answer: A**

A is the answer.

<https://cloud.google.com/container-analysis/docs/os-overview>

upvoted 1 times

Question #140

Topic 1

You are configuring a continuous integration pipeline using Cloud Build to automate the deployment of new container images to Google Kubernetes Engine (GKE). The pipeline builds the application from its source code, runs unit and integration tests in separate steps, and pushes the container to Container Registry. The application runs on a Python web server.

The Dockerfile is as follows:

```
FROM python:3.7-alpine -
```

```
COPY . /app -
```

```
WORKDIR /app -
```

```
RUN pip install -r requirements.txt
CMD [ "gunicorn", "-w 4", "main:app" ]
```

You notice that Cloud Build runs are taking longer than expected to complete. You want to decrease the build time. What should you do? (Choose two.)

- A. Select a virtual machine (VM) size with higher CPU for Cloud Build runs.
- B. Deploy a Container Registry on a Compute Engine VM in a VPC, and use it to store the final images.
- C. Cache the Docker image for subsequent builds using the -- cache-from argument in your build config file.
- D. Change the base image in the Dockerfile to ubuntu:latest, and install Python 3.7 using a package manager utility.
- E. Store application source code on Cloud Storage, and configure the pipeline to use gsutil to download the source code.

**Correct Answer:** CE

*Community vote distribution*

AC (100%)

 **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: AC**

AC is correct.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: AC**

Apart from A and C, one more good option would be to copy the app directory only after RUN pip install so that we can avoid this copying pa repeatedly after each layer build.

upvoted 1 times

 **telp** 1 year, 3 months ago

**Selected Answer: AC**

A is correct because a high-CPU virtual machine type can increase the speed of your build.

B is not correct because a Container Registry on a VM will not speed up the build.

C is correct because the same container is used in subsequent steps for testing and to be pushed to the registry.

D is not correct because an ubuntu container image will be significantly larger than the python:3.7-alpine image.

E is not correct because storing the application source code on Cloud Storage does not decrease the time to build the application.

upvoted 2 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: AC**

<https://cloud.google.com/build/docs/optimize-builds/increase-vcpu-for-builds>

[https://cloud.google.com/build/docs/optimize-builds/building-leaner-containers#building\\_leaner\\_containers](https://cloud.google.com/build/docs/optimize-builds/building-leaner-containers#building_leaner_containers)

Yes, answer A and C are both valid solutions based on the articles you linked.

Increasing the number of vCPUs allocated to the Cloud Build VM can help to decrease build time because it provides the build environment with more CPU resources to use, which can help to speed up the build process. This can be achieved by selecting a VM size with higher CPU for Cloud Build runs.

as mentioned, caching the Docker image for subsequent builds can also help to decrease build time by reusing previously built image layers. This can be achieved by adding the --cache-from argument to the build command in the build config file, which tells Cloud Build to use the specified images as a cache source.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Option E Storing application source code on Cloud Storage and configuring the pipeline to use gsutil to download the source code can also be a good way to optimize the pipeline. However, it may be less effective than option A and C, so it may be less beneficial to be chosen as a single solution.

In summary, option A and C are the best solutions that can help to optimize the CI/CD pipeline in this scenario as they directly impact the build process and it also depends on the current infrastructure and requirements of your pipeline if you consider using other options.

upvoted 1 times

 **TNT87** 1 year, 4 months ago

<https://cloud.google.com/build/docs/optimize-builds/increase-vcpu-for-builds>

Answer A

[https://cloud.google.com/build/docs/optimize-builds/building-leaner-containers#building\\_leaner\\_containers](https://cloud.google.com/build/docs/optimize-builds/building-leaner-containers#building_leaner_containers)

Answer C

upvoted 2 times

 **zellick** 1 year, 4 months ago

**Selected Answer: AC**

AC is the answer.

<https://cloud.google.com/build/docs/optimize-builds/increase-vcpu-for-builds>

By default, Cloud Build runs your builds on a standard virtual machine (VM). In addition to the standard VM, Cloud Build provides several high CPU VM types to run builds. To increase the speed of your build, select a machine with a higher vCPU to run builds. Keep in mind that although selecting a high vCPU machine increases your build speed, it may also increase the startup time of your build as Cloud Build only starts non-standard machines on demand.

[https://cloud.google.com/build/docs/optimize-builds/speeding-up-builds#using\\_a\\_cached\\_docker\\_image](https://cloud.google.com/build/docs/optimize-builds/speeding-up-builds#using_a_cached_docker_image)

The easiest way to increase the speed of your Docker image build is by specifying a cached image that can be used for subsequent builds. You can specify the cached image by adding the --cache-from argument in your build config file, which will instruct Docker to build using that image as a cache source.

upvoted 1 times

 **sharath25** 1 year, 4 months ago

**Selected Answer: AC**

A and C are correct

Question #141

Topic 1

You are building a CI/CD pipeline that consists of a version control system, Cloud Build, and Container Registry. Each time a new tag is pushed to the repository, a Cloud Build job is triggered, which runs unit tests on the new code, builds a new Docker container image, and pushes it into the Container Registry. The last step of your pipeline should deploy the new container to your production Google Kubernetes Engine (GKE) cluster. You need to select a tool and deployment strategy that meets the following requirements:

- Zero downtime is incurred
- Testing is fully automated
- Allows for testing before being rolled out to users
- Can quickly rollback if needed

What should you do?

- A. Trigger a Spinnaker pipeline configured as an A/B test of your new code and, if it is successful, deploy the container to production.
- B. Trigger a Spinnaker pipeline configured as a canary test of your new code and, if it is successful, deploy the container to production.
- C. Trigger another Cloud Build job that uses the Kubernetes CLI tools to deploy your new container to your GKE cluster, where you can perform a canary test.
- D. Trigger another Cloud Build job that uses the Kubernetes CLI tools to deploy your new container to your GKE cluster, where you can perform a shadow test.

**Correct Answer: D**

*Community vote distribution*

D (88%)

13%

 **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: B**

Spinnaker is a cloud native continuous delivery platform that can be used to deploy applications to a variety of cloud providers, including Google Kubernetes Engine (GKE). Spinnaker is a good choice for deploying applications to GKE because it provides a number of features that make it easy to deploy applications quickly and reliably, including:

Canary deployments: Canary deployments allow you to deploy a new version of your application to a small subset of users before rolling it out to all users. This allows you to test the new version of your application and identify any problems before they impact all of your users.

Rollback: Spinnaker can be used to quickly rollback to a previous version of your application if you encounter any problems with the new version.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: D**

Shadow testing is the right choice. Canary is not suitable here since the requirement is to test before rolling new version to users. Option A also comes very closer since it has A/B testing that is done only after releasing the newer version to users that is only a small amount of traffic is diverted to dedicated users (testers) who gives faster feedback about newer product/service.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: D**

Option D, triggering another Cloud Build job that uses the Kubernetes CLI tools to deploy your new container to your GKE cluster, where you perform a shadow test, could meet the requirements you specified.

Shadow testing is a technique where you can test the new version of an application by mirroring user traffic to it, without impacting the user requests to the current version. This way, you can test the new version of your application in a real-world environment with real user traffic, which allows for testing before being rolled out to users and allows for a quick rollback if needed. And with the use of Kubernetes CLI tools you can automate this process, so the testing and deployment is fully automated.

upvoted 2 times

 **zellck** 1 year, 4 months ago

**Selected Answer: D**

D is the answer.

[https://cloud.google.com/architecture/implementing-deployment-and-testing-strategies-on-gke#perform\\_a\\_shadow\\_test](https://cloud.google.com/architecture/implementing-deployment-and-testing-strategies-on-gke#perform_a_shadow_test)

With a shadow test, you test the new version of your application by mirroring user traffic from the current application version without impacting the user requests.

upvoted 1 times

 **test010101** 1 year, 4 months ago

**Selected Answer: D**

vote D

upvoted 1 times

 **gardislan18** 1 year, 4 months ago

**Selected Answer: D**

IMHO by eliminating

B and C - uses canary which letting the users use the new version without testing

A - canary is often a synonym of A/B testing

upvoted 2 times

Your operations team has asked you to create a script that lists the Cloud Bigtable, Memorystore, and Cloud SQL databases running within a project. The script should allow users to submit a filter expression to limit the results presented. How should you retrieve the data?

- A. Use the HBase API, Redis API, and MySQL connection to retrieve database lists. Combine the results, and then apply the filter to display the results
- B. Use the HBase API, Redis API, and MySQL connection to retrieve database lists. Filter the results individually, and then combine them to display the results
- C. Run gcloud bigtable instances list, gcloud redis instances list, and gcloud sql databases list. Use a filter within the application, and then display the results
- D. Run gcloud bigtable instances list, gcloud redis instances list, and gcloud sql databases list. Use --filter flag with each command, and then display the results

**Correct Answer: A**

*Community vote distribution*

D (100%)

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: D**

D is correct

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: D**

Easy and simple. List all the different types of instances and apply '--filter' option in a command.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: D**

Option D is correct, running gcloud bigtable instances list, gcloud redis instances list, and gcloud sql databases list and using the --filter flag each command can be used to filter the results before displaying them. This would allow users to submit a filter expression to limit the results presented as specified in the question. As per the google official documentation.

upvoted 1 times

 **TNT87** 1 year, 4 months ago

<https://cloud.google.com/sdk/gcloud/reference/topic/filters>

Answer D

upvoted 1 times

 **zellick** 1 year, 4 months ago

**Selected Answer: D**

D is the answer.

<https://cloud.aoole.com/sdk/acloud/reference/topic/filters>

Question #143

Topic 1

You need to deploy a new European version of a website hosted on Google Kubernetes Engine. The current and new websites must be accessed via the same HTTP(S) load balancer's external IP address, but have different domain names. What should you do?

- A. Define a new Ingress resource with a host rule matching the new domain
- B. Modify the existing Ingress resource with a host rule matching the new domain
- C. Create a new Service of type LoadBalancer specifying the existing IP address as the loadBalancerIP
- D. Generate a new Ingress resource and specify the existing IP address as the kubernetes.io/ingress.global-static-ip-name annotation value

**Correct Answer: A**

*Community vote distribution*

B (88%)

13%

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: B**

B is correct.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: B**

Right answer is B. Existing Ingress resource needs to be updated to add new domain for the new service that runs within the cluster of worker nodes. It looks like this:

User ----> HTTP(S) Load balance IP -----> Domain 1 -----> Older version of application.

-----> Domain 2 -----> New version of application.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: B**

Based on the requirements and the references

<https://kubernetes.io/docs/concepts/services-networking/ingress/#name-based-virtual-hosting>

<https://cloud.google.com/kubernetes-engine/docs/tutorials/configuring-domain-name-static-ip>

B. You should modify the existing Ingress resource with a host rule matching the new domain. This will allow you to route traffic to the new website while still using the same IP address and load balancer. This approach allows you to use name-based virtual hosting, which supports routing HTTP traffic to multiple host names at the same IP address. It also enables you to reuse the existing IP address and load balancer, which means that the existing website and the new website can be accessed through the same IP address while having different domain names.

upvoted 1 times

 **zellick** 1 year, 4 months ago

**Selected Answer: B**

B is the answer.

<https://kubernetes.io/docs/concepts/services-networking/ingress/#name-based-virtual-hosting>

Name-based virtual hosts support routing HTTP traffic to multiple host names at the same IP address.

upvoted 1 times

 **gardislan18** 1 year, 4 months ago

**Selected Answer: D**

Answer is D

<https://cloud.google.com/kubernetes-engine/docs/tutorials/configuring-domain-name-static-ip>

upvoted 1 times

 **kisswd** 1 year, 4 months ago

**Selected Answer: B**

"must be accessed via the same HTTP(S) load balancer's external IP address" means re-use the existing ingress resource

upvoted 3 times

You are developing a single-player mobile game backend that has unpredictable traffic patterns as users interact with the game throughout the day and night. You want to optimize costs by ensuring that you have enough resources to handle requests, but minimize over-provisioning. You also want the system to handle traffic spikes efficiently. Which compute platform should you use?

- A. Cloud Run
- B. Compute Engine with managed instance groups
- C. Compute Engine with unmanaged instance groups
- D. Google Kubernetes Engine using cluster autoscaling

**Correct Answer: B***Community vote distribution*

A (67%)

D (33%)

**✉️**  **alpha\_canary** 2 weeks ago**Selected Answer: A**

"handle traffic spikes efficiently"  
Cloud run the fastest to autoscale among the given options.  
GKE could be considered too, but Cloud Run is cheaper

upvoted 1 times

**✉️**  **wanrltw** 4 months, 3 weeks ago**Selected Answer: A**

Cloud Run is the cheapest solution among these options and can scale up and down to 0 instances.  
upvoted 1 times

**✉️**  **\_rajan\_** 7 months, 1 week ago**Selected Answer: D**

Google Kubernetes Engine (GKE) is a managed Kubernetes service that allows you to deploy and run containerized applications. GKE is a good choice for running a single-player mobile game backend because it can be easily scaled up or down to meet the needs of your game.  
Cloud Run is a serverless computing platform that allows you to run code without managing servers. Cloud Run is a good choice for running simple applications, but it is not as scalable as GKE.

upvoted 1 times

**✉️**  **purushi** 8 months, 3 weeks ago**Selected Answer: A**

I go with A. The requirement is to optimize the cost while scaling for unexpected spikes in the traffic. Cloud Run is the cheapest among all the other options given.  
upvoted 1 times

**✉️**  **allalla** 1 year ago**Selected Answer: D**

Bing chose D: For a single-player mobile game backend with unpredictable traffic patterns and a need to optimize costs while handling traffic spikes efficiently, Google Kubernetes Engine (GKE) using cluster autoscaling (option D) would be a good choice. GKE's cluster autoscaler automatically resizes the number of nodes in a node pool based on the demands of your workloads. This helps ensure that you have enough resources to handle requests while minimizing over-provisioning and optimizing costs.

upvoted 1 times

 **TNT87** 1 year, 4 months ago

Answer A

upvoted 1 times

 **Georgianaaa** 1 year, 4 months ago

Did you take the exam?

upvoted 1 times

 **TNT87** 1 year, 3 months ago

Not yet

upvoted 1 times

 **micoams** 1 year, 4 months ago

**Selected Answer: A**

Compute Engine answers are eliminated because they can't scale quickly enough.

GKE Answer is ruled out because you can end up overprovisioned, also cannot scale out to add more nodes quickly enough.

upvoted 4 times

 **zelliCK** 1 year, 4 months ago

**Selected Answer: A**

A is the answer.

upvoted 1 times

 **test010101** 1 year, 4 months ago

**Selected Answer: D**

vote D

upvoted 1 times

 **gardisan18** 1 year, 4 months ago

**Selected Answer: D**

Answer is D to lessen the over-provisioning

Not A - the app is not containerized

Not sure with Compute Engine

<https://cloud.google.com/blog/products/containers-kubernetes/gke-best-practices-to-lessen-over-provisioning>

upvoted 1 times

 **zelliCK** 1 year, 4 months ago

GKE requires app to be containerised.

upvoted 3 times

Question #145

Topic 1

The development teams in your company want to manage resources from their local environments. You have been asked to enable developer access to each team's Google Cloud projects. You want to maximize efficiency while following Google-recommended best practices. What should you do?

- A. Add the users to their projects, assign the relevant roles to the users, and then provide the users with each relevant Project ID.
- B. Add the users to their projects, assign the relevant roles to the users, and then provide the users with each relevant Project Number.
- C. Create groups, add the users to their groups, assign the relevant roles to the groups, and then provide the users with each relevant Project ID.
- D. Create groups, add the users to their groups, assign the relevant roles to the groups, and then provide the users with each relevant Project Number.

**Correct Answer: B***Community vote distribution*

C (100%)

  **alpha\_canary** 2 weeks ago**Selected Answer: C**

. Create groups, add the users to their groups, assign the relevant roles to the groups, and then provide the users with each relevant Project ID  
upvoted 1 times

  **\_\_rajan\_\_** 7 months, 1 week ago**Selected Answer: C**

This is the most efficient and secure way to enable developer access to Google Cloud projects. By creating groups and assigning roles to the groups, you can minimize the administrative overhead of managing user permissions. You can also provide developers with access to the projects they need, while limiting their access to other resources.

upvoted 1 times

  **purushi** 8 months, 3 weeks ago**Selected Answer: C**

I choose C. Adding users to a group and assigning the role to a group is a good practice as IAM is concerned. The project ID is the more user friendly identifier and the one which most Cloud APIs and user interfaces use when interfacing with you, the customer.

The project number is an internal implementation detail and is the key that most Google Cloud services use for storing data in their databases  
most API calls implicitly translate the ID to the number when performing queries for project details.

upvoted 1 times

  **TNT87** 1 year, 4 months ago

Answer C

upvoted 1 times

  **zellck** 1 year, 4 months ago**Selected Answer: C**

C is the answer.

upvoted 1 times

  **sharath25** 1 year, 4 months ago**Selected Answer: C**

option C

upvoted 1 times

  **test010101** 1 year, 4 months ago**Selected Answer: C**

vote C

upvoted 2 times

  **gardisan18** 1 year, 4 months ago**Selected Answer: C**

Best practice is to create a group  
not sure between project ID and project number  
upvoted 1 times

  **phil\_thain** 10 months, 2 weeks ago

What is the difference between C & D? I can use both project ID and project number to find a project in the GCP console

upvoted 1 times

Question #146

Topic 1

Your company's product team has a new requirement based on customer demand to autoscale your stateless and distributed service running in a Google Kubernetes Engine (GKE) cluster. You want to find a solution that minimizes changes because this feature will go live in two weeks. What should you do?

- A. Deploy a Vertical Pod Autoscaler, and scale based on the CPU load.
- B. Deploy a Vertical Pod Autoscaler, and scale based on a custom metric.
- C. Deploy a Horizontal Pod Autoscaler, and scale based on the CPU load.
- D. Deploy a Horizontal Pod Autoscaler, and scale based on a custom metric.

**Correct Answer: A**

*Community vote distribution*

C (92%)

8%

 **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: C**

C is correct.

upvoted 1 times

 **purush** 8 months, 3 weeks ago

**Selected Answer: C**

Since minimum number of changes, I go with C. Scaling based on the custom metrics might take more time compared to built in CPU load metric. Also, we need to see that application is stateless. So simple CPU metric is enough as a scaling parameter.

upvoted 1 times

 **abhishek\_verma1\_stl\_tech** 8 months, 3 weeks ago

Have you given the exam yet. Are these questions similar to actual exam questions?

upvoted 1 times

 **telp** 1 year, 3 months ago

**Selected Answer: C**

A. Incorrect: This doesn't help with a distributed application.

B. Incorrect: This would work, but would require Cloud Monitoring integration and possible application modification. This would also not apply a distributed application.

C. Correct: This will require the least number of changes to the code and fits the requirements.

D. Incorrect: This would work, but would require Cloud Monitoring integration and possible application modification.

upvoted 1 times

 **TNT87** 1 year, 4 months ago

Answer C

Scale based on the percent utilization of CPUs across nodes. This can be cost effective, letting you maximize CPU resource utilization. Because CPU usage is a trailing metric, however, your users might experience latency while a scale-up is in progress.

upvoted 1 times

 **zellick** 1 year, 4 months ago

**Selected Answer: C**

C is the answer.

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

The Horizontal Pod Autoscaler changes the shape of your Kubernetes workload by automatically increasing or decreasing the number of Pod response to the workload's CPU or memory consumption, or in response to custom metrics reported from within Kubernetes or external metrics from sources outside of your cluster.

upvoted 2 times

 **melisargh** 1 year, 4 months ago

**Selected Answer: C**

AB are wrong because it is recommended to start with HPA if you have nothing

D would take time and effort since you have to tune the metric

C is right because is the most simple entry level solution for autoscaling due the unknown new requirements

upvoted 3 times

 **TrainingProgram** 1 year, 4 months ago

**Selected Answer: D**

I think D is option.

upvoted 1 times

 **gardislan18** 1 year, 4 months ago

**Selected Answer: C**

there are too many typos here but if it is really typo then the answer is C

upvoted 3 times

 **ash\_meharun** 1 year, 4 months ago

Please share your views about why it's not D? Question doesn't say anything about increasing load utilization but about new(addition) requirements.

upvoted 1 times

 **zellck** 1 year, 4 months ago

scaling based on CPU load will be sufficient. you don't need to create custom metric.

upvoted 2 times

Question #147

*Topic 1*

Your application is composed of a set of loosely coupled services orchestrated by code executed on Compute Engine. You want your application to easily bring up new Compute Engine instances that find and use a specific version of a service. How should this be configured?

- A. Define your service endpoint information as metadata that is retrieved at runtime and used to connect to the desired service.
- B. Define your service endpoint information as label data that is retrieved at runtime and used to connect to the desired service.
- C. Define your service endpoint information to be retrieved from an environment variable at runtime and used to connect to the desired service.
- D. Define your service to use a fixed hostname and port to connect to the desired service. Replace the service at the endpoint with your new version.

**Correct Answer: C**

*Community vote distribution*

A (64%)

B (36%)

 **alpha\_canary** 2 weeks ago

**Selected Answer: A**

Go with A

why not B?

Labels are used for organizing Google Cloud resources, not for storing configuration data that your application needs to run.

upvoted 1 times

✉  **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: A**

The best answer is: A. Define your service endpoint information as metadata that is retrieved at runtime and used to connect to the desired service.

This is the most flexible and scalable way to configure your application to easily bring up new Compute Engine instances that find and use a specific version of a service.

upvoted 1 times

✉  **purush** 8 months, 3 weeks ago

**Selected Answer: A**

It is either A or C.

We can define a host URL as metadata in a virtual machine instance that orchestrates different services based on urls defined as metadata. C more way is to retrieve the urls from environment variables. Environment variables can be passed from,

- 1) command line
- 2) docker file
- 3) kubernetes deployment descriptor
- 4) through config server - application properties / yml file and so on.

The easier way is to define it as metadata in the compute engine instance itself.

upvoted 2 times

✉  **TQM\_9MD** 9 months ago

**Selected Answer: B**

I think B

upvoted 1 times

✉  **ryuhei** 12 months ago

**Selected Answer: B**

Answer is [B] .

upvoted 1 times

✉  **mrvergara** 1 year, 2 months ago

**Selected Answer: B**

An example of how you can retrieve the endpoint information from a label in Python:

```
import google.auth
from google.cloud import compute

# Authenticate and create a client for the Compute Engine API
credentials, project = google.auth.default()
compute_client = compute.Client(credentials=credentials, project=project)

# Get the instance based on the instance name
instance_name = "example-instance"
instance = compute_client.instance(instance_name)

# Get the endpoint information from the instance's labels
endpoint = instance.labels.get("endpoint")
```

upvoted 2 times

✉  **mrvergara** 1 year, 2 months ago

Answer is A:

Labels are used to categorize and organize resources in Google Cloud Platform, such as Compute Engine instances. While they can also be used to store endpoint information, they may not be as flexible as metadata when it comes to dynamically retrieving information at runtime. Additionally, labels are associated with individual resources, so updating the label data would require modifying the specific resource, rather than a centralized metadata store.

In some cases, using labels may be more appropriate, such as when you want to categorize and organize your resources, but for managing service endpoints in a loosely coupled architecture, metadata is generally a more flexible and scalable solution.

upvoted 4 times

 **TNT87** 1 year, 4 months ago

[https://cloud.google.com/apis/design/glossary#api\\_service\\_endpoint](https://cloud.google.com/apis/design/glossary#api_service_endpoint)

<https://cloud.google.com/compute/docs/metadata/overview>

Answer A

Answer A

upvoted 2 times

 **zelliCK** 1 year, 4 months ago

**Selected Answer: A**

A is the answer.

<https://cloud.google.com/service-infrastructure/docs/service-metadata/reference/rest#service-endpoint>

upvoted 2 times

 **gardislan18** 1 year, 4 months ago

**Selected Answer: A**

Correct Answer: A. best practice

B - There's no label data

C - harder to commit env?

D - not sure about this

upvoted 1 times

Question #148

Topic 1

You are developing a microservice-based application that will run on Google Kubernetes Engine (GKE). Some of the services need to access different Google Cloud APIs. How should you set up authentication of these services in the cluster following Google-recommended best practices? (Choose two.)

- A. Use the service account attached to the GKE node.
- B. Enable Workload Identity in the cluster via the gcloud command-line tool.
- C. Access the Google service account keys from a secret management service.
- D. Store the Google service account keys in a central secret management service.
- E. Use gcloud to bind the Kubernetes service account and the Google service account using roles/iam.workloadIdentity.

**Correct Answer: CE**

*Community vote distribution*

BE (100%)

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: BE**

BE is correct.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: BE**

I go with B and E. They are almost same.

upvoted 1 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: BE**

<https://cloud.google.com/kubernetes-engine/docs/how-to/workload-identity>

upvoted 1 times

 **telp** 1 year, 3 months ago

**Selected Answer: BE**

A is incorrect. While it could work, all the services are using the same service account, there is no separation of permissions, and no detailed logging.

B and E together connect GKE and Google service accounts, so GKE can authenticate a service with a Google service account.

C is incorrect. While this is feasible, it's not the recommended practice for workload identity because of the mandatory key rotation of the service accounts.

D is incorrect. While this is feasible, it's not the recommended practice for workload identity because of the mandatory key rotation of the service accounts.

E and B together connect GKE and Google service accounts, so GKE can authenticate a service with a Google service account.

upvoted 2 times

 **TNT87** 1 year, 4 months ago

[https://cloud.google.com/kubernetes-engine/docs/tutorials/authenticating-to-cloud-platform#use\\_workload\\_identity](https://cloud.google.com/kubernetes-engine/docs/tutorials/authenticating-to-cloud-platform#use_workload_identity)

Answer B

<https://cloud.google.com/kubernetes-engine/docs/how-to/kubernetes-service-accounts>

Answer E

upvoted 2 times

 **zelliCK** 1 year, 4 months ago

**Selected Answer: BE**

BE is the answer.

<https://cloud.google.com/kubernetes-engine/docs/how-to/workload-identity>

upvoted 2 times

Question #149

Topic 1

Your development team has been tasked with maintaining a .NET legacy application. The application incurs occasional changes and was recently updated. Your goal is to ensure that the application provides consistent results while moving through the CI/CD pipeline from environment to environment. You want to minimize the cost of deployment while making sure that external factors and dependencies between hosting environments are not problematic. Containers are not yet approved in your organization. What should you do?

- A. Rewrite the application using .NET Core, and deploy to Cloud Run. Use revisions to separate the environments.
- B. Use Cloud Build to deploy the application as a new Compute Engine image for each build. Use this image in each environment.
- C. Deploy the application using MS Web Deploy, and make sure to always use the latest, patched MS Windows Server base image in Compute

Engine.

D. Use Cloud Build to package the application, and deploy to a Google Kubernetes Engine cluster. Use namespaces to separate the environments.

**Correct Answer: A**

*Community vote distribution*

B (100%)

 **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: B**

B is correct.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: B**

The key is containers are not supported. The best possible option is, use cloud build to build the application and deploy under the virtual machine instance. Create a snapshot of the disk and create image out of it. Or create an image directly. Use this image as instance template for other environments.

upvoted 1 times

 **TNT87** 1 year, 4 months ago

**Selected Answer: B**

[https://cloud.google.com/architecture/modernization-path-dotnet-applications-google-cloud#take\\_advantage\\_of\\_compute\\_engine](https://cloud.google.com/architecture/modernization-path-dotnet-applications-google-cloud#take_advantage_of_compute_engine)  
The reason why B is better than D, hence had to paste the link above.

Answer B

upvoted 2 times

 **zellck** 1 year, 4 months ago

**Selected Answer: B**

B is the answer.

[https://cloud.google.com/architecture/modernization-path-dotnet-applications-google-cloud#phase\\_1\\_rehost\\_in\\_the\\_cloud](https://cloud.google.com/architecture/modernization-path-dotnet-applications-google-cloud#phase_1_rehost_in_the_cloud)  
upvoted 2 times

 **melisargh** 1 year, 4 months ago

**Selected Answer: B**

AD are wrong because containers are not yet approved!  
for the simplicity part i thinks is B

<https://cloud.google.com/architecture/modernization-path-dotnet-applications-google-cloud>

upvoted 3 times

The new version of your containerized application has been tested and is ready to deploy to production on Google Kubernetes Engine. You were not able to fully load-test the new version in pre-production environments, and you need to make sure that it does not have performance problems once deployed. Your deployment must be automated. What should you do?

- A. Use Cloud Load Balancing to slowly ramp up traffic between versions. Use Cloud Monitoring to look for performance issues.
- B. Deploy the application via a continuous delivery pipeline using canary deployments. Use Cloud Monitoring to look for performance issues, and ramp up traffic as the metrics support it.
- C. Deploy the application via a continuous delivery pipeline using blue/green deployments. Use Cloud Monitoring to look for performance issues, and launch fully when the metrics support it.
- D. Deploy the application using kubectl and set the spec.updateStrategy.type to RollingUpdate. Use Cloud Monitoring to look for performance issues, and run the kubectl rollback command if there are any issues.

**Correct Answer: A***Community vote distribution*

B (62%)	D (23%)	Other
---------	---------	-------

✉  **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: B**

B. Deploy the application via a continuous delivery pipeline using canary deployments. Use Cloud Monitoring to look for performance issues, ramp up traffic as the metrics support it.

upvoted 1 times

✉  **purushi** 8 months, 3 weeks ago

**Selected Answer: B**

I go with B. The key is deployment must be automated. With canary and CI/CD pipeline in place, we can adjust the traffic based on the input from Canary users.

upvoted 1 times

✉  **zanhsieh** 10 months, 3 weeks ago

**Selected Answer: B**

B. Automated deployment can be done with Cloud Deploy.

A: No. Not relevant and I can't find documents for Cloud Load Balancing supports canary deployment.

C: No. Blue / green is not possible because "not able to fully load-test the new version in pre-production environments" - either no budget or other causes.

D: No. Not automated and in-place upgrade will have performance hit.

upvoted 1 times

✉  **closer89** 1 year ago

**Selected Answer: B**

deployment should be automated

[https://cloud.google.com/deploy/docs/deployment-strategies/canary#types\\_of\\_canary](https://cloud.google.com/deploy/docs/deployment-strategies/canary#types_of_canary)

upvoted 2 times

 **Teraflow** 1 year ago

**Selected Answer: B**

B. Deploy the application via a continuous delivery pipeline using canary deployments. Use Cloud Monitoring to look for performance issues, ramp up traffic as the metrics support it.

Canary deployment strategy can be used to mitigate risk in the production deployment process. In this strategy, a small subset of traffic is routed to the new version of the application, while the rest of the traffic is sent to the current version. This allows for real-time monitoring of the new version's performance before fully rolling it out to all users. If there are any issues or performance problems, the traffic can be immediately rolled back to the previous version. Cloud Monitoring can be used to monitor performance metrics and make informed decisions about when to ramp up traffic to the new version.

upvoted 3 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: D**

i'd choose d.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: A**

Based on the link provided by the guys on the comments, after reviewing the links, I can see that

Option A "Use Cloud Load Balancing to slowly ramp up traffic between versions. Use Cloud Monitoring to look for performance issues" is a good approach, using Cloud Load Balancing, traffic is gradually shifted between the versions, and by using Cloud monitoring, you can detect any performance issues early on.

upvoted 1 times

 **closer89** 1 year ago

deployment should be automated

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Option C "Deploy the application via a continuous delivery pipeline using blue/green deployments. Use Cloud Monitoring to look for performance issues, and launch fully when the metrics support it" is also a good approach, as it allows you to test the new version of the application on a production-like environment and compare it against the previous version using real traffic, and once the metrics are good, switch all traffic to the new version.

Option D "Deploy the application using kubectl and set the spec.updateStrategy.type to RollingUpdate. Use Cloud Monitoring to look for performance issues, and run the kubectl rollback command if there are any issues" is also a good option, in this case as well you are incrementally rolling out the new version, and monitoring its performance, if any issues occur, you can roll back the update.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

Ultimately, the approach you choose will depend on the specifics of your application and infrastructure, but any of these options can work well if implemented correctly.

upvoted 1 times

 **TNT87** 1 year, 3 months ago

**Selected Answer: D**

Answer D

<https://kubernetes.io/docs/tutorials/kubernetes-basics/update/update-intro/>

<https://cloud.google.com/kubernetes-engine/docs/how-to/updating-apps#overview>

Kindly master the requirements of the question, and be very aware of the question's key words

upvoted 2 times

 **Kadhem** 5 months, 1 week ago

deployment shouldn't be automated ?

upvoted 1 times

 **TNT87** 1 year, 4 months ago

<https://kubernetes.io/docs/tutorials/kubernetes-basics/update/update-intro/>

<https://cloud.google.com/kubernetes-engine/docs/how-to/updating-apps#overview>

Answer D.

The rest need testing before...

upvoted 2 times

 **zelick** 1 year, 4 months ago

**Selected Answer: C**

C is the answer.

Question #151

*Topic 1*

Users are complaining that your Cloud Run-hosted website responds too slowly during traffic spikes. You want to provide a better user experience during traffic peaks. What should you do?

- A. Read application configuration and static data from the database on application startup.
- B. Package application configuration and static data into the application image during build time.
- C. Perform as much work as possible in the background after the response has been returned to the user.**
- D. Ensure that timeout exceptions and errors cause the Cloud Run instance to exit quickly so a replacement instance can be started.

**Correct Answer: C**

*Community vote distribution*

B (88%)

13%

 **purushi** 8 months, 3 weeks ago

**Selected Answer: B**

If images and config info available in the image (within the namespace of the hosting system) then latency is less. Can serve resources easily.  
upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: B**

B. Package application configuration and static data into the application image during build time.

By packaging application configuration and static data into the application image during build time, the application can quickly serve requests without having to make additional requests to a database, thus reducing response time. Additionally, you might consider caching static data in the application to reduce latency and provide faster responses to user requests, also you could move some of the computation that is not time critical to be done asynchronously.

upvoted 2 times

 **omermahgoub** 1 year, 3 months ago

Option A "Read application configuration and static data from the database on application startup" will put more load on database during traffic spike, this will slow down the application's response time.

Option C "Perform as much work as possible in the background after the response has been returned to the user" could be a good approach. It allows the user to receive a response quickly, but the background work could take a long time and cause a delay in processing and might not be acceptable for certain use-cases.

Option D "Ensure that timeout exceptions and errors cause the Cloud Run instance to exit quickly so a replacement instance can be started." This is good practice and can help ensure that when an instance is having problems, it can be quickly replaced with a new one, but this will not improve the user experience during traffic peaks, but instead it will minimize the impact of a failed instance on the service's availability.

upvoted 1 times

Question #152

Topic 1

You are a developer working on an internal application for payroll processing. You are building a component of the application that allows an employee to submit a timesheet, which then initiates several steps:

- An email is sent to the employee and manager, notifying them that the timesheet was submitted.
- A timesheet is sent to payroll processing for the vendor's API.
- A timesheet is sent to the data warehouse for headcount planning.

These steps are not dependent on each other and can be completed in any order. New steps are being considered and will be implemented by different development teams. Each development team will implement the error handling specific to their step. What should you do?

- A. Deploy a Cloud Function for each step that calls the corresponding downstream system to complete the required action.
- B. Create a Pub/Sub topic for each step. Create a subscription for each downstream development team to subscribe to their step's topic.
- C. Create a Pub/Sub topic for timesheet submissions. Create a subscription for each downstream development team to subscribe to the topic.
- D. Create a timesheet microservice deployed to Google Kubernetes Engine. The microservice calls each downstream step and waits for a successful response before calling the next step.

**Correct Answer: A**

*Community vote distribution*

C (100%)

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: C**

Pub/Sub is a messaging service that allows you to decouple microservices and other applications. It is a good choice for this use case because it is scalable, reliable, and easy to use.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: C**

This is a tricky question. The context is in developing team developing the application. So C is the best fit. After the development, when the application is running then each timesheet submit event can publish 3 events/messages so that 3 independent microservices for each operation can kick in parallel and perform the tasks.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: C**

C is correct

upvoted 1 times

 **TNT87** 1 year, 4 months ago

Answer C

upvoted 3 times

 **zellick** 1 year, 4 months ago

**Selected Answer: C**

C is the answer.

upvoted 2 times

 **sharath25** 1 year, 4 months ago

**Selected Answer: C**

option c

upvoted 1 times

 **kisswd** 1 year, 4 months ago

**Selected Answer: C**

One to many pattern, C is correct

upvoted 3 times

You are designing an application that uses a microservices architecture. You are planning to deploy the application in the cloud and on-premises. You want to make sure the application can scale up on demand and also use managed services as much as possible. What should you do?

- A. Deploy open source Istio in a multi-cluster deployment on multiple Google Kubernetes Engine (GKE) clusters managed by Anthos.
- B. Create a GKE cluster in each environment with Anthos, and use Cloud Run for Anthos to deploy your application to each cluster.
- C. Install a GKE cluster in each environment with Anthos, and use Cloud Build to create a Deployment for your application in each cluster.
- D. Create a GKE cluster in the cloud and install open-source Kubernetes on-premises. Use an external load balancer service to distribute traffic across the two environments.

**Correct Answer: B**

*Community vote distribution*

B (100%)

✉  **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: B**

Anthos with Cloud Run is the best option here.

upvoted 1 times

✉  **purushi** 8 months, 3 weeks ago

**Selected Answer: B**

Anthos supports GKE cluster creation in both On-premises and GCP cloud environments. Cloud run for Anthos supports autoscaling in both environments.

upvoted 1 times

✉  **Teraflow** 1 year ago

**Selected Answer: B**

B. Create a GKE cluster in each environment with Anthos, and use Cloud Run for Anthos to deploy your application to each cluster.

Using Anthos to manage Kubernetes clusters in both cloud and on-premises environments allows for consistency in deployment and management across both environments. Deploying the application using Cloud Run for Anthos allows for easy scaling on demand and use of managed services such as Cloud SQL and Memorystore. Additionally, Cloud Run for Anthos can be deployed to both GKE clusters and on-premises Kubernetes clusters, allowing for a consistent deployment experience across environments.

upvoted 2 times

✉  **TNT87** 1 year, 4 months ago

<https://cloud.google.com/anthos/run/docs/deploy-application>

Answer B

upvoted 2 times

✉  **zellick** 1 year, 4 months ago

**Selected Answer: B**

B is the answer.

<https://cloud.google.com/anthos/run>

Integrated with Anthos, Cloud Run for Anthos provides a flexible serverless development platform for hybrid and multicloud environments. Cloud Run for Anthos is Google's managed and fully supported Knative offering, an open source project that enables serverless workloads on Kubernetes.

upvoted 1 times



You want to migrate an on-premises container running in Knative to Google Cloud. You need to make sure that the migration doesn't affect your application's deployment strategy, and you want to use a fully managed service. Which Google Cloud service should you use to deploy your container?

- A. Cloud Run
- B. Compute Engine
- C. Google Kubernetes Engine
- D. App Engine flexible environment

**Correct Answer: A***Community vote distribution*

A (100%)

**✉️**  \_\_rajan\_\_ 7 months, 1 week ago**Selected Answer: A**

A is correct.

upvoted 1 times

**✉️**  purushi 8 months, 3 weeks ago**Selected Answer: A**

A is perfect since Cloud Run is built on Knative.

upvoted 1 times

**✉️**  TNT87 1 year, 4 months ago

Answer A

upvoted 1 times

**✉️**  zellick 1 year, 4 months ago**Selected Answer: A**

A is the answer.

<https://cloud.google.com/blog/products/serverless/knative-based-cloud-run-services-are-ga>

upvoted 2 times

**✉️**  sharath25 1 year, 4 months ago**Selected Answer: A**

A. container running in knative

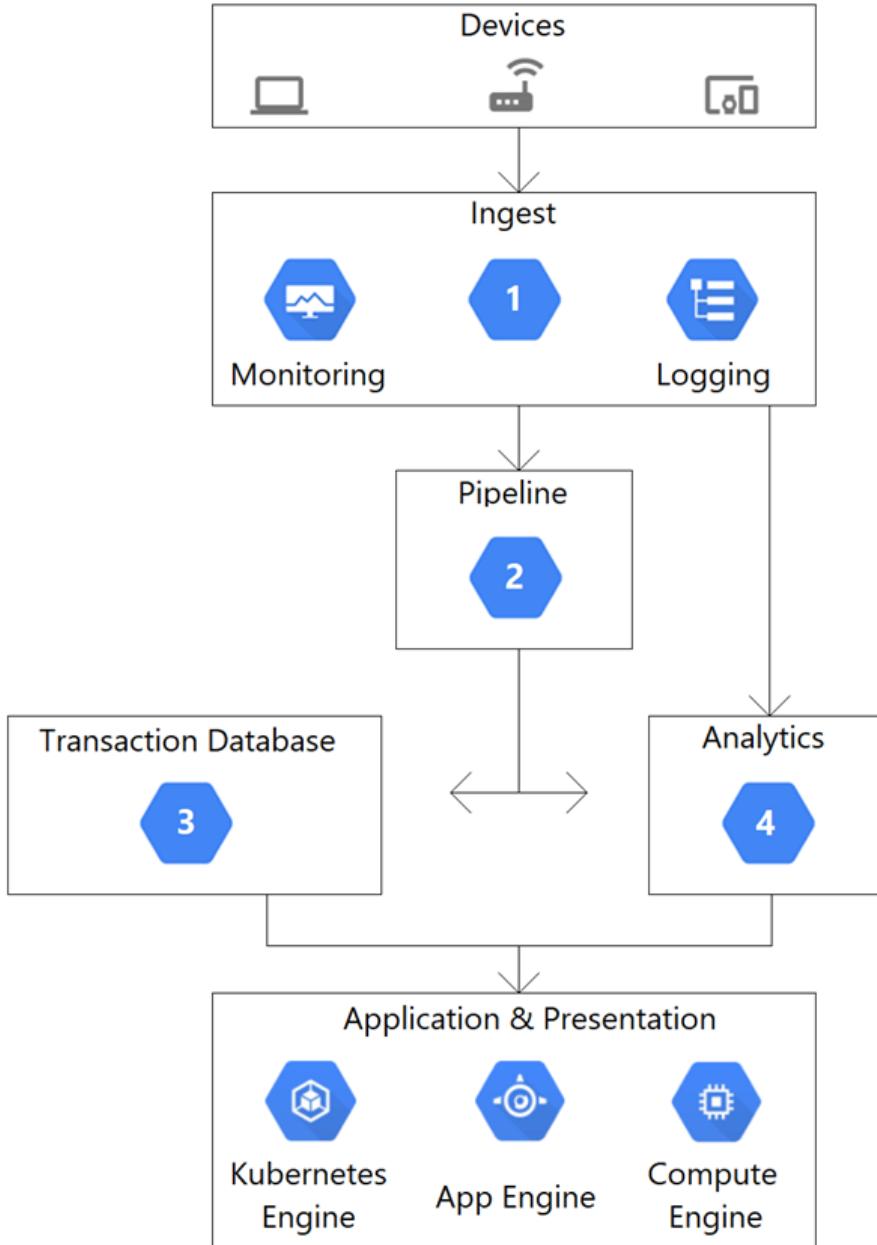
upvoted 1 times

**✉️**  aa654321 1 year, 4 months ago**Selected Answer: A**

Cloud run

upvoted 1 times

This architectural diagram depicts a system that streams data from thousands of devices. You want to ingest data into a pipeline, store the data, and analyze the data using SQL statements. Which Google Cloud services should you use for steps 1, 2, 3, and 4?



A. 1. App Engine

2. Pub/Sub

3. BigQuery

4. Firestore

B. 1. Dataflow

2. Pub/Sub

3. Firestore

4. BigQuery

C. 1. Pub/Sub

2. Dataflow

3. BigQuery

4. Firestore

D. 1. Pub/Sub

2. Dataflow

3. Firestore

4. BigQuery

**Correct Answer: D**

*Community vote distribution*

D (100%)

✉  **rajan\_** 7 months, 1 week ago

**Selected Answer: D**

D is correct.

upvoted 1 times

✉  **purushi** 8 months, 3 weeks ago

**Selected Answer: D**

Data ingest -> Pub sub

Pipeline -> Dataflow

Transaction -> Firestore

Analytics -> BigQuery

upvoted 2 times

✉  **TNT87** 1 year, 4 months ago

Answer D

upvoted 2 times

✉  **zellick** 1 year, 4 months ago

**Selected Answer: D**

D is the answer.

upvoted 1 times

✉  **sharath25** 1 year, 4 months ago

**Selected Answer: D**

option D

upvoted 1 times

✉  **gardislan18** 1 year, 4 months ago

**Selected Answer: D**

1. Pub/Sub - for ingest

2. Dataflow - dataflow pipeline

3. Firestore - transaction DB

4. BigQuery - analytics

upvoted 3 times

Question #156

*Topic 1*

Your company just experienced a Google Kubernetes Engine (GKE) API outage due to a zone failure. You want to deploy a highly available GKE architecture that minimizes service interruption to users in the event of a future zone failure. What should you do?

- A. Deploy Zonal clusters
- B. Deploy Regional clusters
- C. Deploy Multi-Zone clusters
- D. Deploy GKE on-premises clusters

**Correct Answer: A**

*Community vote distribution*

B (100%)

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: B**

B is correct.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: B**

Regional cluster with master plane to be in multiple zones is a correct option.

upvoted 1 times

 **TNT87** 1 year, 4 months ago

<https://cloud.google.com/blog/products/containers-kubernetes/best-practices-for-creating-a-highly-available-gke-cluster>

Answer B

[https://cloud.google.com/kubernetes-engine/docs/concepts/types-of-clusters#regional\\_clusters](https://cloud.google.com/kubernetes-engine/docs/concepts/types-of-clusters#regional_clusters)

upvoted 3 times

 **zellck** 1 year, 4 months ago

**Selected Answer: B**

B is the answer.

[https://cloud.google.com/kubernetes-engine/docs/concepts/types-of-clusters#regional\\_clusters](https://cloud.google.com/kubernetes-engine/docs/concepts/types-of-clusters#regional_clusters)

A regional cluster has multiple replicas of the control plane, running in multiple zones within a given region. Nodes in a regional cluster can run in multiple zones or a single zone depending on the configured node locations. By default, GKE replicates each node pool across three zones of the control plane's region. When you create a cluster or when you add a new node pool, you can change the default configuration by specifying the zone(s) in which the cluster's nodes run. All zones must be within the same region as the control plane.

upvoted 4 times

 **sharath25** 1 year, 4 months ago

**Selected Answer: B**

regional cluster

upvoted 1 times

 **melisargh** 1 year, 4 months ago

**Selected Answer: B**

Regional cluster replicates in at least 3 zones

upvoted 1 times

 **aa654321** 1 year, 4 months ago

**Selected Answer: B**

Regional cluster for protection against zonal outages

upvoted 1 times

Your team develops services that run on Google Cloud. You want to process messages sent to a Pub/Sub topic, and then store them. Each message must be processed exactly once to avoid duplication of data and any data conflicts. You need to use the cheapest and most simple solution. What should you do?

- A. Process the messages with a Dataproc job, and write the output to storage.
- B. Process the messages with a Dataflow streaming pipeline using Apache Beam's PubSubIO package, and write the output to storage.
- C. Process the messages with a Cloud Function, and write the results to a BigQuery location where you can run a job to deduplicate the data.
- D. Retrieve the messages with a Dataflow streaming pipeline, store them in Cloud Bigtable, and use another Dataflow streaming pipeline to deduplicate messages.

**Correct Answer: B***Community vote distribution*

B (100%)

**✉️**  \_\_rajan\_\_ 7 months, 1 week ago**Selected Answer: B**

B is correct.

upvoted 1 times

**✉️**  purushi 8 months, 3 weeks ago**Selected Answer: B**

Dataflow ensures that the data will be processed only once.

upvoted 1 times

**✉️**  wrakky 1 year, 3 months ago

Answer is B

<https://cloud.google.com/blog/products/data-analytics/handling-duplicate-data-in-streaming-pipeline-using-pubsub-dataflow>  
"...because Pub/Sub provides each message with a unique message\_id, Dataflow uses it to deduplicate messages by default if you use the b in Apache Beam PubSubIO"

upvoted 3 times

**✉️**  TNT87 1 year, 4 months ago**Selected Answer: B**<https://cloud.google.com/pubsub/docs/stream-messages-dataflow><https://cloud.google.com/community/tutorials/pubsub-spring-dedup-messages><https://cloud.google.com/blog/products/data-analytics/handling-duplicate-data-in-streaming-pipeline-using-pubsub-dataflow>

upvoted 1 times

**✉️**  zellick 1 year, 4 months ago**Selected Answer: B**

B is the answer.

<https://cloud.google.com/dataflow/docs/concepts/streaming-with-cloud-pubsub>

upvoted 1 times

Question #158

*Topic 1*

You are running a containerized application on Google Kubernetes Engine. Your container images are stored in Container Registry. Your team uses CI/CD practices. You need to prevent the deployment of containers with known critical vulnerabilities. What should you do?

- A. • Use Web Security Scanner to automatically crawl your application
  - Review your application logs for scan results, and provide an attestation that the container is free of known critical vulnerabilities
  - Use Binary Authorization to implement a policy that forces the attestation to be provided before the container is deployed
- B. • Use Web Security Scanner to automatically crawl your application
  - Review the scan results in the scan details page in the Cloud Console, and provide an attestation that the container is free of known critical vulnerabilities
  - Use Binary Authorization to implement a policy that forces the attestation to be provided before the container is deployed
- C. • Enable the Container Scanning API to perform vulnerability scanning
  - Review vulnerability reporting in Container Registry in the Cloud Console, and provide an attestation that the container is free of known critical vulnerabilities
  - Use Binary Authorization to implement a policy that forces the attestation to be provided before the container is deployed
- D. • Enable the Container Scanning API to perform vulnerability scanning
  - Programmatically review vulnerability reporting through the Container Scanning API, and provide an attestation that the container is free of known critical vulnerabilities
  - Use Binary Authorization to implement a policy that forces the attestation to be provided before the container is deployed

**Correct Answer: C**

*Community vote distribution*

D (67%)

C (33%)

 **xiaofeng\_0226** 5 months, 2 weeks ago

**Selected Answer: C**

i think c is correct  
upvoted 3 times

 **\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: D**

D is correct.  
upvoted 2 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: D**

Using container scanning API is a better choice.  
upvoted 1 times

 **telp** 1 year, 3 months ago

**Selected Answer: D**

Answer is D, use the default tools provided by google like container analysis.  
upvoted 1 times

 **TNT87** 1 year, 4 months ago

<https://cloud.google.com/container-analysis/docs/automated-scanning-howto#view-code>  
<https://cloud.google.com/binary-authorization/docs>

Answer D  
upvoted 2 times

 **zelliCK** 1 year, 4 months ago

**Selected Answer: D**

D is the answer.

<https://cloud.google.com/binary-authorization/docs/creating-attestations-kritis>  
upvoted 2 times

 **KlaasvR** 1 year, 4 months ago

I would go for D  
<https://cloud.google.com/container-analysis/docs/os-overview>  
upvoted 1 times

Question #159

Topic 1

You have an on-premises application that authenticates to the Cloud Storage API using a user-managed service account with a user-managed key. The application connects to Cloud Storage using Private Google Access over a Dedicated Interconnect link. You discover that requests from the application to access objects in the Cloud Storage bucket are failing with a 403 Permission Denied error code. What is the likely cause of this issue?

- A. The folder structure inside the bucket and object paths have changed.
- B. The permissions of the service account's predefined role have changed.

- C. The service account key has been rotated but not updated on the application server.
- D. The Interconnect link from the on-premises data center to Google Cloud is experiencing a temporary outage.

**Correct Answer: C**

*Community vote distribution*

B (56%)

C (44%)

 **mrvergara**  1 year, 2 months ago

**Selected Answer: B**

The correct option is B. The 403 Permission Denied error code indicates that the service account is authenticated, but it doesn't have sufficient permissions to access the Cloud Storage bucket. If the error code were 401 Unauthorized, it would suggest that the authentication failed, which could be caused by a rotated key, as in option C. However, in this case, the error code is 403, which indicates a problem with the permissions for the service account, making option B the most likely cause.

upvoted 6 times

 **prasadjblin**  6 months ago

**Selected Answer: B**

B is the correct answer. 403 denotes user is authenticated but not authorized.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: C**

C is correct

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: C**

The client id/service account key has been updated for the storage bucket but that was not being notified to the client applications or application server that calls cloud storage bucket.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: C**

A user-managed service account authenticates to the Cloud Storage API using a key, which is a unique identifier that proves the identity of the service account. If the key is rotated, meaning it is replaced with a new one, the application will no longer be able to authenticate using the old key, resulting in a 403 Permission Denied error. To resolve this issue, the application server must be updated with the new key.

upvoted 2 times

 **telp** 1 year, 3 months ago

**Selected Answer: B**

Answer B with status code 403 => Forbidden so the first authentication is working just the service has not enough permission to access the document.

upvoted 1 times

 **telp** 1 year, 3 months ago

**Selected Answer: C**

The answer is between B or C.

I will choose C because the question has a context with account service by file with a key. With this setup, the cause of issue 403 will be key is not valid anymore after a rotation. For another context with only account service without a key generated, the B is the first check but with a key you need to check if the key is valid before searching others causes.

upvoted 1 times

 **TNT87** 1 year, 3 months ago

The HTTP 403 Forbidden response status code indicates that the server understands the request but refuses to authorize it. This status is similar to 401 , but for the 403 Forbidden status code, re-authenticating makes no difference. The access is tied to the application logic, so as insufficient rights to a resource.

The reason for denied access is the reason we get 403. as the question says, do not copy what others are saying , do a research and apply your knowledge to this if you have any practical knowledge. the answer is B

upvoted 1 times

 **telp** 1 year, 3 months ago

Yes agree with your comments, Answer is B

upvoted 2 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: C**

C. The service account key has been rotated but not updated on the application server.

When a user-managed service account key is rotated in Google Cloud, the new key must also be updated on the application server that authenticates to the Cloud Storage API using that key. Failure to update the key on the application server will result in requests to the API failing with a 403 Permission Denied error code.

Option B "The permissions of the service account's predefined role have changed" would also result in 403 error, but it would be a role issue, a key issue.

upvoted 1 times

 **TNT87** 1 year, 3 months ago

I dnt know if you have studied cloud security, GCP cloud security and are you actually doing these practically??

upvoted 1 times

 **TNT87** 1 year, 3 months ago

But the key has a role, so i literally do not understand your last statement, actually provide a link to your answer because i dnt think The documentation can lieoi provided links because i needed to support what i know by what is written.

upvoted 1 times

 **TNT87** 1 year, 3 months ago

The question explicitly says "'What is the likely cause of this issue?'" and i answered that by providing links, you are arguing but you dnt provide any links, i do not copy answers from someone , i do a research hence even if i know the answer off head i try to provide links for the sake of others like you, i dnt make baseless arguments

upvoted 1 times

✉  **TNT87** 1 year, 3 months ago

**Selected Answer: B**

Answer B

<https://cloud.google.com/storage/docs/troubleshooting#access-permission>

<https://cloud.google.com/appengine/docs/standard/python/googlecloudstorageclient/errors>

<https://cloud.google.com/storage/docs/xml-api/reference-status#403%20%94forbidden>

upvoted 1 times

✉  **omermahgoub** 1 year, 3 months ago

The links you've provided are helpful resources for troubleshooting 403 "Permission Denied" errors when working with Cloud Storage.

You're correct, the 403 "Permission Denied" error can be caused by various reasons, such as an issue with the folder structure inside the bucket or an issue with the predefined role permissions, but based on the context and the error message it seems that the most likely cause is the service account key being rotated and not updated on the application server as I mentioned earlier.

Additionally, the links you provided provide more information about the possible causes for 403 error, such as the permissions that are associated with the object and the bucket, user authentication and role-based access control. Also, it's important to check the Cloud Storage access logs to determine the cause of the error and take appropriate action.

upvoted 1 times

✉  **TNT87** 1 year, 3 months ago

so what's your argument because i provided the links to prove my point , where are your links? i chose the answer that is supported, hence i provided links. im not seeing anywhere where B is supported because according to the documentation its not B and according to my practical knowledge in GCP it can't be B.

upvoted 1 times

✉  **TNT87** 1 year, 3 months ago

it can't be C i mean.... B is the answer that's what the links are saying

upvoted 1 times

✉  **TNT87** 1 year, 4 months ago

Answer B

<https://cloud.google.com/storage/docs/troubleshooting#access-permission>

<https://cloud.google.com/appengine/docs/standard/python/googlecloudstorageclient/errors>

<https://cloud.google.com/storage/docs/xml-api/reference-status#403%20%94forbidden>

upvoted 2 times

✉  **zellick** 1 year, 4 months ago

**Selected Answer: C**

C is the answer.

upvoted 1 times

Question #160

Topic 1

You are using the Cloud Client Library to upload an image in your application to Cloud Storage. Users of the application report that occasionally the upload does not complete and the client library reports an HTTP 504 Gateway Timeout error. You want to make the application more resilient to errors. What changes to the application should you make?

- A. Write an exponential backoff process around the client library call.
- B. Write a one-second wait time backoff process around the client library call.
- C. Design a retry button in the application and ask users to click if the error occurs.
- D. Create a queue for the object and inform the users that the application will try again in 10 minutes.

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: A**

A is correct.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: A**

Exponential back off strategy is a better choice for retry approach. This is for resiliency.

upvoted 1 times

 **telp** 1 year, 3 months ago

**Selected Answer: A**

When issuing link to charges on server like 504 uses the exponential-backoff

upvoted 1 times

 **TNT87** 1 year, 3 months ago

**Selected Answer: A**

<https://cloud.google.com/storage/docs/retry-strategy#exponential-backoff>

Answer A

upvoted 1 times

 **TNT87** 1 year, 4 months ago

[https://cloud.google.com/storage/docs/json\\_api/v1/status-codes#504\\_Gateway\\_Timeout](https://cloud.google.com/storage/docs/json_api/v1/status-codes#504_Gateway_Timeout)

Answer A

upvoted 1 times

 **zellck** 1 year, 4 months ago

**Selected Answer: A**

A is the answer.

upvoted 1 times

sync changes when they are back online. A backend service will enrich the data in the database using a service account. The application is expected to be very popular and needs to scale seamlessly and securely. Which database and IAM role should you use?

- A. Use Cloud SQL, and assign the roles/cloudsql.editor role to the service account.
- B. Use Bigtable, and assign the roles/bigtable.viewer role to the service account.
- C. Use Firestore in Native mode and assign the roles/datastore.user role to the service account.
- D. Use Firestore in Datastore mode and assign the roles/datastore.viewer role to the service account.

**Correct Answer: A**

*Community vote distribution*

C (100%)

✉  \_\_rajan\_\_ 7 months, 1 week ago

**Selected Answer: C**

C is correct.

upvoted 1 times

✉  purush 8 months, 3 weeks ago

**Selected Answer: C**

IAM role should be roles/datastore.user role and not a viewer role as of option D. Firestore is suitable for storing semi structured and hierarchical mobile data.

upvoted 2 times

✉  Oleksii\_ki 9 months, 3 weeks ago

**Selected Answer: C**

C. Use Firestore in Native mode and assign the roles/datastore.user role to the service account.

roles/datastore.user role - have permissions to Read/write access to data in a Datastore mode database. Intended for application developers service accounts.

<https://cloud.google.com/datastore/docs/access/iam>

upvoted 1 times

✉  TNT87 1 year, 4 months ago

Answer C

<https://cloud.google.com/architecture/building-scalable-apps-with-cloud-firebase>

upvoted 3 times

✉  zellick 1 year, 4 months ago

**Selected Answer: C**

C is the answer.

<https://firebase.google.com/docs/firestore/manage-data/enable-offline>

Cloud Firestore supports offline data persistence. This feature caches a copy of the Cloud Firestore data that your app is actively using, so your app can access the data when the device is offline. You can write, read, listen to, and query the cached data. When the device comes back online, Cloud Firestore synchronizes any local changes made by your app to the Cloud Firestore backend.

upvoted 2 times

✉  sharath25 1 year, 4 months ago

**Selected Answer: C**

option C

upvoted 1 times

✉  kisswd 1 year, 4 months ago

**Selected Answer: C**

<https://firebase.google.com/docs/firestore/manage-data/enable-offline>

upvoted 1 times

Question #162

Topic 1

Your application is deployed on hundreds of Compute Engine instances in a managed instance group (MIG) in multiple zones. You need to deploy a new instance template to fix a critical vulnerability immediately but must avoid impact to your service. What setting should be made to the MIG after updating the instance template?

- A. Set the Max Surge to 100%.
- B. Set the Update mode to Opportunistic.
- C. Set the Maximum Unavailable to 100%.
- D. Set the Minimum Wait time to 0 seconds.

**Correct Answer:** C

*Community vote distribution*

D (72%)

B (28%)

 **micoams** Highly Voted 1 year, 4 months ago

**Selected Answer: D**

You can eliminate:

- B. Because the MIG needs to be updated immediately, which is what Opportunistic does
- C. Because max unavailable at 100% will cause downtime

So that leaves A, and D.

If you choose A. The MIG will spin up hundreds of new machines, to replace the existing one, and shutdown the old ones. This is the fastest method, but could be costly, or you could run into quota issues.

If you choose D, the MIG will spin up 3 VMs at a time (maxSurge default to 3), and then it will bring up one at a time, as soon as more surge slots are available, so it won't be really that fast.

I think D is the most sensible in this case.

upvoted 9 times

✉  **wanrltw** Most Recent 4 months, 3 weeks ago

**Selected Answer: D**

I vote D.

There are 2 requirements: to deploy the new instance template immediately and to avoid impact. Option D matches the urgency of the issue while it also allows to control (minimize) the level of disruption to the service.

[https://cloud.google.com/compute/docs/instance-groups/updating-migs#choosing\\_between\\_automated\\_and\\_selective\\_updates](https://cloud.google.com/compute/docs/instance-groups/updating-migs#choosing_between_automated_and_selective_updates)

upvoted 2 times

✉  **\_rajan\_** 7 months, 1 week ago

**Selected Answer: B**

When you set the update mode to Opportunistic, the group will continue to serve requests from existing instances while the new instances are being created and started. Once the new instances are ready, the group will start routing requests to them. The group will continue to serve requests from both the old and new instances until all of the old instances have been terminated.

upvoted 2 times

✉  **purushi** 8 months, 3 weeks ago

**Selected Answer: D**

The key here is fixing the vulnerability immediately which is not possible with Opportunistic mode.

upvoted 2 times

✉  **NewComer200** 12 months ago

**Selected Answer: D**

I think updating "deployed on hundreds of Compute Engine instances" is impossible with Opportunistic mode.

So I agree with D.

upvoted 1 times

✉  **sbonessi** 11 months, 2 weeks ago

And also said changes immediately, so opportunistic mode is not suitable as well.

Agree with D

upvoted 1 times

✉  **closer89** 1 year ago

**Selected Answer: D**

i go for D

you've updated template and want apply changes immediately

upvoted 1 times

✉  **Pime13** 1 year, 1 month ago

**Selected Answer: D**

[https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups#minimum\\_wait\\_time](https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups#minimum_wait_time)

Use the minReadySec option to specify the amount of time to wait before considering a new or restarted instance as updated. Use this option to control the rate at which the automated update is deployed. The timer starts when both of the following conditions are satisfied:

The instance's status is RUNNING.

If health checking is enabled, when the health check returns HEALTHY.

However: minReadySec is only available in the beta Compute Engine API and might be deprecated in a future release.

upvoted 1 times

 **mrvergara** 1 year, 2 months ago

**Selected Answer: D**

Setting the "Minimum Wait time" to 0 seconds means that there is no delay in launching the new instances after the instance template is updated, allowing you to deploy the fix for the critical vulnerability immediately. On the other hand, setting the "Update mode to Opportunistic" would mean that the new instances are created at an opportune time and may result in a delay in deploying the fix. In this scenario, where a critical vulnerability needs to be fixed immediately, it's important to deploy the fix as soon as possible, making the "Minimum Wait time to 0 seconds" the better approach.

upvoted 2 times

 **TNT87** 1 year, 4 months ago

**Selected Answer: B**

[https://cloud.google.com/compute/docs/instance-groups/updating-migs#opportunistic\\_updates](https://cloud.google.com/compute/docs/instance-groups/updating-migs#opportunistic_updates)

Answer B

upvoted 1 times

 **zellick** 1 year, 4 months ago

**Selected Answer: B**

B is the answer.

<https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups#type>

Alternatively, if an automated update is potentially too disruptive, you can choose to perform an opportunistic update. The MIG applies an opportunistic update only when you manually initiate the update on selected instances or when new instances are created. New instances can be created when you or another service, such as an autoscaler, resizes the MIG. Compute Engine does not actively initiate requests to apply opportunistic updates on existing instances.

upvoted 4 times

 **sahith24** 1 year, 4 months ago

Answer?

upvoted 1 times

Question #163

Topic 1

You made a typo in a low-level Linux configuration file that prevents your Compute Engine instance from booting to a normal run level. You just created the Compute Engine instance today and have done no other maintenance on it, other than tweaking files. How should you correct this error?

- A. Download the file using scp, change the file, and then upload the modified version
- B. Configure and log in to the Compute Engine instance through SSH, and change the file
- C. Configure and log in to the Compute Engine instance through the serial port, and change the file
- D. Configure and log in to the Compute Engine instance using a remote desktop client, and change the file

**Correct Answer: B**

*Community vote distribution*

C (86%)

14%

 **purushi** 8 months, 3 weeks ago

**Selected Answer: C**

If booting issue with Compute engine instance, then serial port access is one of the solution. SSH, RDP and SCP are not possible.  
upvoted 4 times

 **NewComer200** 12 months ago

**Selected Answer: C**

According to the explanation "prevents your Compute Engine instance from booting to a normal run level".  
So I think sshd deamon has not launched yet and you can't use ssh.  
I can't think of a correct answer to anything other than C.

upvoted 1 times

 **Teraflow** 1 year ago

**Selected Answer: B**

The correct answer is B: Configure and log in to the Compute Engine instance through SSH, and change the file.

This is the recommended method to make changes to a Linux configuration file on a Compute Engine instance. SSH allows secure remote access to the instance's command line interface, and it is designed to enable you to make changes to the instance's configuration files.

Option A, downloading and uploading the modified version of the file, is not the recommended method as it requires more steps and can introduce errors.

Option C, using the serial port, may be used in some cases, but it is not the recommended method as it requires more steps and can be more complex.

Option D, using a remote desktop client, is not applicable as Linux instances on Compute Engine do not come with a graphical user interface (GUI) by default.

upvoted 1 times

 **NewComer200** 12 months ago

Computer access through serial ports has been the method used by server administrators for a long time, so it is normal for professionals be able to do this.

If we consider that the computer is not running, there is no correct answer other than C.

upvoted 1 times

 **TNT87** 1 year, 4 months ago

<https://cloud.google.com/compute/docs/troubleshooting/troubleshooting-using-serial-console>

Answer C

upvoted 2 times

 **zellck** 1 year, 4 months ago

**Selected Answer: C**

C is the answer.

<https://cloud.google.com/compute/docs/troubleshooting/troubleshooting-using-serial-console>

upvoted 1 times

You are developing an application that needs to store files belonging to users in Cloud Storage. You want each user to have their own subdirectory in Cloud Storage. When a new user is created, the corresponding empty subdirectory should also be created. What should you do?

- A. Create an object with the name of the subdirectory ending with a trailing slash ('/') that is zero bytes in length.
- B. Create an object with the name of the subdirectory, and then immediately delete the object within that subdirectory.
- C. Create an object with the name of the subdirectory that is zero bytes in length and has WRITER access control list permission.
- D. Create an object with the name of the subdirectory that is zero bytes in length. Set the Content-Type metadata to CLOUDSTORAGE\_FOLDER.

**Correct Answer: A**

*Community vote distribution*

A (82%)

C (18%)

 zelick  1 year, 4 months ago

**Selected Answer: A**

A is the answer.

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

If you create an empty folder using the Google Cloud console, Cloud Storage creates a zero-byte object as a placeholder. For example, if you create a folder called folder in a bucket called my-bucket, a zero- byte object called gs://my-bucket/folder/ is created. This placeholder is discoverable by other tools when listing the objects in the bucket, for example when using the gsutil ls command.

upvoted 7 times

 \_\_rajan\_\_  7 months, 1 week ago

**Selected Answer: A**

When you create an object with the name of the subdirectory ending with a trailing slash, Cloud Storage will treat the object as a subdirectory. This means that you can then store other objects in the subdirectory.

upvoted 2 times

 purushi 8 months, 3 weeks ago

**Selected Answer: C**

I go with C. WRITER permission and folder with zero bytes size is correct.

upvoted 1 times

 NewComer200 12 months ago

**Selected Answer: C**

<https://cloud.google.com/storage/docs/folders#overview>

According to the explanation upper URL, " Cloud Storage operates with a flat namespace, which means that folders don't actually exist within Cloud Storage. ".

That's right. You can't create the state "foo/".

This is an actual experience using Cloud Storage.

Therefore, I think the correct answer is C.

upvoted 1 times

Question #165

Topic 1

Your company's corporate policy states that there must be a copyright comment at the very beginning of all source files. You want to write a custom step in Cloud Build that is triggered by each source commit. You need the trigger to validate that the source contains a copyright and add one for subsequent steps if not there. What should you do?

- A. Build a new Docker container that examines the files in /workspace and then checks and adds a copyright for each source file. Changed files are explicitly committed back to the source repository.
- B. Build a new Docker container that examines the files in /workspace and then checks and adds a copyright for each source file. Changed files do not need to be committed back to the source repository.
- C. Build a new Docker container that examines the files in a Cloud Storage bucket and then checks and adds a copyright for each source file. Changed files are written back to the Cloud Storage bucket.
- D. Build a new Docker container that examines the files in a Cloud Storage bucket and then checks and adds a copyright for each source file. Changed files are explicitly committed back to the source repository.

**Correct Answer: C**

*Community vote distribution*

A (88%)

13%

 **purushi** 8 months, 3 weeks ago

**Selected Answer: A**

If a company policy states that every source code should have the copyright comment at the beginning of each file then for every build, we need to scan for each source code file and generate the copyright comments if not there, commit the updated files back to the repository. This is like a prebuild check.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: A**

A. Build a new Docker container that examines the files in /workspace and then checks and adds a copyright for each source file. Changed files are explicitly committed back to the source repository.

This option would allow you to create a custom step in Cloud Build that is triggered by each source commit, which would examine the source files in the /workspace directory, check for the presence of a copyright comment, and add one if not present. By committing the changed files back to the source repository, you ensure that the updated files with the added copyright comment are properly tracked and stored in the source control system.

upvoted 2 times

 **telp** 1 year, 3 months ago

**Selected Answer: A**

the code changes must be put back in the workplace folder or the sub other sub-step won't have the changes.

upvoted 1 times

 **TNT87** 1 year, 4 months ago

<https://cloud.google.com/build/docs/automating-builds/create-manage-triggers>

Answer A

upvoted 1 times

 **zelliCK** 1 year, 4 months ago

**Selected Answer: A**

A is the answer.

[https://cloud.google.com/build/docs/configuring-builds/pass-data-between-steps#passing\\_data\\_using\\_workspaces](https://cloud.google.com/build/docs/configuring-builds/pass-data-between-steps#passing_data_using_workspaces)

To pass data between build steps, store the assets produced by the build step in /workspace and these assets will be available to any subsequent build steps.

upvoted 3 times

 **zelliCK** 1 year, 4 months ago

**Selected Answer: B**

B is the answer.

[https://cloud.google.com/build/docs/configuring-builds/pass-data-between-steps#passing\\_data\\_using\\_workspaces](https://cloud.google.com/build/docs/configuring-builds/pass-data-between-steps#passing_data_using_workspaces)

To pass data between build steps, store the assets produced by the build step in /workspace and these assets will be available to any subsequent build steps.

upvoted 1 times

 **zelliCK** 1 year, 4 months ago

Sorry answer should be A.

upvoted 2 times

One of your deployed applications in Google Kubernetes Engine (GKE) is having intermittent performance issues. Your team uses a third-party logging solution. You want to install this solution on each node in your GKE cluster so you can view the logs. What should you do?

- A. Deploy the third-party solution as a DaemonSet
- B. Modify your container image to include the monitoring software
- C. Use SSH to connect to the GKE node, and install the software manually
- D. Deploy the third-party solution using Terraform and deploy the logging Pod as a Kubernetes Deployment

**Correct Answer: A***Community vote distribution*

A (100%)

  **rajan\_** 7 months, 1 week ago**Selected Answer: A**

DaemonSet is correct choice here.

upvoted 1 times

  **purushi** 8 months, 3 weeks ago**Selected Answer: A**

A is best suitable than D here. D is complicated with Terraform and so on. Another solution would be to deploy the third party logging solution a sidecar container with the main application.

upvoted 1 times

  **telp** 1 year, 3 months ago**Selected Answer: A**

A is the answer, it's the use of daemonSet to ensures that a specific Pod is always running on all or some subset of the nodes

upvoted 1 times

  **TNT87** 1 year, 4 months ago<https://kubernetes.io/docs/concepts/workloads/controllers/daemonset/>

Answer A

upvoted 1 times

  **zelliCK** 1 year, 4 months ago**Selected Answer: A**

A is the answer.

[https://cloud.google.com/kubernetes-engine/docs/concepts/daemonset#usage\\_patterns](https://cloud.google.com/kubernetes-engine/docs/concepts/daemonset#usage_patterns)

DaemonSets are useful for deploying ongoing background tasks that you need to run on all or certain nodes, and which do not require user intervention. Examples of such tasks include storage daemons like ceph, log collection daemons like fluent-bit, and node monitoring daemon like collectd.

upvoted 2 times

## Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

#### To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

#### Company Overview -

HipLocal is a community application designed to facilitate communication between people in close proximity. It is used for event planning and organizing sporting events, and for businesses to connect with their local communities. HipLocal launched recently in a few neighborhoods in Dallas and is rapidly growing into a global phenomenon. Its unique style of hyper-local community communication and business outreach is in demand around the world.

#### Executive Statement -

We are the number one local community app; it's time to take our local community services global. Our venture capital investors want to see rapid growth and the same great experience for new local and virtual communities that come online, whether their members are 10 or 10000 miles away from each other.

#### Solution Concept -

HipLocal wants to expand their existing service, with updated functionality, in new regions to better serve their global customers. They want to hire and train a new team to support these regions in their time zones. They will need to ensure that the application scales smoothly and provides clear uptime data, and that they analyze and respond to any issues that occur.

#### Existing Technical Environment -

HipLocal's environment is a mix of on-premises hardware and infrastructure running in Google Cloud Platform. The HipLocal team understands their application well, but has limited experience in global scale applications. Their existing technical environment is as follows:

- Existing APIs run on Compute Engine virtual machine instances hosted in GCP.
- State is stored in a single instance MySQL database in GCP.
- Release cycles include development freezes to allow for QA testing.
- The application has no logging.
- Applications are manually deployed by infrastructure engineers during periods of slow traffic on weekday evenings.
- There are basic indicators of uptime; alerts are frequently fired when the APIs are unresponsive.

#### Business Requirements -

HipLocal's investors want to expand their footprint and support the increase in demand they are seeing. Their requirements are:

- Expand availability of the application to new regions.
- Support 10x as many concurrent users.
- Ensure a consistent experience for users when they travel to different regions.

- Obtain user activity metrics to better understand how to monetize their product.
  - Ensure compliance with regulations in the new regions (for example, GDPR).
  - Reduce infrastructure management time and cost.
  - Adopt the Google-recommended practices for cloud computing.
- Develop standardized workflows and processes around application lifecycle management.
- Define service level indicators (SLIs) and service level objectives (SLOs).

#### Technical Requirements -

- Provide secure communications between the on-premises data center and cloud-hosted applications and infrastructure.
- The application must provide usage metrics and monitoring.
- APIs require authentication and authorization.
- Implement faster and more accurate validation of new features.
- Logging and performance metrics must provide actionable information to be able to provide debugging information and alerts.
- Must scale to meet user demand.

For this question, refer to the HipLocal case study.

How should HipLocal redesign their architecture to ensure that the application scales to support a large increase in users?

- A. Use Google Kubernetes Engine (GKE) to run the application as a microservice. Run the MySQL database on a dedicated GKE node.
- B. Use multiple Compute Engine instances to run MySQL to store state information. Use a Google Cloud-managed load balancer to distribute the load between instances. Use managed instance groups for scaling.
- C. Use Memorystore to store session information and CloudSQL to store state information. Use a Google Cloud-managed load balancer to distribute the load between instances. Use managed instance groups for scaling.
- D. Use a Cloud Storage bucket to serve the application as a static website, and use another Cloud Storage bucket to store user state information.

**Correct Answer: D**

*Community vote distribution*

C (100%)

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: C**

C is correct.

upvoted 2 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: C**

HipLocal Standard Cloud Computing Scenario:

MySQL to Cloud SQL definitely needed.

Managed Instance group and load balancer are required.

Memorystore (Redis) to store user's session data is required.

upvoted 3 times

 **telp** 1 year, 3 months ago

**Selected Answer: C**

C is the answer.

upvoted 1 times

 **zelliCK** 1 year, 4 months ago

**Selected Answer: C**

C is the answer.

upvoted 1 times

 **micoams** 1 year, 4 months ago

**Selected Answer: C**

A,B and D can be eliminated

A. Because running MySQL inside GKE is not a GCP Best practice (there is CloudSQL)

B. Running MySQL manually on CE instances is not best practice (there is CloudSQL)

D. State information does not belong in cloud storage

So that leaves C as the only valid option.

upvoted 3 times

Question #168

Topic 1

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

#### **Company Overview -**

HipLocal is a community application designed to facilitate communication between people in close proximity. It is used for event planning and organizing sporting events, and for businesses to connect with their local communities. HipLocal launched recently in a few neighborhoods in Dallas and is rapidly growing into a global phenomenon. Its unique style of hyper-local community communication and business outreach is in demand around the world.

#### **Executive Statement -**

We are the number one local community app; it's time to take our local community services global. Our venture capital investors want to see rapid growth and the same great experience for new local and virtual communities that come online, whether their members are 10 or 10000 miles away from each other.

#### **Solution Concept -**

HipLocal wants to expand their existing service, with updated functionality, in new regions to better serve their global customers. They want to hire and train a new team to support these regions in their time zones. They will need to ensure that the application scales smoothly and provides clear uptime data, and that they analyze and respond to any issues that occur.

#### **Existing Technical Environment -**

HipLocal's environment is a mix of on-premises hardware and infrastructure running in Google Cloud Platform. The HipLocal team understands their application well, but has limited experience in global scale applications. Their existing technical environment is as follows:

- Existing APIs run on Compute Engine virtual machine instances hosted in GCP.
- State is stored in a single instance MySQL database in GCP.
- Release cycles include development freezes to allow for QA testing.
- The application has no logging.
- Applications are manually deployed by infrastructure engineers during periods of slow traffic on weekday evenings.
- There are basic indicators of uptime; alerts are frequently fired when the APIs are unresponsive.

#### **Business Requirements -**

HipLocal's investors want to expand their footprint and support the increase in demand they are seeing. Their requirements are:

- Expand availability of the application to new regions.
  - Support 10x as many concurrent users.
  - Ensure a consistent experience for users when they travel to different regions.
  - Obtain user activity metrics to better understand how to monetize their product.
  - Ensure compliance with regulations in the new regions (for example, GDPR).
  - Reduce infrastructure management time and cost.
  - Adopt the Google-recommended practices for cloud computing.
- Develop standardized workflows and processes around application lifecycle management.
- Define service level indicators (SLIs) and service level objectives (SLOs).

#### **Technical Requirements -**

- Provide secure communications between the on-premises data center and cloud-hosted applications and infrastructure.
- The application must provide usage metrics and monitoring.
- APIs require authentication and authorization.
- Implement faster and more accurate validation of new features.
- Logging and performance metrics must provide actionable information to be able to provide debugging information and alerts.

- Must scale to meet user demand.

For this question, refer to the HipLocal case study.

How should HipLocal increase their API development speed while continuing to provide the QA team with a stable testing environment that meets feature requirements?

- Include unit tests in their code, and prevent deployments to QA until all tests have a passing status.
- Include performance tests in their code, and prevent deployments to QA until all tests have a passing status.
- Create health checks for the QA environment, and redeploy the APIs at a later time if the environment is unhealthy.
- Redeploy the APIs to App Engine using Traffic Splitting. Do not move QA traffic to the new versions if errors are found.

**Correct Answer: B**

*Community vote distribution*

A (100%)

 rajan 7 months, 1 week ago

**Selected Answer: A**

A is correct.

upvoted 1 times

 purushi 8 months, 3 weeks ago

**Selected Answer: A**

The answer must be A. Dev team's responsibility is to make sure all unit tests are passed before saying code is ready for testing.  
Note: GCP PCD questions are really ridiculous. There are many ways to ask this question in a very simple way. I guess the questions are being prepared by a non-technical staff of GCP.

upvoted 2 times

 telp 1 year, 3 months ago

**Selected Answer: A**

Answer A

upvoted 1 times

 TNT87 1 year, 4 months ago

Answer A

upvoted 1 times

 zellck 1 year, 4 months ago

**Selected Answer: A**

A is the answer.

upvoted 1 times

 swifty512 1 year, 4 months ago

**Selected Answer: A**

A stable environment is one that works. Performance testing does not mean it works fine, unit testing will enable this.

upvoted 2 times

Question #169

Topic 1

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions

included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

#### To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

#### Company Overview -

HipLocal is a community application designed to facilitate communication between people in close proximity. It is used for event planning and organizing sporting events, and for businesses to connect with their local communities. HipLocal launched recently in a few neighborhoods in Dallas and is rapidly growing into a global phenomenon. Its unique style of hyper-local community communication and business outreach is in demand around the world.

#### Executive Statement -

We are the number one local community app; it's time to take our local community services global. Our venture capital investors want to see rapid growth and the same great experience for new local and virtual communities that come online, whether their members are 10 or 10000 miles away from each other.

#### Solution Concept -

HipLocal wants to expand their existing service, with updated functionality, in new regions to better serve their global customers. They want to hire and train a new team to support these regions in their time zones. They will need to ensure that the application scales smoothly and provides clear uptime data, and that they analyze and respond to any issues that occur.

#### Existing Technical Environment -

HipLocal's environment is a mix of on-premises hardware and infrastructure running in Google Cloud Platform. The HipLocal team understands their application well, but has limited experience in global scale applications. Their existing technical environment is as follows:

- Existing APIs run on Compute Engine virtual machine instances hosted in GCP.
- State is stored in a single instance MySQL database in GCP.
- Release cycles include development freezes to allow for QA testing.
- The application has no logging.
- Applications are manually deployed by infrastructure engineers during periods of slow traffic on weekday evenings.
- There are basic indicators of uptime; alerts are frequently fired when the APIs are unresponsive.

#### Business Requirements -

HipLocal's investors want to expand their footprint and support the increase in demand they are seeing. Their requirements are:

- Expand availability of the application to new regions.
- Support 10x as many concurrent users.

- Ensure a consistent experience for users when they travel to different regions.
  - Obtain user activity metrics to better understand how to monetize their product.
  - Ensure compliance with regulations in the new regions (for example, GDPR).
  - Reduce infrastructure management time and cost.
  - Adopt the Google-recommended practices for cloud computing.
- Develop standardized workflows and processes around application lifecycle management.
- Define service level indicators (SLIs) and service level objectives (SLOs).

#### Technical Requirements -

- Provide secure communications between the on-premises data center and cloud-hosted applications and infrastructure.
- The application must provide usage metrics and monitoring.
- APIs require authentication and authorization.
- Implement faster and more accurate validation of new features.
- Logging and performance metrics must provide actionable information to be able to provide debugging information and alerts.
- Must scale to meet user demand.

For this question, refer to the HipLocal case study.

HipLocal's application uses Cloud Client Libraries to interact with Google Cloud. HipLocal needs to configure authentication and authorization in the Cloud Client Libraries to implement least privileged access for the application. What should they do?

- A. Create an API key. Use the API key to interact with Google Cloud.
- B. Use the default compute service account to interact with Google Cloud.
- C. Create a service account for the application. Export and deploy the private key for the application. Use the service account to interact with Google Cloud.
- D. Create a service account for the application and for each Google Cloud API used by the application. Export and deploy the private keys used by the application. Use the service account with one Google Cloud API to interact with Google Cloud.

**Correct Answer: A**

*Community vote distribution*

C (100%)

 **JonathanSJ** 2 months, 3 weeks ago

**Selected Answer: C**

C is correct.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: C**

C is correct.

upvoted 1 times

 **purushি** 8 months, 3 weeks ago

**Selected Answer: C**

B is easily eliminated.

A is not that much secure. Provides only authorization and not authentication. There is no IAM here.

D is more complex and not necessary to create service account for every API within the application.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

C. Create a service account for the application. Export and deploy the private key for the application. Use the service account to interact with Google Cloud.

This approach allows for least privileged access, as the service account will only have the necessary permissions to access the specific Google Cloud resources that the application needs. Option A, using an API key, would not provide the same level of granularity in terms of access permissions. Option B, using the default compute service account, would not provide the ability to restrict access to specific resources. Option D, creating a service account for each API, would be overly complex and may not be necessary if the permissions can be granted on a more general level.

upvoted 1 times

 **telp** 1 year, 3 months ago

**Selected Answer: C**

Answer C

upvoted 1 times

 **TNT87** 1 year, 4 months ago

Answer C

upvoted 1 times

 **zellck** 1 year, 4 months ago

**Selected Answer: C**

C is the answer.

upvoted 1 times

Question #170

Topic 1

You are in the final stage of migrating an on-premises data center to Google Cloud. You are quickly approaching your deadline, and discover that a web API is running on a server slated for decommissioning. You need to recommend a solution to modernize this API while migrating to Google Cloud. The modernized web API must meet the following requirements:

- Autoscales during high traffic periods at the end of each month
- Written in Python 3.x
- Developers must be able to rapidly deploy new versions in response to frequent code changes

You want to minimize cost, effort, and operational overhead of this migration. What should you do?

- Modernize and deploy the code on App Engine flexible environment.
- Modernize and deploy the code on App Engine standard environment.
- Deploy the modernized application to an n1-standard-1 Compute Engine instance.
- Ask the development team to re-write the application to run as a Docker container on Google Kubernetes Engine.

**Correct Answer: C**

*Community vote distribution*

B (88%)

13%

✉  **rajan\_** 7 months, 1 week ago

**Selected Answer: A**

App Engine flexible environment is a fully managed platform for running Python 3.x applications. It autoscales during high traffic periods and can be rapidly deployed using the App Engine SDK or the App Engine gcloud command-line tool. Additionally, App Engine flexible environment is a cost-effective solution, as you only pay for the resources that you use.

upvoted 1 times

✉  **wanrltw** 4 months, 3 weeks ago

Keep in mind that we're also asked to minimize the cost here.

The GAE Standard is better as it supports Python 3.x already and it's a cheaper solution. GAE Flexible doesn't scale down to 0 and it will always have at least 1 instance running.

upvoted 1 times

✉  **purushi** 8 months, 3 weeks ago

**Selected Answer: B**

B is a very straight forward option.

Clue: Python + Easy and fast scaling + Cost effective + frequent releases

upvoted 1 times

✉  **TNT87** 1 year, 4 months ago

[https://cloud.google.com/appengine/docs/standard#standard\\_environment\\_languages\\_and\\_runtimes](https://cloud.google.com/appengine/docs/standard#standard_environment_languages_and_runtimes)

Answer B

upvoted 1 times

✉  **micoams** 1 year, 4 months ago

**Selected Answer: B**

A,C and D can be eliminated

A. App engine flexible cannot scale down to 0, thus not minimizes the cost

C. Deploying to a single VM will not allow autoscaling

D. Running in a GKE cluster will not minimize the cost

That leaves B as the only valid option.

upvoted 2 times

✉  **zellck** 1 year, 4 months ago

**Selected Answer: B**

B is the answer.

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

upvoted 4 times

You are developing an application that consists of several microservices running in a Google Kubernetes Engine cluster. One microservice needs to connect to a third-party database running on-premises. You need to store credentials to the database and ensure that these credentials can be rotated while following security best practices. What should you do?

- A. Store the credentials in a sidecar container proxy, and use it to connect to the third-party database.
- B. Configure a service mesh to allow or restrict traffic from the Pods in your microservice to the database.
- C. Store the credentials in an encrypted volume mount, and associate a Persistent Volume Claim with the client Pod.
- D. Store the credentials as a Kubernetes Secret, and use the Cloud Key Management Service plugin to handle encryption and decryption.

**Correct Answer: A***Community vote distribution*

D (100%)

**rajan** 7 months, 1 week ago**Selected Answer: D**

D is correct.

upvoted 1 times

**purushi** 8 months, 3 weeks ago**Selected Answer: D**

Storing credentials as a Kubernetes secret + KMS for encryption and decryption of the DB credentials are the best answer.

upvoted 2 times

**mrvergara** 1 year, 2 months ago**Selected Answer: D**

Storing sensitive information such as database credentials in Kubernetes Secrets is a common and secure way to manage sensitive information in a cluster. The Cloud Key Management Service (KMS) can be used to further protect the secrets by encrypting and decrypting them, ensuring that they are protected both at rest and in transit. This combination of Kubernetes Secrets and Cloud KMS provides a secure way to manage and rotate credentials while following security best practices.

Options A and B are not recommended, as they do not provide a secure and centralized way to manage and rotate credentials. Option C is not recommended because storing secrets in an encrypted volume mount is not as secure as using a Key Management Service, as the encryption keys must still be managed and protected within the cluster.

upvoted 1 times

**TNT87** 1 year, 4 months ago<https://cloud.google.com/kubernetes-engine/docs/how-to/encrypting-secrets#reencrypt-secrets>

Answer D

upvoted 3 times

**zellick** 1 year, 4 months ago**Selected Answer: D**

D is the answer.

<https://cloud.google.com/kubernetes-engine/docs/how-to/encrypting-secrets>

By default, Google Kubernetes Engine (GKE) encrypts customer content stored at rest, including Secrets. GKE handles and manages this default encryption for you without any additional action on your part.

Application-layer secrets encryption provides an additional layer of security for sensitive data, such as Secrets, stored in etcd. Using this functionality, you can use a key managed with Cloud KMS to encrypt data at the application layer. This encryption protects against attackers who gain access to an offline copy of etcd.

upvoted 3 times

Question #172

Topic 1

You manage your company's ecommerce platform's payment system, which runs on Google Cloud. Your company must retain user logs for 1 year for internal auditing purposes and for 3 years to meet compliance requirements. You need to store new user logs on Google Cloud to minimize on-premises storage usage and ensure that they are easily searchable. You want to minimize effort while ensuring that the logs are stored correctly. What should you do?

- A. Store the logs in a Cloud Storage bucket with bucket lock turned on.
- B. Store the logs in a Cloud Storage bucket with a 3-year retention period.
- C. Store the logs in Cloud Logging as custom logs with a custom retention period.
- D. Store the logs in a Cloud Storage bucket with a 1-year retention period. After 1 year, move the logs to another bucket with a 2-year retention period.

**Correct Answer:** C

*Community vote distribution*

C (93%)

7%

 **micoams** Highly Voted 1 year, 4 months ago

**Selected Answer: C**

The requirements say that the logs should be easily searchable. This is not easily achieved in Cloud Storage, so that eliminates A,B and D.

That leaves C and the valid option.

Note, that it's possible to configure Cloud Logging with a custom retention period.

<https://cloud.google.com/logging/docs/buckets#custom-retention>

upvoted 9 times

 **zellck** 1 year, 4 months ago

Agree that Cloud Logging will be better for search.

upvoted 1 times

 **rajan\_** Most Recent 7 months, 1 week ago

**Selected Answer: C**

C is correct.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: C**

Tricky question.

Easily searchable is the key here.

Cloud logging supports retaining the logs between 1 to 3650 (10 years max) and we can set custom retention period on the cloud logs.

upvoted 1 times

 **telp** 1 year, 3 months ago

**Selected Answer: C**

C is the correct answer because Cloud Logging to retain logs between 1 day and 3650 days

upvoted 1 times

 **zellck** 1 year, 4 months ago

**Selected Answer: C**

C is the correct answer instead.

<https://cloud.google.com/logging/docs/routing/overview#logs-retention>

Cloud Logging retains logs according to retention rules applying to the log bucket type where the logs are held.

You can configure Cloud Logging to retain logs between 1 day and 3650 days. Custom retention rules apply to all the logs in a bucket, regard of the log type or whether that log has been copied from another location.

upvoted 2 times

Question #173

*Topic 1*

Your company has a new security initiative that requires all data stored in Google Cloud to be encrypted by customer-managed encryption keys. You plan to use Cloud Key Management Service (KMS) to configure access to the keys. You need to follow the "separation of duties" principle and Google-recommended best practices. What should you do? (Choose two.)

- A. Provision Cloud KMS in its own project.
- B. Do not assign an owner to the Cloud KMS project.
- C. Provision Cloud KMS in the project where the keys are being used.
- D. Grant the roles/cloudkms.admin role to the owner of the project where the keys from Cloud KMS are being used.
- E. Grant an owner role for the Cloud KMS project to a different user than the owner of the project where the keys from Cloud KMS are being used.

**Correct Answer: AE**

*Community vote distribution*

AB (74%)

AE (26%)

 **zellck** Highly Voted 1 year, 4 months ago

**Selected Answer: AB**

AB should be correct instead.

[https://cloud.google.com/kms/docs/separation-of-duties#using\\_separate\\_project](https://cloud.google.com/kms/docs/separation-of-duties#using_separate_project)

Instead, to allow for a separation of duties, you could run Cloud KMS in its own project, for example your-key-project. Then, depending on the strictness of your separation requirements, you could either:

- (recommended) Create your-key-project without an owner at the project level, and designate an Organization Admin granted at the organization-level. Unlike an owner, an Organization Admin can't manage or use keys directly. They are restricted to setting IAM policies, which restrict who can manage and use keys. Using an organization-level node, you can further restrict permissions for projects in your organization

upvoted 5 times

 **\_\_rajan\_\_** Most Recent 7 months, 1 week ago

**Selected Answer: AB**

AB is correct.

upvoted 2 times

 **\_\_rajan\_\_** 7 months, 1 week ago

AE is correct as E provide separation of duty.

upvoted 2 times

 **mrvergara** 1 year, 2 months ago

**Selected Answer: AE**

To follow Google-recommended best practices, I would recommend choosing options A and E:

A. Provision Cloud KMS in its own project - this helps to ensure that the management of encryption keys is isolated and separate from other projects in your Google Cloud organization.

E. Grant an owner role for the Cloud KMS project to a different user than the owner of the project where the keys from Cloud KMS are being used - this follows the "separation of duties" principle and helps to ensure that the management of encryption keys is not tied to the project where keys are being used.

upvoted 3 times

 **TNT87** 1 year, 4 months ago

**Selected Answer: AB**

Answer A, B

upvoted 3 times

 **micoams** 1 year, 4 months ago

**Selected Answer: AB**

As per the docs, [https://cloud.google.com/kms/docs/separation-of-duties#using\\_separate\\_project](https://cloud.google.com/kms/docs/separation-of-duties#using_separate_project)

1. The KMS should be in its own project

2. Ideally, you should not assign an owner to the KMS project

upvoted 4 times

 **zellck** 1 year, 4 months ago

After reading the documentation again, agree with you on AB.

[https://cloud.google.com/kms/docs/separation-of-duties#using\\_separate\\_project](https://cloud.google.com/kms/docs/separation-of-duties#using_separate_project)

(recommended) Create your-key-project without an owner at the project level, and designate an Organization Admin granted at the organization-level. Unlike an owner, an Organization Admin can't manage or use keys directly. They are restricted to setting IAM policies, which restrict who can manage and use keys. Using an organization-level node, you can further restrict permissions for projects in your organization.

upvoted 4 times

 **zellck** 1 year, 4 months ago

For E, the owner of the KMS project is different from the project where keys from Cloud KMS is used.

upvoted 1 times

 **zelick** 1 year, 4 months ago

**Selected Answer: AE**

AE is the answer.

[https://cloud.google.com/kms/docs/separation-of-duties#using\\_separate\\_project](https://cloud.google.com/kms/docs/separation-of-duties#using_separate_project)

Cloud KMS could be run in an existing project, for example your-project, and this might be sensible if the data being encrypted with keys in Cloud KMS is stored in the same project.

However, any user with owner access on that project is then also able to manage (and perform cryptographic operations with) keys in Cloud KMS in that project. This is because the keys themselves are owned by the project, of which the user is an owner.

Question #174

*Topic 1*

You need to migrate a standalone Java application running in an on-premises Linux virtual machine (VM) to Google Cloud in a cost-effective manner. You decide not to take the lift-and-shift approach, and instead you plan to modernize the application by converting it to a container. How should you accomplish this task?

- A. Use Migrate for Anthos to migrate the VM to your Google Kubernetes Engine (GKE) cluster as a container.
- B. Export the VM as a raw disk and import it as an image. Create a Compute Engine instance from the Imported image.
- C. Use Migrate for Compute Engine to migrate the VM to a Compute Engine instance, and use Cloud Build to convert it to a container.
- D. Use Jib to build a Docker image from your source code, and upload it to Artifact Registry. Deploy the application in a GKE cluster, and test the application.

**Correct Answer: A**

*Community vote distribution*

D (86%)

14%

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: D**

Jib is a tool that builds Docker images from Java code without the need for a Dockerfile. This makes it easy to containerize Java applications, even if you don't have any experience with Docker.

upvoted 2 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: D**

Going for D for the below reasons:

- Cost effective way
- Modernize the application by converting it to a container

upvoted 2 times

 **phil\_thain** 10 months, 2 weeks ago

**Selected Answer: A**

This seems to be exactly the situation described in this tutorial:

<https://cloud.google.com/migrate/containers/docs/migrating-monolith-vm-overview-setup>

So I think that option A is correct

upvoted 1 times

 **examprof** 4 months, 3 weeks ago

Indeed, but I think Alt A doesn't address the whole picture. Migrate for Anthos itself would not automatically containerize the Java app running on the Linux VM. Migrate for Anthos can package the VM as a Kubernetes pod, but the application within the VM remains unchanged in its original form. To containerize this application and make it fully compatible with GKE, additional steps - those described in Alt D - would be required.

Alternative D is correct.

upvoted 1 times

 **telp** 1 year, 3 months ago

**Selected Answer: D**

Answer D

<https://cloud.google.com/blog/products/application-development/introducing-jib-build-java-docker-images-better>

upvoted 1 times

 **TNT87** 1 year, 4 months ago

Answer D

<https://cloud.google.com/blog/products/application-development/introducing-jib-build-java-docker-images-better>

upvoted 1 times

 **zellck** 1 year, 4 months ago

**Selected Answer: D**

D is the answer.

<https://cloud.google.com/blog/products/application-development/introducing-jib-build-java-docker-images-better>

upvoted 1 times

Question #175

Topic 1

Your organization has recently begun an initiative to replatform their legacy applications onto Google Kubernetes Engine. You need to decompose a monolithic application into microservices. Multiple instances have read and write access to a configuration file, which is stored on a shared file system. You want to minimize the effort required to manage this transition, and you want to avoid rewriting the application code. What should you do?

- A. Create a new Cloud Storage bucket, and mount it via FUSE in the container.
- B. Create a new persistent disk, and mount the volume as a shared PersistentVolume.
- C. Create a new Filestore instance, and mount the volume as an NFS PersistentVolume.
- D. Create a new ConfigMap and volumeMount to store the contents of the configuration file.

**Correct Answer: A**

*Community vote distribution*

C (81%)

D (19%)

 **x\_cath** Highly Voted 1 year, 4 months ago

**Selected Answer: C**

- A is incorrect, because Cloud Storage FUSE does not support concurrency and file locking.  
B is incorrect, because a persistent disk PersistentVolume is not read-write-many. It can only be read-write once or read-many.  
C is correct, because it's the only managed, supported read-write-many storage option available for file-system access in Google Kubernetes Engine.  
D is incorrect, because the ConfigMap cannot be written to from the Pods.

Question #176

Topic 1

Your development team has built several Cloud Functions using Java along with corresponding integration and service tests. You are building and deploying the functions and launching the tests using Cloud Build. Your Cloud Build job is reporting deployment failures immediately after successfully validating the code. What should you do?

- A. Check the maximum number of Cloud Function instances.
- B. Verify that your Cloud Build trigger has the correct build parameters.
- C. Retry the tests using the truncated exponential backoff polling strategy.
- D. Verify that the Cloud Build service account is assigned the Cloud Functions Developer role.

**Correct Answer: C**

*Community vote distribution*

D (100%)

 **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: D**

D is correct.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: D**

Cloud Build service account must have the IAM developer role in order to deploy cloud functions.

upvoted 1 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: D**

[https://cloud.google.com/build/docs/securing-builds/configure-access-for-cloud-build-service-account#granting\\_a\\_role\\_using\\_the\\_iam\\_page](https://cloud.google.com/build/docs/securing-builds/configure-access-for-cloud-build-service-account#granting_a_role_using_the_iam_page)

[https://cloud.google.com/build/docs/troubleshooting#build\\_trigger\\_fails\\_due\\_to\\_missing\\_cloudbuildbuildscreate\\_permission](https://cloud.google.com/build/docs/troubleshooting#build_trigger_fails_due_to_missing_cloudbuildbuildscreate_permission)

upvoted 1 times

 **telp** 1 year, 3 months ago

**Selected Answer: D**

Answer D

upvoted 1 times

 **TNT87** 1 year, 4 months ago

[https://cloud.google.com/build/docs/troubleshooting#build\\_trigger\\_fails\\_due\\_to\\_missing\\_cloudbuildbuildscreate\\_permission](https://cloud.google.com/build/docs/troubleshooting#build_trigger_fails_due_to_missing_cloudbuildbuildscreate_permission)

Answer D

upvoted 1 times

 **zellick** 1 year, 4 months ago

**Selected Answer: D**

D is the answer.

<https://cloud.google.com/build/docs/securing-builds/configure-access-for-cloud-build-service-account>

upvoted 1 times

Question #177

*Topic 1*

You manage a microservices application on Google Kubernetes Engine (GKE) using Istio. You secure the communication channels between your microservices by implementing an Istio AuthorizationPolicy, a Kubernetes NetworkPolicy, and mTLS on your GKE cluster. You discover that HTTP requests between two Pods to specific URLs fail, while other requests to other URLs succeed. What is the cause of the connection issue?

- A. A Kubernetes NetworkPolicy resource is blocking HTTP traffic between the Pods.
- B. The Pod initiating the HTTP requests is attempting to connect to the target Pod via an incorrect TCP port.
- C. The Authorization Policy of your cluster is blocking HTTP requests for specific paths within your application.
- D. The cluster has mTLS configured in permissive mode, but the Pod's sidecar proxy is sending unencrypted traffic in plain text.

**Correct Answer:** D

*Community vote distribution*

C (100%)

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: C**

C is correct.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: C**

Key here is "HTTP requests between two Pods to specific URLs fail", this means no auth rule set for these urls in the Istio configuration.

upvoted 1 times

 **telp** 1 year, 3 months ago

**Selected Answer: C**

A is not correct because Kubernetes NetworkPolicy resources allow you to block HTTP traffic between groups of pods but not for selected paths. (<https://kubernetes.io/docs/concepts/services-networking/network-policies/>).

B is not correct because if the client pod is using an incorrect port to communicate with the server, pod requests will time out for all URL path  
C is correct because an Istio Authorization policy allows you to block HTTP methods between pods for specific URL paths

(<https://istio.io/latest/docs/tasks/security/authorization/authz-http/>).

D is not correct because mTLS configuration using Istio should not cause HTTP requests to fail. In permissive mode (default configuration), a service can accept both plain text and mTLS encrypted traffic (<https://istio.io/latest/docs/tasks/security/authentication/mtls-migration/>).

upvoted 3 times

 **TNT87** 1 year, 4 months ago

**Selected Answer: C**

[https://cloud.google.com/service-mesh/docs/troubleshooting/troubleshoot-security#authorization\\_policy\\_denial\\_logging](https://cloud.google.com/service-mesh/docs/troubleshooting/troubleshoot-security#authorization_policy_denial_logging)

Answer C

<https://istio.io/latest/docs/ops/common-problems/network-issues/#sending-https-to-an-http-port>

upvoted 1 times

 **zellck** 1 year, 4 months ago

**Selected Answer: C**

C is the answer.

upvoted 1 times

Question #178

Topic 1

You recently migrated an on-premises monolithic application to a microservices application on Google Kubernetes Engine (GKE). The application has dependencies on backend services on-premises, including a CRM system and a MySQL database that contains personally identifiable information (PII). The backend services must remain on-premises to meet regulatory requirements.

You established a Cloud VPN connection between your on-premises data center and Google Cloud. You notice that some requests from your microservices application on GKE to the backend services are failing due to latency issues caused by fluctuating bandwidth, which is causing the application to crash. How should you address the latency issues?

- A. Use Memorystore to cache frequently accessed PII data from the on-premises MySQL database

- B. Use Istio to create a service mesh that includes the microservices on GKE and the on-premises services
- C. Increase the number of Cloud VPN tunnels for the connection between Google Cloud and the on-premises services
- D. Decrease the network layer packet size by decreasing the Maximum Transmission Unit (MTU) value from its default value on Cloud VPN

**Correct Answer: A**

*Community vote distribution*

C (69%)

B (23%)

8%

 **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: B**

To use Istio to reduce latency in your microservices application, you would create a service mesh that includes the microservices on GKE and on-premises services. Istio would then manage traffic between the microservices and the on-premises services, and would use its features to reduce latency.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: C**

Cloud Interconnect would be better option than C, I guess. Increase the VPN tunnels would provide the required bandwidth for the GCP and on-premises services to communicate.

upvoted 1 times

 **DonWang** 10 months ago

**Selected Answer: C**

C for increase bandwidth

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: B**

Istio can help to address the latency issues by creating a service mesh that allows you to control the flow of traffic between the microservices on GKE and the on-premises services. This can allow you to monitor and manage the traffic, as well as implement features such as load balancing and circuit breaking to help mitigate the impact of latency on the application. It also allows to increase the number of Cloud VPN tunnels for the connection between Google Cloud and the on-premises services, but it is not the best approach. Increasing the number of tunnels can help to increase the available bandwidth, but it does not address the underlying issues causing the latency. Decreasing the network layer packet size or decreasing the MTU value on Cloud VPN can cause fragmentation, which can increase latency, so it is not a good approach. Caching of PII data can be a good practice but it does not address the latency issues caused by fluctuating bandwidth.

upvoted 2 times

 **mrvergara** 1 year, 3 months ago

It could be D. If you decrease the MTU, the packets get priority in FIFO queue of the routers.

upvoted 1 times

 **TNT87** 1 year, 4 months ago

Answer C.

Take note the question is asking you to address a bandwidth issue, C is the most appropriate answer.

upvoted 2 times

 **zellick** 1 year, 4 months ago

**Selected Answer: C**

C is the correct answer instead.

<https://cloud.google.com/network-connectivity/docs/vpn/concepts/topologies#more-bandwidth>  
To increase the bandwidth of your HA VPN gateways, add more HA VPN tunnels.

upvoted 3 times

 **micoams** 1 year, 4 months ago

**Selected Answer: C**

A, B, and D can be eliminated

- A. Caching PII (Personally Identifiable Information) is never a good practice
- B. Using Istio is not going to improve the latency (the network hops remain the same)
- C. Reducing the packet size, has the effect of more packets being sent across which is counter productive

That leaves C as the valid option

GCP does support having multiple VPN Tunnels on the same gateway

<https://cloud.google.com/network-connectivity/docs/vpn/concepts/choosing-networks-routing#route-alignment>  
upvoted 4 times

 **zellck** 1 year, 4 months ago

Agree with you on C.

<https://cloud.google.com/network-connectivity/docs/vpn/concepts/topologies#more-bandwidth>

To increase the bandwidth of your HA VPN gateways, add more HA VPN tunnels.

upvoted 1 times

 **zellck** 1 year, 4 months ago

**Selected Answer: A**

A is the answer.

upvoted 1 times

 **TNT87** 1 year, 4 months ago

Tjats not a bandwidth issue , you want to address the bandwidth issue here

upvoted 1 times

Question #179

Topic 1

Your company has deployed a new API to a Compute Engine instance. During testing, the API is not behaving as expected. You want to monitor the application over 12 hours to diagnose the problem within the application code without redeploying the application. Which tool should you use?

- A. Cloud Trace
- B. Cloud Monitoring

C. Cloud Debugger logpoints

D. Cloud Debugger snapshots

**Correct Answer: B**

*Community vote distribution*

C (100%)

**rajan** 7 months, 1 week ago

Question #180

Topic 1

You are designing an application that consists of several microservices. Each microservice has its own RESTful API and will be deployed as a separate Kubernetes Service. You want to ensure that the consumers of these APIs aren't impacted when there is a change to your API, and also ensure that third-party systems aren't interrupted when new versions of the API are released. How should you configure the connection to the application following Google-recommended best practices?

- A. Use an Ingress that uses the API's URL to route requests to the appropriate backend.
- B. Leverage a Service Discovery system, and connect to the backend specified by the request.
- C. Use multiple clusters, and use DNS entries to route requests to separate versioned backends.
- D. Combine multiple versions in the same service, and then specify the API version in the POST request.

**Correct Answer: C**

*Community vote distribution*

A (73%)

D (18%)

9%

**rajan** 7 months, 1 week ago

**Selected Answer: B**

This approach is recommended by Google because it allows you to decouple the consumers of your APIs from the specific backend services that are providing those APIs. This makes it easier to scale your application and to make changes to your APIs without impacting the consumers.

upvoted 1 times

**rajan** 7 months, 1 week ago

Answer will be A.

upvoted 1 times

**purushi** 8 months, 3 weeks ago

**Selected Answer: A**

Ingress or Nginx service that routes ( reverse proxy ) to the appropriate urls is a best solution.

upvoted 2 times

**TNT87** 1 year, 4 months ago

**Selected Answer: A**

[https://cloud.google.com/kubernetes-engine/docs/concepts/ingress#deprecated\\_annotation](https://cloud.google.com/kubernetes-engine/docs/concepts/ingress#deprecated_annotation)

[https://cloud.google.com/kubernetes-engine/docs/concepts/ingress#features\\_of\\_https\\_load\\_balancing](https://cloud.google.com/kubernetes-engine/docs/concepts/ingress#features_of_https_load_balancing)

Answer A

upvoted 3 times

**micoams** 1 year, 4 months ago

**Selected Answer: A**

B,C, and D can be eliminated

B. Service discovery only works within the cluster itself, so external clients can't use it

C. Using multiple clusters is an overkill, you can deploy multiple versions of the same service within a single cluster

D. Passing the API version in the request body is not a REST best practice

The best practice is to pass the version of the API in the URL path, e.g /v1/foo, /v2/foo

Using this approach, you can route requests to the appropriate backend service within the GKE cluster using an Ingress resource, which is optional.

upvoted 3 times

**zellick** 1 year, 4 months ago

**Selected Answer: D**

D is the answer.

upvoted 2 times

Question #181

Topic 1

Your team is building an application for a financial institution. The application's frontend runs on Compute Engine, and the data resides in Cloud SQL and one Cloud Storage bucket. The application will collect data containing PII, which will be stored in the Cloud SQL database and the Cloud Storage bucket. You need to secure the PII data. What should you do?

- A. 1. Create the relevant firewall rules to allow only the frontend to communicate with the Cloud SQL database  
2. Using IAM, allow only the frontend service account to access the Cloud Storage bucket
- B. 1. Create the relevant firewall rules to allow only the frontend to communicate with the Cloud SQL database  
2. Enable private access to allow the frontend to access the Cloud Storage bucket privately
- C. 1. Configure a private IP address for Cloud SQL  
2. Use VPC-SC to create a service perimeter  
3. Add the Cloud SQL database and the Cloud Storage bucket to the same service perimeter
- D. 1. Configure a private IP address for Cloud SQL  
2. Use VPC-SC to create a service perimeter  
3. Add the Cloud SQL database and the Cloud Storage bucket to different service perimeters

**Correct Answer:** *B*

*Community vote distribution*

C (93%)

7%

 **micoams**  1 year, 4 months ago

**Selected Answer: C**

Without using VPC-SC, the PII data is not secure from exfiltration. So that leaves only C, and D as possible valid responses. However, D can be eliminated because both the Cloud SQL instance and Cloud Storage bucket must be within the same perimeter, which leaves C and the \ answer.

upvoted 5 times

 **\_rajan\_**  7 months, 1 week ago

**Selected Answer: C**

I would go with C

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: C**

C is correct compared to other options.

upvoted 2 times

 **zellck** 1 year, 3 months ago

**Selected Answer: C**

C should be the correct answer instead.

upvoted 2 times

 **TNT87** 1 year, 3 months ago

**Selected Answer: C**

Answer C

upvoted 3 times

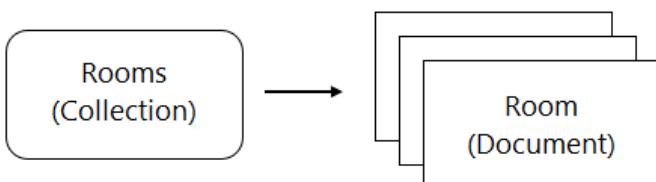
 **zellck** 1 year, 4 months ago

Question #182

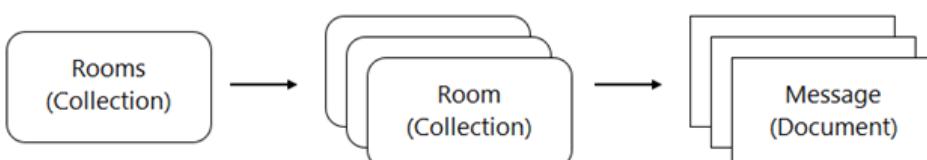
Topic 1

You are designing a chat room application that will host multiple rooms and retain the message history for each room. You have selected Firestore as your database. How should you represent the data in Firestore?

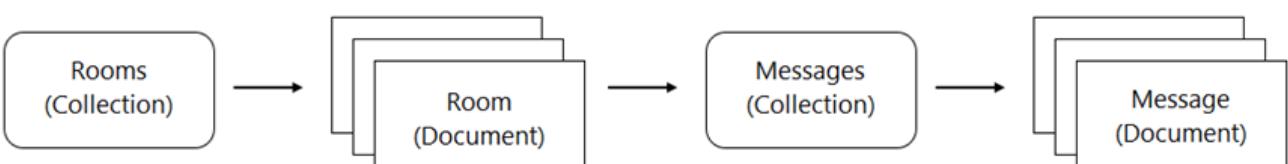
- A. Create a collection for the rooms. For each room, create a document that lists the contents of the messages



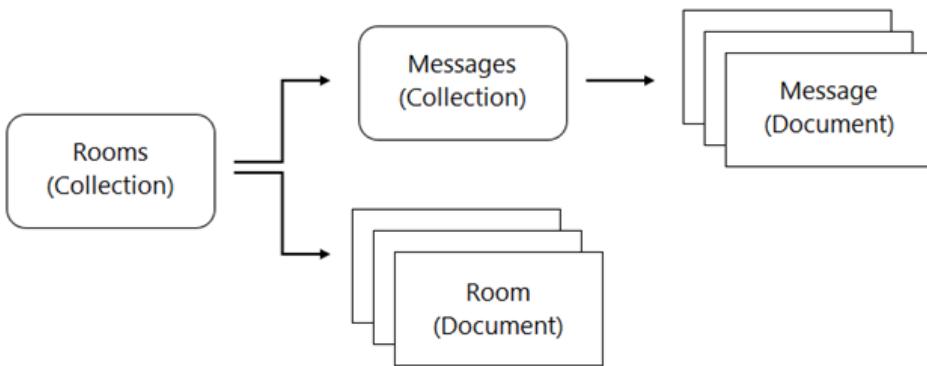
- B. Create a collection for the rooms. For each room, create a collection that contains a document for each message



- C. Create a collection for the rooms. For each room, create a document that contains a collection for documents, each of which contains a message.



- D. Create a collection for the rooms, and create a document for each room. Create a separate collection for messages, with one document per message. Each room's document contains a list of references to the messages.



**Correct Answer: C**

*Community vote distribution*

C (100%)

 \_\_rajan\_\_ 7 months, 1 week ago

**Selected Answer: C**

Community answer C.

upvoted 1 times

 **TNT87** 1 year, 4 months ago

Answer C

upvoted 1 times

 **zellick** 1 year, 4 months ago

**Selected Answer: C**

C is the answer.

<https://firebase.google.com/docs/firestore/data-model#hierarchical-data>

upvoted 2 times

 **gardislan18** 1 year, 4 months ago

**Selected Answer: C**

Answer is C. "The best way to store messages in this scenario is by using subcollections. A subcollection is a collection associated with a specific document."

<https://firebase.google.com/docs/firestore/data-model#subcollections>

upvoted 1 times

You are developing an application that will handle requests from end users. You need to secure a Cloud Function called by the application to allow authorized end users to authenticate to the function via the application while restricting access to unauthorized users. You will integrate Google Sign-In as part of the solution and want to follow Google-recommended best practices. What should you do?

- A. Deploy from a source code repository and grant users the roles/cloudfunctions.viewer role.
- B. Deploy from a source code repository and grant users the roles/cloudfunctions.invoker role
- C. Deploy from your local machine using gcloud and grant users the roles/cloudfunctions.admin role
- D. Deploy from your local machine using gcloud and grant users the roles/cloudfunctions.developer role

**Correct Answer: C***Community vote distribution*

B (100%)

**✉️**  **JonathanSJ** 2 months, 3 weeks ago**Selected Answer: B**

B is the answer

upvoted 1 times

**✉️**  **purushi** 8 months, 3 weeks ago**Selected Answer: B**

The key here is "secure a Cloud Function CALLED by the application to allow authorized end users to authenticate to the function via the application while restricting access to unauthorized users"

upvoted 1 times

**✉️**  **TNT87** 1 year, 4 months ago

Answer B

upvoted 2 times

**✉️**  **zellick** 1 year, 4 months ago**Selected Answer: B**

B is the answer.

upvoted 1 times

**✉️**  **esc** 1 year, 4 months ago**Selected Answer: B**

Have the user account you are using to access Cloud Functions assigned a role that contains the cloudfunctions.functions.invoke permission default, the Cloud Functions Admin and Cloud Functions Developer roles have this permission. See Cloud Functions IAM Roles for the full list of roles and their associated permissions.

upvoted 1 times

You are running a web application on Google Kubernetes Engine that you inherited. You want to determine whether the application is using libraries with known vulnerabilities or is vulnerable to XSS attacks. Which service should you use?

- A. Google Cloud Armor
- B. Debugger
- C. Web Security Scanner
- D. Error Reporting

**Correct Answer: C**

*Community vote distribution*

C (100%)

✉️  **alpha\_canary** 2 weeks, 1 day ago

**Selected Answer: C**

<https://cloud.google.com/security-command-center/docs/how-to-remediate-web-security-scanner-findings#xss>

upvoted 1 times

✉️  **JonathanSJ** 2 months, 3 weeks ago

**Selected Answer: C**

Answer is C

upvoted 1 times

✉️  **purushi** 8 months, 3 weeks ago

**Selected Answer: C**

Web security scanner under gcp environment or we can use GRYPE for vulnerability scanning in on premise networks.

upvoted 2 times

✉️  **TNT87** 1 year, 4 months ago

<https://cloud.google.com/security-command-center/docs/how-to-remediate-web-security-scanner-findings>

Answer C

upvoted 1 times

✉️  **zellck** 1 year, 4 months ago

**Selected Answer: C**

C is the answer.

<https://cloud.google.com/security-command-center/docs/concepts-web-security-scanner-overview>

Web Security Scanner identifies security vulnerabilities in your App Engine, Google Kubernetes Engine (GKE), and Compute Engine web applications. It crawls your application, following all links within the scope of your starting URLs, and attempts to exercise as many user input and event handlers as possible.

upvoted 2 times

✉️  **melisargh** 1 year, 4 months ago

C is correct

<https://cloud.google.com/security-command-center/docs/concepts-web-security-scanner-overview>

upvoted 1 times

Question #185

*Topic 1*

You are building a highly available and globally accessible application that will serve static content to users. You need to configure the storage and serving components. You want to minimize management overhead and latency while maximizing reliability for users. What should you do?

- A. 1. Create a managed instance group. Replicate the static content across the virtual machines (VMs)  
2. Create an external HTTP(S) load balancer.  
3. Enable Cloud CDN, and send traffic to the managed instance group.
- B. 1. Create an unmanaged instance group. Replicate the static content across the VMs.  
2. Create an external HTTP(S) load balancer  
3. Enable Cloud CDN, and send traffic to the unmanaged instance group.
- C. 1. Create a Standard storage class, regional Cloud Storage bucket. Put the static content in the bucket  
2. Reserve an external IP address, and create an external HTTP(S) load balancer  
3. Enable Cloud CDN, and send traffic to your backend bucket
- D. 1. Create a Standard storage class, multi-regional Cloud Storage bucket. Put the static content in the bucket.  
2. Reserve an external IP address, and create an external HTTP(S) load balancer.  
3. Enable Cloud CDN, and send traffic to your backend bucket.

**Correct Answer: B**

*Community vote distribution*

D (100%)

 **alpha\_canary** 2 weeks, 1 day ago

**Selected Answer: D**

A & B are out easily.

we might be tempted to go for C for lower cost, however, using a regional bucket could increase latency for users who are not located near the chosen region. A multi-regional bucket would be a better choice for a globally accessible application. So go with D

upvoted 1 times

 **JonathanSJ** 2 months, 3 weeks ago

**Selected Answer: D**

D is the answer.

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: D**

D is correct.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: D**

Highly available = Multi-region Cloud Storage bucket

Globally accessible: Https load balancer

Application that will serve static content to users: Cloud CDN

upvoted 4 times

 **TNT87** 1 year, 4 months ago

Answer D

upvoted 2 times

 **zellick** 1 year, 4 months ago

**Selected Answer: D**

D is the answer.

upvoted 1 times

 **esc** 1 year, 4 months ago

**Selected Answer: D**

multi regional, less maintenance

upvoted 1 times

Question #186

Topic 1

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Company Overview -

HipLocal is a community application designed to facilitate communication between people in close proximity. It is used for event planning and organizing sporting events, and for businesses to connect with their local communities. HipLocal launched recently in a few neighborhoods in Dallas and is rapidly growing into a global phenomenon. Its unique style of hyper-local community communication and business outreach is in demand around the world.

Executive Statement -

We are the number one local community app; it's time to take our local community services global. Our venture capital investors want to see rapid growth and the same great experience for new local and virtual communities that come online, whether their members are 10 or 10000 miles away from each other.

Solution Concept -

HipLocal wants to expand their existing service, with updated functionality, in new regions to better serve their global customers. They want to hire and train a new team to support these regions in their time zones. They will need to ensure that the application scales smoothly and provides clear uptime data, and that they analyze and respond to any issues that occur.

Existing Technical Environment -

HipLocal's environment is a mix of on-premises hardware and infrastructure running in Google Cloud Platform. The HipLocal team understands their application well, but has limited experience in global scale applications. Their existing technical environment is as follows:

- Existing APIs run on Compute Engine virtual machine instances hosted in GCP.
- State is stored in a single instance MySQL database in GCP.
- Release cycles include development freezes to allow for QA testing.
- The application has no logging.
- Applications are manually deployed by infrastructure engineers during periods of slow traffic on weekday evenings.
- There are basic indicators of uptime; alerts are frequently fired when the APIs are unresponsive.

Business Requirements -

HipLocal's investors want to expand their footprint and support the increase in demand they are seeing. Their requirements are:

- Expand availability of the application to new regions.
  - Support 10x as many concurrent users.
  - Ensure a consistent experience for users when they travel to different regions.
  - Obtain user activity metrics to better understand how to monetize their product.
  - Ensure compliance with regulations in the new regions (for example, GDPR).
  - Reduce infrastructure management time and cost.
  - Adopt the Google-recommended practices for cloud computing.
- Develop standardized workflows and processes around application lifecycle management.
- Define service level indicators (SLIs) and service level objectives (SLOs).

**Technical Requirements -**

- Provide secure communications between the on-premises data center and cloud-hosted applications and infrastructure.
- The application must provide usage metrics and monitoring.
- APIs require authentication and authorization.
- Implement faster and more accurate validation of new features.
- Logging and performance metrics must provide actionable information to be able to provide debugging information and alerts.
- Must scale to meet user demand.

For this question refer to the HipLocal case study.

HipLocal wants to reduce the latency of their services for users in global locations. They have created read replicas of their database in locations where their users reside and configured their service to read traffic using those replicas. How should they further reduce latency for all database interactions with the least amount of effort?

- A. Migrate the database to Bigtable and use it to serve all global user traffic.
- B. Migrate the database to Cloud Spanner and use it to serve all global user traffic.
- C. Migrate the database to Firestore in Datastore mode and use it to serve all global user traffic.
- D. Migrate the services to Google Kubernetes Engine and use a load balancer service to better scale the application.

**Correct Answer: D**

*Community vote distribution*

B (100%)

 **JonathanSJ** 2 months, 3 weeks ago

**Selected Answer: B**

B is the answer.  
upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: B**

B is correct.  
upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: B**

Cloud spanner is the only best fit solution here.  
upvoted 1 times

 **zellck** 1 year, 4 months ago

**Selected Answer: B**

B is the answer.  
upvoted 1 times

 **TNT87** 1 year, 4 months ago

Answer B  
upvoted 1 times

 **micoams** 1 year, 4 months ago

**Selected Answer: B**

While the question asks for "least amount of effort" ... all possible answers require a database migration. So it really boils down, to which database will be easiest to migrate to.

Question #187

Topic 1

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Company Overview -

HipLocal is a community application designed to facilitate communication between people in close proximity. It is used for event planning and organizing sporting events, and for businesses to connect with their local communities. HipLocal launched recently in a few neighborhoods in Dallas and is rapidly growing into a global phenomenon. Its unique style of hyper-local community communication and business outreach is in

demand around the world.

#### Executive Statement -

We are the number one local community app; it's time to take our local community services global. Our venture capital investors want to see rapid growth and the same great experience for new local and virtual communities that come online, whether their members are 10 or 10000 miles away from each other.

#### Solution Concept -

HipLocal wants to expand their existing service, with updated functionality, in new regions to better serve their global customers. They want to hire and train a new team to support these regions in their time zones. They will need to ensure that the application scales smoothly and provides clear uptime data, and that they analyze and respond to any issues that occur.

#### Existing Technical Environment -

HipLocal's environment is a mix of on-premises hardware and infrastructure running in Google Cloud Platform. The HipLocal team understands their application well, but has limited experience in global scale applications. Their existing technical environment is as follows:

- Existing APIs run on Compute Engine virtual machine instances hosted in GCP.
- State is stored in a single instance MySQL database in GCP.
- Release cycles include development freezes to allow for QA testing.
- The application has no logging.
- Applications are manually deployed by infrastructure engineers during periods of slow traffic on weekday evenings.
- There are basic indicators of uptime; alerts are frequently fired when the APIs are unresponsive.

#### Business Requirements -

HipLocal's investors want to expand their footprint and support the increase in demand they are seeing. Their requirements are:

- Expand availability of the application to new regions.
- Support 10x as many concurrent users.
- Ensure a consistent experience for users when they travel to different regions.
- Obtain user activity metrics to better understand how to monetize their product.
- Ensure compliance with regulations in the new regions (for example, GDPR).
- Reduce infrastructure management time and cost.
- Adopt the Google-recommended practices for cloud computing.
- Develop standardized workflows and processes around application lifecycle management.
- Define service level indicators (SLIs) and service level objectives (SLOs).

#### Technical Requirements -

- Provide secure communications between the on-premises data center and cloud-hosted applications and infrastructure.
- The application must provide usage metrics and monitoring.
- APIs require authentication and authorization.
- Implement faster and more accurate validation of new features.
- Logging and performance metrics must provide actionable information to be able to provide debugging information and alerts.
- Must scale to meet user demand.

For this question, refer to the HipLocal case study.

Which Google Cloud product addresses HipLocal's business requirements for service level indicators and objectives?

- A. Cloud Profiler
- B. Cloud Monitoring
- C. Cloud Trace
- D. Cloud Logging

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **JonathanSJ** 2 months, 3 weeks ago

**Selected Answer: B**

B is the answer.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: B**

B is correct. Simple and straight forward.

upvoted 1 times

 **telp** 1 year, 3 months ago

**Selected Answer: B**

Answer B

upvoted 1 times

 **TNT87** 1 year, 4 months ago

Answer B

upvoted 1 times

 **zellck** 1 year, 4 months ago

**Selected Answer: B**

B is the answer.

<https://cloud.google.com/stackdriver/docs/solutions/slo-monitoring>

upvoted 1 times

 **gardislan18** 1 year, 4 months ago

**Selected Answer: B**

Answer is B

<https://cloud.google.com/stackdriver/docs/solutions/slo-monitoring#defn-sli>

upvoted 1 times

**Case study -**

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

**To start the case study -**

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

**Company Overview -**

HipLocal is a community application designed to facilitate communication between people in close proximity. It is used for event planning and organizing sporting events, and for businesses to connect with their local communities. HipLocal launched recently in a few neighborhoods in Dallas and is rapidly growing into a global phenomenon. Its unique style of hyper-local community communication and business outreach is in demand around the world.

**Executive Statement -**

We are the number one local community app; it's time to take our local community services global. Our venture capital investors want to see rapid growth and the same great experience for new local and virtual communities that come online, whether their members are 10 or 10000 miles away from each other.

**Solution Concept -**

HipLocal wants to expand their existing service, with updated functionality, in new regions to better serve their global customers. They want to hire and train a new team to support these regions in their time zones. They will need to ensure that the application scales smoothly and provides

clear uptime data, and that they analyze and respond to any issues that occur.

#### Existing Technical Environment -

HipLocal's environment is a mix of on-premises hardware and infrastructure running in Google Cloud Platform. The HipLocal team understands their application well, but has limited experience in global scale applications. Their existing technical environment is as follows:

- Existing APIs run on Compute Engine virtual machine instances hosted in GCP.
- State is stored in a single instance MySQL database in GCP.
- Release cycles include development freezes to allow for QA testing.
- The application has no logging.
- Applications are manually deployed by infrastructure engineers during periods of slow traffic on weekday evenings.
- There are basic indicators of uptime; alerts are frequently fired when the APIs are unresponsive.

#### Business Requirements -

HipLocal's investors want to expand their footprint and support the increase in demand they are seeing. Their requirements are:

- Expand availability of the application to new regions.
  - Support 10x as many concurrent users.
  - Ensure a consistent experience for users when they travel to different regions.
  - Obtain user activity metrics to better understand how to monetize their product.
  - Ensure compliance with regulations in the new regions (for example, GDPR).
  - Reduce infrastructure management time and cost.
  - Adopt the Google-recommended practices for cloud computing.
- Develop standardized workflows and processes around application lifecycle management.
- Define service level indicators (SLIs) and service level objectives (SLOs).

#### Technical Requirements -

- Provide secure communications between the on-premises data center and cloud-hosted applications and infrastructure.
- The application must provide usage metrics and monitoring.
- APIs require authentication and authorization.
- Implement faster and more accurate validation of new features.
- Logging and performance metrics must provide actionable information to be able to provide debugging information and alerts.
- Must scale to meet user demand.

For this question, refer to the HipLocal case study.

A recent security audit discovers that HipLocal's database credentials for their Compute Engine-hosted MySQL databases are stored in plain text on persistent disks. HipLocal needs to reduce the risk of these credentials being stolen. What should they do?

- A. Create a service account and download its key. Use the key to authenticate to Cloud Key Management Service (KMS) to obtain the database credentials.
- B. Create a service account and download its key. Use the key to authenticate to Cloud Key Management Service (KMS) to obtain a key used to decrypt the database credentials.
- C. Create a service account and grant it the roles/iam.serviceAccountUser role. Impersonate as this account and authenticate using the Cloud SQL Proxy.
- D. Grant the roles/secretmanager.secretAccessor role to the Compute Engine service account. Store and access the database credentials with the Secret Manager API.

**Correct Answer: C***Community vote distribution*

D (100%)

  **JonathanSJ** 2 months, 3 weeks ago**Selected Answer: D**

D is the answer.

upvoted 1 times

  **\_\_rajan\_\_** 7 months, 1 week ago**Selected Answer: D**

Secret Manager is a service that helps you manage and protect your secrets. You can store secrets such as passwords, API keys, and SSH keys in Secret Manager. Secret Manager encrypts your secrets using Google-managed encryption keys, and it provides you with a number of features to help you manage and protect your secrets.

upvoted 1 times

  **purushi** 8 months, 3 weeks ago**Selected Answer: D**

D is the best option here.

upvoted 1 times

  **zellick** 1 year, 4 months ago**Selected Answer: D**

D is the answer.

upvoted 1 times

  **TNT87** 1 year, 4 months ago

Answer D

<https://cloud.google.com/secret-manager/docs/best-practices>

upvoted 1 times

  **micoams** 1 year, 4 months ago**Selected Answer: D**

Both A, and B go against best practices that say you should try avoiding service account keys. Plus, these two answers would still store the service account key in the VM.

Option C is completely irrelevant as it does not address the issue at hand, which is plain text credentials stored on disk.

This leaves option D as the valid option.

upvoted 1 times

  **micoams** 1 year, 4 months ago

Correction: "avoid downloading service account keys"

upvoted 1 times

  **esc** 1 year, 4 months ago**Selected Answer: D**<https://cloud.google.com/secret-manager/docs/overview>

upvoted 1 times

Question #189

Topic 1

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

#### To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

#### Company Overview -

HipLocal is a community application designed to facilitate communication between people in close proximity. It is used for event planning and organizing sporting events, and for businesses to connect with their local communities. HipLocal launched recently in a few neighborhoods in Dallas and is rapidly growing into a global phenomenon. Its unique style of hyper-local community communication and business outreach is in demand around the world.

#### Executive Statement -

We are the number one local community app; it's time to take our local community services global. Our venture capital investors want to see rapid growth and the same great experience for new local and virtual communities that come online, whether their members are 10 or 10000 miles away from each other.

#### Solution Concept -

HipLocal wants to expand their existing service, with updated functionality, in new regions to better serve their global customers. They want to hire and train a new team to support these regions in their time zones. They will need to ensure that the application scales smoothly and provides clear uptime data, and that they analyze and respond to any issues that occur.

#### Existing Technical Environment -

HipLocal's environment is a mix of on-premises hardware and infrastructure running in Google Cloud Platform. The HipLocal team understands their application well, but has limited experience in global scale applications. Their existing technical environment is as follows:

- Existing APIs run on Compute Engine virtual machine instances hosted in GCP.
- State is stored in a single instance MySQL database in GCP.
- Release cycles include development freezes to allow for QA testing.
- The application has no logging.
- Applications are manually deployed by infrastructure engineers during periods of slow traffic on weekday evenings.
- There are basic indicators of uptime; alerts are frequently fired when the APIs are unresponsive.

#### Business Requirements -

HipLocal's investors want to expand their footprint and support the increase in demand they are seeing. Their requirements are:

- Expand availability of the application to new regions.
- Support 10x as many concurrent users.
- Ensure a consistent experience for users when they travel to different regions.
- Obtain user activity metrics to better understand how to monetize their product.

- Ensure compliance with regulations in the new regions (for example, GDPR).
- Reduce infrastructure management time and cost.
- Adopt the Google-recommended practices for cloud computing.
- Develop standardized workflows and processes around application lifecycle management.
- Define service level indicators (SLIs) and service level objectives (SLOs).

**Technical Requirements -**

- Provide secure communications between the on-premises data center and cloud-hosted applications and infrastructure.
- The application must provide usage metrics and monitoring.
- APIs require authentication and authorization.
- Implement faster and more accurate validation of new features.
- Logging and performance metrics must provide actionable information to be able to provide debugging information and alerts.
- Must scale to meet user demand.

For this question, refer to the HipLocal case study.

HipLocal is expanding into new locations. They must capture additional data each time the application is launched in a new European country. This is causing delays in the development process due to constant schema changes and a lack of environments for conducting testing on the application changes. How should they resolve the issue while meeting the business requirements?

- A. Create new Cloud SQL instances in Europe and North America for testing and deployment. Provide developers with local MySQL instances to conduct testing on the application changes.
- B. Migrate data to Bigtable. Instruct the development teams to use the Cloud SDK to emulate a local Bigtable development environment.
- C. Move from Cloud SQL to MySQL hosted on Compute Engine. Replicate hosts across regions in the Americas and Europe. Provide developers with local MySQL instances to conduct testing on the application changes.
- D. Migrate data to Firestore in Native mode and set up instances in Europe and North America. Instruct the development teams to use the Cloud SDK to emulate a local Firestore in Native mode development environment.

**Correct Answer: B**

*Community vote distribution*

D (100%)

 **purushi** 8 months, 3 weeks ago

**Selected Answer: D**

Schema changes -> Firestore document database is a best fit.

upvoted 1 times

 **zellck** 1 year, 4 months ago

**Selected Answer: D**

D is the answer.

Question #190

Topic 1

You are writing from a Go application to a Cloud Spanner database. You want to optimize your application's performance using Google-recommended best practices. What should you do?

- A. Write to Cloud Spanner using Cloud Client Libraries.
- B. Write to Cloud Spanner using Google API Client Libraries
- C. Write to Cloud Spanner using a custom gRPC client library.
- D. Write to Cloud Spanner using a third-party HTTP client library.

**Correct Answer: C**

*Community vote distribution*

A (100%)

 **alpha\_canary** 2 weeks, 1 day ago

**Selected Answer: A**

<https://cloud.google.com/spanner/docs/reference/libraries#client-libraries-install-go>:~:text=Although%20you%20can%20use%20Google%20Cloud%20APIs%20directly%20by%20making%20raw%20requests%20to%20the%20server%2C%20client%20libraries%20provide%20simplifications%20that%20significantly%20reduce%20the%20amount%20of%20code%20you%20need%20to%20write

upvoted 1 times

 **JonathanSJ** 2 months, 3 weeks ago

**Selected Answer: A**

A is the answer.

upvoted 1 times

 **PatilVenkatesh** 5 months, 2 weeks ago

**Selected Answer: A**

A is correct

upvoted 1 times

 **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: A**

A is correct.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: A**

We should know what cloud client libraries are. Pl refer to <https://cloud.google.com/apis/docs/cloud-client-libraries>

upvoted 2 times

 **TNT87** 1 year, 4 months ago

Answer A

upvoted 1 times

✉️  **micoams** 1 year, 4 months ago

**Selected Answer: A**

<https://cloud.google.com/apis/docs/cloud-client-libraries>

upvoted 1 times

✉️  **sharath25** 1 year, 4 months ago

**Selected Answer: A**

option A

upvoted 1 times

✉️  **zellck** 1 year, 4 months ago

**Selected Answer: A**

A is the answer.

<https://cloud.google.com/spanner/docs/reference/libraries>

upvoted 2 times

✉️  **melisargh** 1 year, 4 months ago

**Selected Answer: A**

A is correct

BC are part of A

D idk

"Cloud Client Libraries are the recommended option for accessing Cloud APIs programmatically, where available. Cloud Client Libraries use the latest client library models"

<https://cloud.google.com/apis/docs/client-libraries-explained>

<https://cloud.google.com/go/docs/reference>

upvoted 2 times

✉️  **NewComer200** 12 months ago

<https://developers.google.com/api-client-library>

Google APIs give you programmatic access to Google Maps, Google Drive, YouTube, and many other Google products.

∴ B is wrong.

upvoted 1 times

Question #191

Topic 1

You have an application deployed in Google Kubernetes Engine (GKE). You need to update the application to make authorized requests to Google Cloud managed services. You want this to be a one-time setup, and you need to follow security best practices of auto-rotating your security keys and storing them in an encrypted store. You already created a service account with appropriate access to the Google Cloud service. What should you do next?

- A. Assign the Google Cloud service account to your GKE Pod using Workload Identity.
- B. Export the Google Cloud service account, and share it with the Pod as a Kubernetes Secret.
- C. Export the Google Cloud service account, and embed it in the source code of the application.
- D. Export the Google Cloud service account, and upload it to HashiCorp Vault to generate a dynamic service account for your application.

**Correct Answer: B**

*Community vote distribution*

A (100%)

 **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: A**

A is correct.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: A**

Service account with proper IAM configurations already exists.

We should link the existing service account with GKE pod as workload identity. This applies to all the pods running within a cluster.

upvoted 2 times

 **NewComer200** 12 months ago

**Selected Answer: A**

<https://cloud.google.com/iam/docs/best-practices-service-accounts#use-workload-identity>

upvoted 2 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: A**

workload identity

upvoted 1 times

 **TNT87** 1 year, 4 months ago

Answer A

upvoted 1 times

 **sharath25** 1 year, 4 months ago

**Selected Answer: A**

option A

upvoted 1 times

 **zellick** 1 year, 4 months ago

**Selected Answer: A**

A is the answer.

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

Applications running on GKE might need access to Google Cloud APIs such as Compute Engine API, BigQuery Storage API, or Machine Learning APIs.

Workload Identity allows a Kubernetes service account in your GKE cluster to act as an IAM service account. Pods that use the configured Kubernetes service account automatically authenticate as the IAM service account when accessing Google Cloud APIs. Using Workload Identity allows you to assign distinct, fine-grained identities and authorization for each application in your cluster.

upvoted 1 times

You are planning to deploy hundreds of microservices in your Google Kubernetes Engine (GKE) cluster. How should you secure communication between the microservices on GKE using a managed service?

- A. Use global HTTP(S) Load Balancing with managed SSL certificates to protect your services
- B. Deploy open source Istio in your GKE cluster, and enable mTLS in your Service Mesh
- C. Install cert-manager on GKE to automatically renew the SSL certificates.
- D. Install Anthos Service Mesh, and enable mTLS in your Service Mesh.

**Correct Answer: B**

*Community vote distribution*

D (87%)

13%

✉️  **JonathanSJ** 2 months, 3 weeks ago

**Selected Answer: D**

Answer is D.

upvoted 2 times

✉️  **Xoxoo** 4 months ago

**Selected Answer: D**

Istio on GKE cluster has deprecated.

upvoted 1 times

✉️  **\_rajan\_** 7 months, 1 week ago

**Selected Answer: B**

I will go with B.

upvoted 1 times

✉️  **purushi** 8 months, 3 weeks ago

**Selected Answer: D**

Initially I thought B can be the option. Later realized that directly using Istio on GKE cluster is deprecated. Hence going for D.

upvoted 1 times

✉  **mrvergara** 1 year, 3 months ago

**Selected Answer: B**

Google Cloud provides a service called Istio on GKE, that simplifies the management, scaling and automatic upgrades of Istio on GKE cluster giving you the flexibility of Istio with the ease of a managed service.

Anthos Service Mesh is a service mesh built on top of Istio, and is designed to be used in conjunction with Google Cloud's Anthos platform. It provides many of the same features as Istio, but it also includes some additional features that are specific to Anthos, such as support for hybrid and multi-cloud environments.

upvoted 1 times

✉  **TNT87** 1 year, 2 months ago

Warning: Istio on GKE is deprecated. After December 31, 2021, the UI no longer supports this feature during the creation of new clusters. After September 30, 2022, Istio on GKE will no longer be supported in existing clusters. You can migrate Istio on GKE to Anthos Service Mesh to continue using your service meshes. For more information, see the migration FAQ.

upvoted 4 times

✉  **mrvergara** 1 year, 2 months ago

Changing to the D option

upvoted 3 times

✉  **TNT87** 1 year, 3 months ago

**Selected Answer: D**

[https://cloud.google.com/architecture/service-meshes-in-microservices-architecture#security\\_2](https://cloud.google.com/architecture/service-meshes-in-microservices-architecture#security_2)

[https://cloud.google.com/architecture/service-meshes-in-microservices-architecture#security\\_2](https://cloud.google.com/architecture/service-meshes-in-microservices-architecture#security_2)

upvoted 3 times

✉  **TNT87** 1 year, 4 months ago

**Selected Answer: D**

Answer D

upvoted 2 times

✉  **sharath25** 1 year, 4 months ago

**Selected Answer: D**

option D

upvoted 1 times

Question #193

Topic 1

You are developing an application that will store and access sensitive unstructured data objects in a Cloud Storage bucket. To comply with regulatory requirements, you need to ensure that all data objects are available for at least 7 years after their initial creation. Objects created more than 3 years ago are accessed very infrequently (less than once a year). You need to configure object storage while ensuring that storage cost is optimized. What should you do? (Choose two.)

- A. Set a retention policy on the bucket with a period of 7 years.
- B. Use IAM Conditions to provide access to objects 7 years after the object creation date.
- C. Enable Object Versioning to prevent objects from being accidentally deleted for 7 years after object creation.
- D. Create an object lifecycle policy on the bucket that moves objects from Standard Storage to Archive Storage after 3 years.
- E. Implement a Cloud Function that checks the age of each object in the bucket and moves the objects older than 3 years to a second bucket with the Archive Storage class. Use Cloud Scheduler to trigger the Cloud Function on a daily schedule.

**Correct Answer: BD**

*Community vote distribution*

AD (100%)

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: AD**

AD is correct.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: AD**

Keys:

- 1) all data objects are available for at least 7 years after their initial creation : A. Set a retention policy on the bucket with a period of 7 years
- 2) Objects created more than 3 years ago are accessed very infrequently (less than once a year) : D. Create an object lifecycle policy on the bucket that moves objects from Standard Storage to Archive Storage after 3 years.

upvoted 1 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: AD**

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

upvoted 1 times

 **TNT87** 1 year, 3 months ago

**Selected Answer: AD**

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

Answer A,D

upvoted 2 times

 **x\_cath** 1 year, 4 months ago

**Selected Answer: AD**

- A is correct because Cloud Storage provides an option to configure a retention lifecycle rule.  
B is incorrect because it is not a recommended way to implement data retention requirements.  
C is incorrect because it does not guarantee that objects are not deleted within 7 years after object creation.  
D is correct because it's the easiest and recommended way to implement a storage lifecycle policy to move objects from Standard to Archive  
E is incorrect because you do not require two buckets to store objects on two storage tiers.

upvoted 1 times

 **sharath25** 1 year, 4 months ago

**Selected Answer: AD**

option AD

upvoted 1 times

 **zellick** 1 year, 4 months ago

**Selected Answer: AD**

AD is the answer.

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

This page discusses the Bucket Lock feature, which allows you to configure a data retention policy for a Cloud Storage bucket that governs how long objects in the bucket must be retained. The feature also allows you to lock the data retention policy, permanently preventing the policy from being reduced or removed.

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

Archive storage is the lowest-cost, highly durable storage service for data archiving, online backup, and disaster recovery. Unlike the "coldest" storage services offered by other Cloud providers, your data is available within milliseconds, not hours or days.

Archive storage is the best choice for data that you plan to access less than once a year.

upvoted 1 times

Question #194

Topic 1

You are developing an application using different microservices that must remain internal to the cluster. You want the ability to configure each microservice with a specific number of replicas. You also want the ability to address a specific microservice from any other microservice in a uniform way, regardless of the number of replicas the microservice scales to. You plan to implement this solution on Google Kubernetes Engine. What should you do?

- A. Deploy each microservice as a Deployment. Expose the Deployment in the cluster using a Service, and use the Service DNS name to

address it from other microservices within the cluster.

B. Deploy each microservice as a Deployment. Expose the Deployment in the cluster using an Ingress, and use the Ingress IP address to address the Deployment from other microservices within the cluster.

C. Deploy each microservice as a Pod. Expose the Pod in the cluster using a Service, and use the Service DNS name to address the microservice from other microservices within the cluster.

D. Deploy each microservice as a Pod. Expose the Pod in the cluster using an Ingress, and use the Ingress IP address to address the Pod from other microservices within the cluster.

**Correct Answer: C**

*Community vote distribution*

A (100%)

 **alpha\_canary** 2 weeks, 1 day ago

**Selected Answer: A**

"configure each microservice with a specific number of replicas"

-- Deployment

"address a specific microservice from any other microservice in a uniform way, regardless of the number of replicas the microservice scales to"

-- Service

upvoted 1 times

 **JonathanSJ** 2 months, 3 weeks ago

**Selected Answer: A**

Answer is A.

upvoted 2 times

Question #195

Topic 1

You are building an application that uses a distributed microservices architecture. You want to measure the performance and system resource utilization in one of the microservices written in Java. What should you do?

- A. Instrument the service with Cloud Profiler to measure CPU utilization and method-level execution times in the service.
- B. Instrument the service with Debugger to investigate service errors.
- C. Instrument the service with Cloud Trace to measure request latency.
- D. Instrument the service with OpenCensus to measure service latency, and write custom metrics to Cloud Monitoring.

**Correct Answer: C**

*Community vote distribution*

A (100%)

yn  
a  
. .

 **alpha\_canary** 2 weeks, 1 day ago

**Selected Answer: A**

Measure resource utilization?

-- Cloud profiler comes to mind

<https://cloud.google.com/profiler/docs/profiling-java>

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: A**

A is correct.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: A**

This is very similar to using JProfiler. A is correct.

upvoted 1 times

 **DonWang** 10 months ago

**Selected Answer: A**

A, use profiler

upvoted 1 times

 **TNT87** 1 year, 3 months ago

**Selected Answer: A**

Answer A

<https://cloud.google.com/profiler/docs/profiling-java>

<https://cloud.google.com/appengine/docs/standard/java/microservice-performance>

upvoted 4 times

 **sharath25** 1 year, 4 months ago

**Selected Answer: A**

A.

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

upvoted 1 times

 **zellck** 1 year, 4 months ago

**Selected Answer: A**

A is the answer.

<https://cloud.google.com/profiler/docs/profiling-java>

upvoted 1 times

Question #196

Topic 1

Your team is responsible for maintaining an application that aggregates news articles from many different sources. Your monitoring dashboard contains publicly accessible real-time reports and runs on a Compute Engine instance as a web application. External stakeholders and analysts need to access these reports via a secure channel without authentication. How should you configure this secure channel?

- A. Add a public IP address to the instance. Use the service account key of the instance to encrypt the traffic.
- B. Use Cloud Scheduler to trigger Cloud Build every hour to create an export from the reports. Store the reports in a public Cloud Storage bucket.
- C. Add an HTTP(S) load balancer in front of the monitoring dashboard. Configure Identity-Aware Proxy to secure the communication channel.

D. Add an HTTP(S) load balancer in front of the monitoring dashboard. Set up a Google-managed SSL certificate on the load balancer for traffic encryption.

**Correct Answer: B**

*Community vote distribution*

D (100%)

 **\_rajan\_** 6 months, 1 week ago

**Selected Answer: D**

D. Add an HTTP(S) load balancer in front of the monitoring dashboard. Set up a Google-managed SSL certificate on the load balancer for traffic encryption.

This option provides the most secure way to configure a publicly accessible channel for your monitoring dashboard without authentication. The HTTP(S) load balancer will distribute traffic to the backend instances of the dashboard, and the Google-managed SSL certificate will encrypt the traffic between the load balancer and the users.

upvoted 2 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: D**

This approach is the most secure and reliable way to configure a secure channel for external stakeholders and analysts to access the publicly accessible real-time reports in your monitoring dashboard.

upvoted 2 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: D**

SSL/TLS is must for data in transit encryption. Since without authentication, D is more suitable option. If authentication required, then we could have chosen C.

upvoted 3 times

 **TNT87** 1 year, 4 months ago

Answer D

<https://cloud.google.com/load-balancing/docs/ssl-certificates/google-managed-certs>

upvoted 1 times

 **x\_cath** 1 year, 4 months ago

**Selected Answer: D**

A is incorrect. A service account cannot be used to encrypt HTTPS traffic.

B is incorrect. Periodical export would not meet the real-time requirement.

C is incorrect. IAP is not securing the communication channel, it authenticates the user. Technically Cloud Load Balancing already secures the channel but without an appropriate certificate.

D is correct. This provides an external HTTPS endpoint, and uses Google-managed services and a valid SSL certificate.

upvoted 4 times

 **sharath25** 1 year, 4 months ago

**Selected Answer: D**

option D

upvoted 1 times

 **zellick** 1 year, 4 months ago

**Selected Answer: D**

D is the answer.

upvoted 2 times

 **melisargh** 1 year, 4 months ago

**Selected Answer: D**

D is correct. This provides an external HTTPS endpoint, and uses Google-managed services and a valid SSL certificate.

<https://cloud.google.com/load-balancing/docs/ssl-certificates/google-managed-certs>

upvoted 1 times

You are planning to add unit tests to your application. You need to be able to assert that published Pub/Sub messages are processed by your subscriber in order. You want the unit tests to be cost-effective and reliable. What should you do?

- A. Implement a mocking framework.
- B. Create a topic and subscription for each tester.
- C. Add a filter by tester to the subscription.
- D. Use the Pub/Sub emulator.

**Correct Answer: D**

*Community vote distribution*

D (75%)

B (25%)

 **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: D**

D is correct.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: D**

Option B, creating a topic and subscription for each tester, would be costly and time-consuming as it would require creating and managing a large number of topics and subscriptions. Additionally, it would not ensure that messages are processed in order, as messages may be delivered out of order to different subscriptions.

Question #198

Topic 1

You have an application deployed in Google Kubernetes Engine (GKE) that reads and processes Pub/Sub messages. Each Pod handles a fixed number of messages per minute. The rate at which messages are published to the Pub/Sub topic varies considerably throughout the day and week, including occasional large batches of messages published at a single moment.

You want to scale your GKE Deployment to be able to process messages in a timely manner. What GKE feature should you use to automatically adapt your workload?

- A. Vertical Pod Autoscaler in Auto mode
- B. Vertical Pod Autoscaler in Recommendation mode
- C. Horizontal Pod Autoscaler based on an external metric
- D. Horizontal Pod Autoscaler based on resources utilization

**Correct Answer: C**

*Community vote distribution*

C (85%)

D (15%)

 **alpha\_canary** 2 weeks ago

**Selected Answer: C**

from documentation:

"If you need to scale your workload based on the performance of an application or service outside of Kubernetes, you can configure an external metric. For example, you might need to increase the capacity of your application to ingest messages from Pub/Sub if the number of undelivered messages is trending upward."

<https://cloud.google.com/kubernetes-engine/docs/concepts/custom-and-external-metrics#external-metrics>

upvoted 1 times

 **JonathanSJ** 2 months, 3 weeks ago

**Selected Answer: C**

Answer is C

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: C**

I go with C since we need to scale GKE Deployment to be able to process messages in a TIMELY manner. External metrics is more suitable for this.

upvoted 1 times

 **Pime13** 1 year, 1 month ago

**Selected Answer: C**

C: <https://cloud.google.com/kubernetes-engine/docs/tutorials/autoscaling-metrics#pubsub>

upvoted 2 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: C**

Based on the requirement that the application reads and processes Pub/Sub messages, and that the rate at which messages are published to the Pub/Sub topic varies considerably throughout the day and week, including occasional large batches of messages published at a single moment, the best choice would be C: Horizontal Pod Autoscaler based on an external metric.

By using an external metric, the Horizontal Pod Autoscaler can monitor the number of messages in the Pub/Sub topic and adjust the number replicas in the GKE Deployment accordingly. This allows the application to automatically adapt to changes in the rate at which messages are being published, ensuring that the pods are able to process messages in a timely manner.

On the other hand, Horizontal Pod Autoscaler based on resources utilization, it would not provide the needed functionality as it bases scaling resource usage of the pods, not the number of messages in the Pub/Sub topic

upvoted 1 times

 **telp** 1 year, 3 months ago

**Selected Answer: C**

The answer is C for me.

The need to scale is from the number of messages in the pub/sub. It's an external metrics that can be reported from pub/sub or cloud monitoring. So the scale will be better to use this metrics to add X pod (each pod is limited on the number of message per minutes so the sys now how much pod you need to scale to answer at X new messages.

upvoted 1 times

 **TNT87** 1 year, 3 months ago

**Selected Answer: C**

Custom and external metrics allow workloads to adapt to conditions besides the workload itself. Consider an application that pulls tasks from queue and completes them.

An external metric is reported from an application or service not running on your cluster, but whose performance impacts your Kubernetes application. For information, the metric could be reported from Cloud Monitoring or Pub/Sub. D isn't the answer, before selecting an answer , please do a thorough research and understand concepts and the key words in a question, D cant be the answer in this case.  
<https://cloud.google.com/kubernetes-engine/docs/concepts/custom-and-external-metrics>

upvoted 4 times

 **[Removed]** 1 year, 4 months ago

The answer is C. Each pod will handle a fixed number of messages, fixed being the key word here. Now let's say this fixed number is "1000" messages per minute. Do you think a 1000 messages in a minute will cause the pod autoscaler to kick in based on resource utilisation?

We need to scale using external metrics here. When Pod 1 is handling the maximum of "fixed number amount" messages, we need to spin up pod 2 etc...

upvoted 2 times

 **sharath25** 1 year, 4 months ago

**Selected Answer: D**

option D

upvoted 1 times

 **zellick** 1 year, 4 months ago

**Selected Answer: D**

D is the answer.

<https://kubernetes.io/docs/tasks/run-application/horizontal-pod-autoscale/>

upvoted 1 times

 **TNT87** 1 year, 3 months ago

Wrong, answer C

<https://cloud.google.com/kubernetes-engine/docs/concepts/custom-and-external-metrics>, the key words are external metrics and pub/su  
read the requirements of the question

upvoted 1 times

- A. Use HTTP requests to query the available metadata server at the `http://metadata.google.internal/` endpoint with the `Metadata-Flavor: Google` header.
- B. In the Google Cloud console, navigate to the Project Dashboard and gather configuration details. Navigate to the Cloud Run "Variables & Secrets" tab, and add the desired environment variables in Key:Value format.
- C. In the Google Cloud console, navigate to the Project Dashboard and gather configuration details. Write the application configuration information to Cloud Run's in-memory container filesystem.
- D. Make an API call to the Cloud Asset Inventory API from the application and format the request to include instance metadata.

**Correct Answer:** *B*

*Community vote distribution*

A (90%)

10%

✉️  **alpha\_canary** 2 weeks ago

**Selected Answer: A**

<https://cloud.google.com/run/docs/container-contract#metadata-server>:~:text=Project%20ID%20of%20the%20project%20the%20Cloud%20Run%20service%20or%20job%20belongs%20to upvoted 1 times

✉️  **alpha\_canary** 2 weeks ago

<https://cloud.google.com/run/docs/container-contract#metadata-server>:~:text=Project%20ID%20of%20the%20project%20the%20Cloud%20Run%20service%20or%20job%20belongs%20to upvoted 1 times

✉️  **\_rajan\_** 7 months, 1 week ago

**Selected Answer: A**

A is correct.

upvoted 1 times

Question #200

Topic 1

You need to deploy resources from your laptop to Google Cloud using Terraform. Resources in your Google Cloud environment must be created using a service account. Your Cloud Identity has the roles/iam.serviceAccountTokenCreator Identity and Access Management (IAM) role and the necessary permissions to deploy the resources using Terraform. You want to set up your development environment to deploy the desired resources following Google-recommended best practices. What should you do?

- A. 1. Download the service account's key file in JSON format, and store it locally on your laptop.  
2. Set the GOOGLE\_APPLICATION\_CREDENTIALS environment variable to the path of your downloaded key file.
- B. 1. Run the following command from a command line: gcloud config set auth/impersonate\_service\_account service-account-name@project.iam.gserviceaccount.com.  
2. Set the GOOGLE\_OAUTH\_ACCESS\_TOKEN environment variable to the value that is returned by the gcloud auth print-access-token command.
- C. 1. Run the following command from a command line: gcloud auth application-default login.  
2. In the browser window that opens, authenticate using your personal credentials.
- D. 1. Store the service account's key file in JSON format in Hashicorp Vault.  
2. Integrate Terraform with Vault to retrieve the key file dynamically, and authenticate to Vault using a short-lived access token.

**Correct Answer: D**

*Community vote distribution*

B (94%)

6%

✉️  **Underverse** Highly Voted 1 year, 4 months ago

**Selected Answer: B**

A&D assume that you download and store SA keys, which violates best practices, since you potentially loose control over what happens to the credentials and makes it impossible to track who actually uses the SA. D makes it even worse since it requires you to maintain your own secret management to minimize the risk.

C does nothing that would give you the SA permissions you need.

B follows best practices, since impersonation permissions can be managed transparently via IAM and via logs you can also see who impersonated/used the SA.

upvoted 5 times

✉️  **alpha\_canary** Most Recent 2 weeks ago

**Selected Answer: B**

<https://cloud.google.com/docs/authentication/use-service-account-impersonation>  
<https://medium.com/bluetuple-ai/terraform-remote-state-on-gcp-d50e2f69b967>

upvoted 1 times

 **namanj71** 1 month, 1 week ago

B is the correct Answer

upvoted 1 times

 **\_\_rajan\_\_** 7 months, 1 week ago

**Selected Answer: B**

B is correct.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: B**

B is the best option here.

D is more complicated.

A & C do not follow google best practices.

upvoted 1 times

 **closer89** 1 year ago

**Selected Answer: B**

B

1. impersonation

2. securely set up env variable that will be used by terraform to deploy

upvoted 1 times

 **saketmurari** 1 year ago

I think its A

upvoted 1 times

 **telp** 1 year, 3 months ago

**Selected Answer: B**

Answer is B

[https://cloud.google.com/sdk/gcloud/reference/config/set#impersonate\\_service\\_account](https://cloud.google.com/sdk/gcloud/reference/config/set#impersonate_service_account)

upvoted 1 times

 **TNT87** 1 year, 3 months ago

**Selected Answer: B**

<https://cloud.google.com/blog/topics/developers-practitioners/using-google-cloud-service-account-impersonation-your-terraform-code>

Answer B not D

upvoted 4 times

 **TNT87** 1 year, 4 months ago

<https://cloud.google.com/docs/terraform/best-practices-for-terraform#default-credhttps://cloud.google.com/docs/terraform/best-practices-fc>

terrafrom#storing-secrets

Answer D.

upvoted 1 times

 **TNT87** 1 year, 3 months ago

Answer B not D

upvoted 1 times

 **micoams** 1 year, 4 months ago

**Selected Answer: B**

I think it's option B.

The question already says that you have the role for impersonating the service account.

This means that option B is a viable, as you can impersonate that service account, and get a token that has the required level of access to create resources.

upvoted 2 times

 **zellick** 1 year, 4 months ago

**Selected Answer: D**

D is the answer.

<https://cloud.google.com/iam/docs/best-practices-for-managing-service-account-keys#file-system>

Whenever possible, avoid storing service account keys on a file system. If you can't avoid storing keys on disk, make sure to restrict access to the key file, configure file access auditing, and encrypt the underlying disk.

<https://cloud.google.com/iam/docs/best-practices-for-managing-service-account-keys#software-keystore>

In situations where using a hardware-based key store isn't viable, use a software-based key store to manage service account keys. Similar to hardware-based options, a software-based key store lets users or applications use service account keys without revealing the private key. Software-based key store solutions can help you control key access in a fine-grained manner and can also ensure that each key access is logged.

upvoted 1 times

 **TNT87** 1 year, 3 months ago

Answer B not D

upvoted 1 times

Question #201

*Topic 1*

Your company uses Cloud Logging to manage large volumes of log data. You need to build a real-time log analysis architecture that pushes logs to a third-party application for processing. What should you do?

- A. Create a Cloud Logging log export to Pub/Sub.
- B. Create a Cloud Logging log export to BigQuery.
- C. Create a Cloud Logging log export to Cloud Storage.
- D. Create a Cloud Function to read Cloud Logging log entries and send them to the third-party application.

**Correct Answer: C**

*Community vote distribution*

A (71%)

B (24%)

6%

 **alpha\_canary** 2 weeks ago

**Selected Answer: A**

A: Creating a Cloud Logging log export to Pub/Sub is the correct solution for this scenario. Pub/Sub is designed for real-time messaging and push messages (in this case, log entries) to a third-party application for processing.

B: While BigQuery is great for analyzing large volumes of data, it's not designed for real-time data pushing to third-party applications.

D: Creating a Cloud Function to read log entries and send them to a third-party application could work, but it would add unnecessary complexity. Using Pub/Sub is a simpler and more efficient solution.

upvoted 1 times

 **alpha\_canary** 2 weeks ago

<https://cloud.google.com/logging/docs/export/pubsub#integrate-thru-pubsub>

upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: A**

A is correct.

upvoted 1 times

✉  **purushi** 8 months, 3 weeks ago

**Selected Answer: A**

My answer is A.

Third party service is the one responsible for analytics.

From Google cloud we just need to push the log messages to a third party application for analytics that is the part of analytics architecture.  
Real time push means, I go with Pub-sub.

upvoted 2 times

✉  **Pime13** 1 year, 1 month ago

**Selected Answer: A**

[https://cloud.google.com/logging/docs/export/configure\\_export\\_v2#overview](https://cloud.google.com/logging/docs/export/configure_export_v2#overview)

<https://cloud.google.com/logging/docs/export/pubsub>:

This document explains how you can find log entries that you routed from Cloud Logging to Pub/Sub topics, which occurs in near real-time. I recommend using Pub/Sub for integrating Cloud Logging logs with third-party software.

When you route logs to a Pub/Sub topic, Logging publishes each log entry as a Pub/Sub message as soon as Logging receives that log entry. Routed logs are generally available within seconds of their arrival to Logging, with 99% of logs available in less than 60 seconds.

upvoted 1 times

✉  **telp** 1 year, 3 months ago

**Selected Answer: A**

The processing will be done in a third-party application so we need a solution to pass logs from GCP to third party in real time and no need for analytics. So the solution is pub/sub.

Example on a case corresponding to the question by Google:

<https://cloud.google.com/architecture/exporting-stackdriver-logging-for-splunk>

upvoted 1 times

✉  **TNT87** 1 year, 3 months ago

No need for analytics??? The question says "You need to build a real-time log analysis architecture that pushes logs to a third-party application for processing" its BigQuery, it can connect to other cloud providers..<https://cloud.google.com/bigquery/docs/introduction#bigquery-analytics>

<https://cloud.google.com/blog/products/data-analytics/bigquery-performance-powers-real-time-analytics>

upvoted 1 times

✉  **mrvergara** 1 year, 2 months ago

While BigQuery can be used for log analysis, it is not well suited for real-time log processing. BigQuery is designed for batch processing large amounts of data and may not be able to provide the low latency and real-time processing capabilities required for real-time log analysis. Additionally, BigQuery may be more expensive than other options for real-time log analysis, as it charges for both storage and processing.

Therefore, for real-time log analysis, it is more appropriate to use a solution like Cloud Pub/Sub, which is specifically designed for real-time streaming of data.

My understanding is that third-party application may not be a GCP solution.

I would go for A

upvoted 1 times

✉  **TNT87** 1 year, 3 months ago

**Selected Answer: B**

Answer B

Third party transfers for BigQuery Data Transfer Service allow you to automatically schedule and manage recurring load jobs for external data sources such as Salesforce CRM, Adobe Analytics, and Facebook Ads.

<https://cloud.google.com/bigquery/docs/introduction#bigquery-analytics>

<https://cloud.google.com/blog/products/data-analytics/bigquery-performance-powers-real-time-analytics>

Pub/Sub does real-time streaming not analytics. Analytics its BigQuery and Dataflow those can do real-time analytics.

upvoted 1 times

 **x\_cath** 1 year, 4 months ago

**Selected Answer: A**

A is the only option that meets all of these requirements:

- Handles large volumes of log data
  - Sends messages (logs) to 3rd party applications in real time
- upvoted 2 times

 **TNT87** 1 year, 3 months ago

Third party transfers for BigQuery Data Transfer Service allow you to automatically schedule and manage recurring load jobs for external d sources such as Salesforce CRM, Adobe Analytics, and Facebook Ads.

to do third party transfers bigquery has this above mentioned capability

upvoted 1 times

 **TNT87** 1 year, 3 months ago

Can pub/sub analyse data?? Kindly revisit the documentation, the question says You need to build a real-time log analysis architecture, no real time streaming, pub/sub does realtime streaming not analysis, so its bigquery , i dnt know if you practically worked on gcp then you w know and understand these solutions

upvoted 1 times

 **sharath25** 1 year, 4 months ago

**Selected Answer: B**

option B

upvoted 1 times

 **jcataluna** 1 year, 4 months ago

**Selected Answer: A**

A -> real-time to a third party app . pubsub..

!C-> GCS not realtime

!B -> No third party

upvoted 4 times

 **TNT87** 1 year, 3 months ago

Third party transfers for BigQuery Data Transfer Service allow you to automatically schedule and manage recurring load jobs for external d sources such as Salesforce CRM, Adobe Analytics, and Facebook Ads.

you cant analyse data on pub/sub but you stream, so understand the difference, answer is Bigquery

upvoted 1 times

 **x\_cath** 1 year, 4 months ago

Agree with this explanation.

upvoted 1 times

 **zellick** 1 year, 4 months ago

**Selected Answer: B**

B is the answer.

upvoted 1 times

 **test010101** 1 year, 4 months ago

**Selected Answer: B**

vote B

upvoted 1 times

 **TNT87** 1 year, 4 months ago

Answer B

Bigquery performs real time analysis

upvoted 2 times

 melisargh 1 year, 4 months ago

Selected Answer: C

key is "large volume"

<https://cloud.google.com/architecture/exporting-stackdriver-logging-for-compliance-requirements>

Question #202

Topic 1

You are developing a new public-facing application that needs to retrieve specific properties in the metadata of users' objects in their respective Cloud Storage buckets. Due to privacy and data residency requirements, you must retrieve only the metadata and not the object data. You want to maximize the performance of the retrieval process. How should you retrieve the metadata?

- A. Use the patch method.
- B. Use the compose method.
- C. Use the copy method.
- D. Use the fields request parameter.

**Correct Answer: D**

*Community vote distribution*

D (100%)

✉️  **alpha\_canary** 2 weeks ago

**Selected Answer: D**

[https://cloud.google.com/storage/docs/json\\_api#partial-response](https://cloud.google.com/storage/docs/json_api#partial-response)

[https://cloud.google.com/storage/docs/json\\_api#partial-example](https://cloud.google.com/storage/docs/json_api#partial-example)

upvoted 1 times

✉️  **purushi** 8 months, 3 weeks ago

**Selected Answer: D**

The requirement here is to access only the metadata. The metadata is stored in key-value pairs and hence that should be retrieved as fields request parameter only.

upvoted 1 times

✉️  **Syed78957895** 1 year, 2 months ago

Did you guyz get all professional developer questions from here

upvoted 1 times

✉️  **Pime13** 1 year, 2 months ago

**Selected Answer: D**

[https://cloud.google.com/storage/docs/json\\_api/v1/objects/get](https://cloud.google.com/storage/docs/json_api/v1/objects/get)

alt:

Question #203

Topic 1

You are deploying a microservices application to Google Kubernetes Engine (GKE) that will broadcast livestreams. You expect unpredictable traffic patterns and large variations in the number of concurrent users. Your application must meet the following requirements:

- Scales automatically during popular events and maintains high availability
- Is resilient in the event of hardware failures

How should you configure the deployment parameters? (Choose two.)

- A. Distribute your workload evenly using a multi-zonal node pool.
- B. Distribute your workload evenly using multiple zonal node pools.
- C. Use cluster autoscaler to resize the number of nodes in the node pool, and use a Horizontal Pod Autoscaler to scale the workload.
- D. Create a managed instance group for Compute Engine with the cluster nodes. Configure autoscaling rules for the managed instance group.
- E. Create alerting policies in Cloud Monitoring based on GKE CPU and memory utilization. Ask an on-duty engineer to scale the workload by executing a script when CPU and memory usage exceed predefined thresholds.

**Correct Answer: CE**

*Community vote distribution*

AC (65%)

BC (35%)

✉️  **closer89**  1 year ago

**Selected Answer: AC**

[https://cloud.google.com/kubernetes-engine/docs/concepts/planning-scalability#choosing\\_multi-zonal\\_or\\_single-zone\\_node\\_pools](https://cloud.google.com/kubernetes-engine/docs/concepts/planning-scalability#choosing_multi-zonal_or_single-zone_node_pools)

upvoted 5 times

✉  **alpha\_canary** Most Recent 2 weeks ago

**Selected Answer: AC**

A: [https://cloud.google.com/kubernetes-engine/docs/concepts/planning-scalability#choosing\\_multi-zonal\\_or\\_single-zone\\_node\\_pools](https://cloud.google.com/kubernetes-engine/docs/concepts/planning-scalability#choosing_multi-zonal_or_single-zone_node_pools):~:text=To%20deploy%20a%20highly%20available%20application%2C%20distribute%20your%20workload%20across%20multiple%20compute%20zones%20in%20a%20region%20by%20using%20multi%2Dzonal%20node%20pools%20which%20distribute%20nodes%20uniformly%20across%20zones.

C: [https://cloud.google.com/kubernetes-engine/docs/concepts/cluster-autoscaler#how\\_cluster\\_autoscaler\\_works](https://cloud.google.com/kubernetes-engine/docs/concepts/cluster-autoscaler#how_cluster_autoscaler_works)  
<https://cloud.google.com/kubernetes-engine/docs/concepts/horizontalpodautoscaler>

upvoted 1 times

✉  **\_rajan\_** 7 months, 1 week ago

**Selected Answer: AC**

AC is correct.

upvoted 1 times

✉  **purushi** 8 months, 3 weeks ago

**Selected Answer: AC**

- 1) Is resilient in the event of hardware failures -> Is resilient in the event of hardware failures
- 2) Scales automatically during popular events and maintains high availability -> Cluster Autoscalar + Horizontal POD Autoscalar

upvoted 1 times

✉  **purushi** 8 months, 3 weeks ago

**Selected Answer: AC**

A is for resiliency.

C is for scalability

upvoted 1 times

✉  **Pime13** 1 year, 2 months ago

**Selected Answer: BC**

[https://cloud.google.com/kubernetes-engine/docs/concepts/planning-scalability#choosing\\_multi-zonal\\_or\\_single-zone\\_node\\_pools](https://cloud.google.com/kubernetes-engine/docs/concepts/planning-scalability#choosing_multi-zonal_or_single-zone_node_pools) : To deploy highly available application, distribute your workload across multiple compute zones in a region by using multi-zonal node pools which distribute nodes uniformly across zones.

upvoted 1 times

✉  **examprof** 4 months, 3 weeks ago

The paragraph you highlight above says "by using MULTI-ZONAL node pools", so why B?

A and C are correct!

upvoted 1 times

✉  **TNT87** 1 year, 3 months ago

**Selected Answer: BC**

[https://cloud.google.com/kubernetes-engine/docs/concepts/planning-scalability#choosing\\_multi-zonal\\_or\\_single-zone\\_node\\_pools](https://cloud.google.com/kubernetes-engine/docs/concepts/planning-scalability#choosing_multi-zonal_or_single-zone_node_pools)  
The answer is B not A, so its BC

upvoted 3 times

✉  **TNT87** 1 year, 4 months ago

<https://cloud.google.com/blog/products/containers-kubernetes/best-practices-for-creating-a-highly-available>

[https://cloud.google.com/kubernetes-engine/docs/concepts/types-of-clusters#multi-zonal\\_clusters](https://cloud.google.com/kubernetes-engine/docs/concepts/types-of-clusters#multi-zonal_clusters)

Answer A, C

upvoted 1 times

✉  **TNT87** 1 year, 3 months ago

To deploy a highly available application, distribute your workload across multiple compute zones in a region by using multi-zonal node pools which distribute nodes uniformly across zones.

Answer B not A

upvoted 1 times

✉  **Mark4321** 1 year, 3 months ago

A says "using multi-zonal node pools" so I think it is not in contradiction with what you copied from the document. B is not referring to multi-zonal pools at all. So I think it is A.

upvoted 2 times

✉  **TNT87** 1 year, 3 months ago

I see yes A is correct

upvoted 1 times

✉  **TNT87** 1 year, 3 months ago

B is correct not A

upvoted 1 times

✉  **TNT87** 1 year, 3 months ago

pools is the key word, multi is from multiple.... so it should be pools not pool

upvoted 1 times

✉  **wanrltw** 4 months, 2 weeks ago

Read the whole phrase, not just a single word. Option B suggests creating multiple ZONAL node pools, while A suggests a MULTIZONAL node pool.

GCP documentation recommends option A: [https://cloud.google.com/kubernetes-engine/docs/concepts/planning-scalability#choosing\\_multi-zonal\\_or\\_single-zone\\_node\\_pools](https://cloud.google.com/kubernetes-engine/docs/concepts/planning-scalability#choosing_multi-zonal_or_single-zone_node_pools)

upvoted 1 times

✉  **sharath25** 1 year, 4 months ago

**Selected Answer: AC**

option A C

upvoted 1 times

✉  **jcataluna** 1 year, 4 months ago

**Selected Answer: BC**

A multi-zonal node pool. We don't have it on GKE ;)

upvoted 2 times

✉  **angelica\_santos** 1 year, 4 months ago

I don't know if I understood it wrong, but it seems that a multizonal cluster automatically has multizonal node pools, isn't that right? Link: <https://cloud.google.com/kubernetes-engine/docs/concepts/node-pools>

upvoted 2 times

 **zellick** 1 year, 4 months ago

**Selected Answer: AC**

AC is the answer.

upvoted 1 times

 **TNT87** 1 year, 3 months ago

A is wrong, according to Best practices its "To deploy a highly available application, distribute your workload across multiple compute zones in a region by using multi-zonal node pools which distribute nodes uniformly across zones."

upvoted 1 times

 **TNT87** 1 year, 3 months ago

A is correct

upvoted 1 times

 **TNT87** 1 year, 3 months ago

Actually the answer is B,C not AC

upvoted 1 times

 **ash\_meharun** 1 year, 3 months ago

stick to one answer

upvoted 6 times

Question #204

Topic 1

You work at a rapidly growing financial technology startup. You manage the payment processing application written in Go and hosted on Cloud Run in the Singapore region (asia-southeast1). The payment processing application processes data stored in a Cloud Storage bucket that is also located in the Singapore region.

The startup plans to expand further into the Asia Pacific region. You plan to deploy the Payment Gateway in Jakarta, Hong Kong, and Taiwan over the next six months. Each location has data residency requirements that require customer data to reside in the country where the transaction was made. You want to minimize the cost of these deployments. What should you do?

- A. Create a Cloud Storage bucket in each region, and create a Cloud Run service of the payment processing application in each region.
- B. Create a Cloud Storage bucket in each region, and create three Cloud Run services of the payment processing application in the Singapore region.
- C. Create three Cloud Storage buckets in the Asia multi-region, and create three Cloud Run services of the payment processing application in the Singapore region.
- D. Create three Cloud Storage buckets in the Asia multi-region, and create three Cloud Run revisions of the payment processing application in the Singapore region.

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **alpha\_canary** 2 weeks ago

**Selected Answer: A**

Question says: "Each location has data residency requirements"  
This means must have cloud bucket in each region and the Run service in each region.  
upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: A**

A is correct  
upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: A**

I go with A not complicating the requirements.  
Cloud bucket in each of the region / multiple multi-region cloud buckets with Cloud run in each region.  
upvoted 1 times

 **hiromi** 10 months, 1 week ago

**Selected Answer: A**

A is ok  
upvoted 1 times

 **nilarndha** 1 year ago

Answer is D  
By creating three Cloud Storage buckets in the Asia multi-region (which includes Jakarta, Hong Kong, and Taiwan), the startup can ensure the customer data resides in the respective countries where the transactions are made, as required by the data residency requirements. The Cloud Run revisions of the payment processing application can be deployed in the Singapore region, which is the closest region to the Asia Pacific region with low-latency connectivity. This way, the application can process data from the Cloud Storage buckets in the Asia multi-region without incurring additional data transfer costs between regions.

upvoted 1 times

 **telp** 1 year, 3 months ago

**Selected Answer: A**

Answer is A  
upvoted 1 times

 **TNT87** 1 year, 4 months ago

Answer A  
upvoted 1 times

 **zellick** 1 year, 4 months ago

**Selected Answer: A**

A is the answer.  
upvoted 2 times

You recently joined a new team that has a Cloud Spanner database instance running in production. Your manager has asked you to optimize the Spanner instance to reduce cost while maintaining high reliability and availability of the database. What should you do?

- A. Use Cloud Logging to check for error logs, and reduce Spanner processing units by small increments until you find the minimum capacity required.
- B. Use Cloud Trace to monitor the requests per sec of incoming requests to Spanner, and reduce Spanner processing units by small increments until you find the minimum capacity required.
- C. Use Cloud Monitoring to monitor the CPU utilization, and reduce Spanner processing units by small increments until you find the minimum capacity required.
- D. Use Snapshot Debugger to check for application errors, and reduce Spanner processing units by small increments until you find the minimum capacity required.

**Correct Answer:** C

*Community vote distribution*

C (100%)

✉️  **alpha\_canary** 2 weeks ago

**Selected Answer: C**

[https://cloud.google.com/spanner/docs/compute-capacity#increasing\\_and\\_decreasing\\_compute\\_capacity](https://cloud.google.com/spanner/docs/compute-capacity#increasing_and_decreasing_compute_capacity):~:text=In%20the%20latter,in%20Cloud%20Monitoring  
upvoted 1 times

✉️  **\_rajan\_** 7 months, 1 week ago

**Selected Answer: C**

C is correct.

upvoted 1 times

✉️  **purushi** 8 months, 3 weeks ago

**Selected Answer: C**

Monitoring allows the behavior and requests per sec to Cloud spanner. By observing these parameter, we can optimize Spanner processing u in small increments until we find the minimum capacity required. After these, we can fine tune Cloud spanner parameter so that costs and resource utilization will be within the limit.

The key here is observe and improve.

upvoted 2 times

✉️  **TNT87** 1 year, 4 months ago

[https://cloud.google.com/spanner/docs/compute-capacity#increasing\\_and\\_decreasing\\_compute\\_capacity](https://cloud.google.com/spanner/docs/compute-capacity#increasing_and_decreasing_compute_capacity)

Answer C

upvoted 2 times

Question #206

Topic 1

You recently deployed a Go application on Google Kubernetes Engine (GKE). The operations team has noticed that the application's CPU usage is high even when there is low production traffic. The operations team has asked you to optimize your application's CPU resource consumption. You want to determine which Go functions consume the largest amount of CPU. What should you do?

- A. Deploy a Fluent Bit daemonset on the GKE cluster to log data in Cloud Logging. Analyze the logs to get insights into your application code's performance.
- B. Create a custom dashboard in Cloud Monitoring to evaluate the CPU performance metrics of your application.
- C. Connect to your GKE nodes using SSH. Run the top command on the shell to extract the CPU utilization of your application.
- D. Modify your Go application to capture profiling data. Analyze the CPU metrics of your application in flame graphs in Profiler.

**Correct Answer: D**

*Community vote distribution*

D (100%)

 **alpha\_canary** 2 weeks ago

**Selected Answer: D**

<https://cloud.google.com/profiler/docs/profiling-go>  
<https://cloud.google.com/profiler/docs/interacting-flame-graph>  
upvoted 1 times

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: D**

D is correct.  
upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: D**

Key here is flame graphs from the profiler. So using cloud profiler is the right choice.  
upvoted 1 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: D**

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

Cloud Profiler is a statistical, low-overhead profiler that continuously gathers CPU usage and memory-allocation information from your production applications. It attributes that information to the application's source code, helping you identify the parts of the application consuming the most resources, and otherwise illuminating the performance characteristics of the code

upvoted 2 times

 **TNT87** 1 year, 4 months ago

Answer D  
upvoted 1 times

 **sharath25** 1 year, 4 months ago

**Selected Answer: D**

option D  
upvoted 1 times

 **zellck** 1 year, 4 months ago

**Selected Answer: D**

D is the answer.

<https://cloud.google.com/profiler/docs/about-profiler>

Cloud Profiler is a statistical, low-overhead profiler that continuously gathers CPU usage and memory-allocation information from your production applications. It attributes that information to the source code that generated it, helping you identify the parts of your application that are consuming the most resources, and otherwise illuminating your application's performance characteristics.

upvoted 2 times

 **melisargh** 1 year, 4 months ago

**Selected Answer: D**

D is correct  
<https://cloud.google.com/profiler/docs>  
upvoted 1 times

Your team manages a Google Kubernetes Engine (GKE) cluster where an application is running. A different team is planning to integrate with this application. Before they start the integration, you need to ensure that the other team cannot make changes to your application, but they can deploy the integration on GKE. What should you do?

- A. Using Identity and Access Management (IAM), grant the Viewer IAM role on the cluster project to the other team.
- B. Create a new GKE cluster. Using Identity and Access Management (IAM), grant the Editor role on the cluster project to the other team.
- C. Create a new namespace in the existing cluster. Using Identity and Access Management (IAM), grant the Editor role on the cluster project to the other team.
- D. Create a new namespace in the existing cluster. Using Kubernetes role-based access control (RBAC), grant the Admin role on the new namespace to the other team.

**Correct Answer: D***Community vote distribution*

D (100%)

**✉️ 🚑 JonathanSJ** 2 months, 3 weeks ago**Selected Answer: D**

D is the answer.  
upvoted 1 times

**✉️ 🚑 Pime13** 1 year, 2 months ago**Selected Answer: D**

D: You define permissions within a Role or ClusterRole object. A Role defines access to resources within a single Namespace, while a ClusterRole defines access to resources in the entire cluster.

<https://cloud.google.com/kubernetes-engine/docs/how-to/role-based-access-control>  
upvoted 2 times

**✉️ 🚑 TNT87** 1 year, 4 months ago

<https://cloud.google.com/kubernetes-engine/docs/concepts/access-control#rbac>  
<https://cloud.google.com/kubernetes-engine/docs/how-to/role-based-access-control>  
Answer D  
upvoted 1 times

**✉️ 🚑 zellick** 1 year, 4 months ago**Selected Answer: D**

D is the answer.  
upvoted 2 times

You have recently instrumented a new application with OpenTelemetry, and you want to check the latency of your application requests in Trace. You want to ensure that a specific request is always traced. What should you do?

- A. Wait 10 minutes, then verify that Trace captures those types of requests automatically.
- B. Write a custom script that sends this type of request repeatedly from your dev project.
- C. Use the Trace API to apply custom attributes to the trace.
- D. Add the X-Cloud-Trace-Context header to the request with the appropriate parameters.

**Correct Answer: D**

*Community vote distribution*

D (100%)

 rajan\_ 7 months, 1 week ago

**Selected Answer: D**

D is correct.

upvoted 1 times

 purushi 8 months, 3 weeks ago

**Selected Answer: D**

To identify specific request is from setting the request header with specific key value pairs.

Key is X-Cloud-Trace-Context, Value is True.

upvoted 1 times

 Oleksii\_ki 9 months, 4 weeks ago

**Selected Answer: D**

According to the Professional Google Cloud Developer documentation, to ensure that a specific request is always traced, the X-Cloud-Trace-Context header must be added to the request with the appropriate parameters. This header ensures that all requests made to the application are traced and added to the Trace list. Additionally, the documentation explains that the Trace ID and Span ID must be included in the header to ensure that the request is correctly attributed to the trace. By using this method, developers can easily monitor and analyze the latency and performance of their applications using Trace.

upvoted 1 times

 TNT87 1 year, 4 months ago

**Selected Answer: D**

To force a specific request to be traced, add an X-Cloud-Trace-Context header to the request.

upvoted 1 times

 zelick 1 year, 4 months ago

**Selected Answer: D**

D is the answer.

<https://cloud.google.com/trace/docs/setup#force-trace>

Cloud Trace doesn't sample every request.

To force a specific request to be traced, add an X-Cloud-Trace-Context header to the request.

upvoted 2 times

You are trying to connect to your Google Kubernetes Engine (GKE) cluster using kubectl from Cloud Shell. You have deployed your GKE cluster with a public endpoint. From Cloud Shell, you run the following command:

```
gcloud container clusters get-credentials <cluster-name> \
--zone <zone> --project <project-name> \
```

You notice that the kubectl commands time out without returning an error message. What is the most likely cause of this issue?

- A. Your user account does not have privileges to interact with the cluster using kubectl.
- B. Your Cloud Shell external IP address is not part of the authorized networks of the cluster.
- C. The Cloud Shell is not part of the same VPC as the GKE cluster.
- D. A VPC firewall is blocking access to the cluster's endpoint.

**Correct Answer:** D

*Community vote distribution*

B (83%)

D (17%)

✉️  **alpha\_canary** 2 weeks ago

**Selected Answer: B**

<https://cloud.google.com/kubernetes-engine/docs/troubleshooting#kubectl-times-out>

"If the cluster is a private GKE cluster, then ensure that the outgoing IP of the machine you are attempting to connect from is included in the list of existing authorized networks."

upvoted 1 times

✉️  **\_rajan\_** 7 months, 1 week ago

**Selected Answer: B**

B is correct.

upvoted 1 times

✉️  **purushi** 8 months, 3 weeks ago

**Selected Answer: B**

Cloud shells public IP is not present in the authorized networks/IP list of the GKE cluster.

upvoted 1 times

✉️  **mrvergara** 1 year, 3 months ago

**Selected Answer: D**

Where is the info that this is a private cluster?

Question #210

Topic 1

You are developing a web application that contains private images and videos stored in a Cloud Storage bucket. Your users are anonymous and do not have Google Accounts. You want to use your application-specific logic to control access to the images and videos. How should you configure access?

- A. Cache each web application user's IP address to create a named IP table using Google Cloud Armor. Create a Google Cloud Armor security policy that allows users to access the backend bucket.
- B. Grant the Storage Object Viewer IAM role to allUsers. Allow users to access the bucket after authenticating through your web application.
- C. Configure Identity-Aware Proxy (IAP) to authenticate users into the web application. Allow users to access the bucket after authenticating through IAP.
- D. Generate a signed URL that grants read access to the bucket. Allow users to access the URL after authenticating through your web application.

**Correct Answer: D**

*Community vote distribution*

D (100%)

 **\_rajan\_** 7 months, 1 week ago

**Selected Answer: D**

D is correct.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: D**

The key here is "application-specific logic to control access to the images and videos". Signed Url with Read only permission with limited acc time is the right choice.

upvoted 1 times

 **hiromi** 10 months, 1 week ago

**Selected Answer: D**

D is ok

<https://cloud.google.com/storage/docs/access-control/signed-urls#should-you-use>

upvoted 1 times

 **zellck** 1 year, 4 months ago

**Selected Answer: D**

D is the answer.

<https://cloud.google.com/storage/docs/access-control/signed-urls#should-you-use>

In some scenarios, you might not want to require your users to have a Google account in order to access Cloud Storage, but you still want to control access using your application-specific logic. The typical way to address this use case is to provide a signed URL to a user, which give the user read, write, or delete access to that resource for a limited time. You specify an expiration time when you create the signed URL. Anyon who knows the URL can access the resource until the expiration time for the URL is reached or the key used to sign the URL is rotated.

upvoted 2 times

 **TNT87** 1 year, 4 months ago

**Selected Answer: D**

<https://cloud.google.com/storage/docs/access-control/signed-urls#should-you-use>

upvoted 3 times

Question #211

Topic 1

You need to configure a Deployment on Google Kubernetes Engine (GKE). You want to include a check that verifies that the containers can connect to the database. If the Pod is failing to connect, you want a script on the container to run to complete a graceful shutdown. How should you configure the Deployment?

- A. Create two jobs: one that checks whether the container can connect to the database, and another that runs the shutdown script if the Pod is failing.
- B. Create the Deployment with a livenessProbe for the container that will fail if the container can't connect to the database. Configure a Prestop lifecycle handler that runs the shutdown script if the container is failing.
- C. Create the Deployment with a PostStart lifecycle handler that checks the service availability. Configure a PreStop lifecycle handler that runs the shutdown script if the container is failing.
- D. Create the Deployment with an initContainer that checks the service availability. Configure a Prestop lifecycle handler that runs the shutdown script if the Pod is failing.

**Correct Answer: C**

*Community vote distribution*

B (86%)

14%

 **TNT87**  1 year, 4 months ago

**Selected Answer: B**

[https://cloud.google.com/architecture/best-practices-for-running-cost-effective-kubernetes-applications-on-gke#make\\_sure\\_your\\_applications\\_are\\_shutting\\_down\\_in\\_accordance\\_with\\_kubernetes\\_expectations](https://cloud.google.com/architecture/best-practices-for-running-cost-effective-kubernetes-applications-on-gke#make_sure_your_applications_are_shutting_down_in_accordance_with_kubernetes_expectations)

upvoted 6 times

 **alpha\_canary**  2 weeks ago

**Selected Answer: B**

"Most programs don't stop accepting requests right away. However, if you're using third-party code or are managing a system that you don't have control over, such as nginx, the preStop hook is a good option for triggering a graceful shutdown without modifying the application. One common strategy is to execute, in the preStop hook, a sleep of a few seconds to postpone the SIGTERM. This gives Kubernetes extra time to finish the Pod deletion process, and reduces connection errors on the client side."

<https://cloud.google.com/architecture/best-practices-for-running-cost-effective-kubernetes-applications-on-gke#:~:text=If%20your%20application%20doesn%27t%20follow%20the%20preceding%20practice%2C%20use%20the%20preStop%20hook>

<https://kubernetes.io/docs/concepts/containers/container-lifecycle-hooks/#container-hooks>

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: B**

I go with B, that is liveness probe and if failed for max retries then call prestop hook to gracefully shutdown the container. D is also very close, it used init container to check for the database connectivity first. I am not sure whether we can prestop hook if initContainer fails to starts.

upvoted 1 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: B**

[https://cloud.google.com/architecture/best-practices-for-running-cost-effective-kubernetes-applications-on-gke#make\\_sure\\_your\\_applications\\_are\\_shutting\\_down\\_in\\_accordance\\_with\\_kubernetes\\_expectations](https://cloud.google.com/architecture/best-practices-for-running-cost-effective-kubernetes-applications-on-gke#make_sure_your_applications_are_shutting_down_in_accordance_with_kubernetes_expectations) -> the preStop hook is a good option for triggering a graceful shutdown without modifying the application.

<https://kubernetes.io/docs/concepts/containers/container-lifecycle-hooks/#hook-details> ->

This hook is called immediately before a container is terminated due to an API request or management event such as a liveness/startup probe failure, preemption, resource contention and others. A call to the PreStop hook fails if the container is already in a terminated or completed state and the hook must complete before the TERM signal to stop the container can be sent. The Pod's termination grace period countdown begins before the PreStop hook is executed, so regardless of the outcome of the handler, the container will eventually terminate within the Pod's termination grace period. No parameters are passed to the handler.

upvoted 1 times

 **telp** 1 year, 3 months ago

**Selected Answer: B**

Answer B

upvoted 1 times

 **zellick** 1 year, 4 months ago

**Selected Answer: B**

B is the answer.

upvoted 2 times

 **kisswd** 1 year, 4 months ago

**Selected Answer: D**

D could be the right answer  
upvoted 2 times

 **[Removed]** 1 year, 4 months ago

The answer is definitely D. Anytime you need to do some work before a container can be considered ready, you use init containers. With a liveness probe we would need to add an endpoint that checks whether we can connect to the database, with init containers we can separate this logic.

Question #212

Topic 1

You are responsible for deploying a new API. That API will have three different URL paths:

- <https://yourcompany.com/students>
- <https://yourcompany.com/teachers>
- <https://yourcompany.com/classes>

You need to configure each API URL path to invoke a different function in your code. What should you do?

- A. Create one Cloud Function as a backend service exposed using an HTTPS load balancer.
- B. Create three Cloud Functions exposed directly.
- C. Create one Cloud Function exposed directly.
- D. Create three Cloud Functions as three backend services exposed using an HTTPS load balancer.

**Correct Answer: D**

*Community vote distribution*

D (53%)

B (47%)

 **phantomsg** 1 month, 1 week ago

**Selected Answer: B**

There's no purpose for a Load Balancer here as you are not balancing traffic across multiple backend server instances. You need 3 different Cloud Functions each with their own Endpoint that's all. See this example: <https://cloud.google.com/functions/docs/create-deploy-gcloud-1st-gen>

upvoted 1 times

 **ka219ra** 2 months ago

**Selected Answer: D**

option D.

When users query "yourcompany.com," they receive an IP address and access the load balancer. Consequently, the load balancer then executes path-based routing.

B is Wrong. It is not possible to deploy three cloud functions with the same domain name.

upvoted 2 times

 **Kadhem** 4 months ago

**Selected Answer: B**

i go for B because i don't understand the necessity of LB in this case

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: B**

I go with B. Exposed using an HTTPS load balancer is not required. Those three are different end points of the service. We no need to setup load balancer in case of Cloud functions, it is serverless.

upvoted 1 times

zanhsieh 10 months, 3 weeks ago

Selected Answer: D

D. The differences between B and D are:

1. Cost: 3 Cloud Function exposed directly (B) will create 3 endpoints / load balancers, whereas D only exposed one load balancer.
2. Scalability: exposing directly with endpoint or instance itself would cause scalability problem - can't upscale the endpoint instance fast enough.
3. Handling service-to-service call: In B, all services rely on external DNS resolution, which is slower. In D, it has chance that cross-service call can be resolved internally.

upvoted 2 times

Teraflow 1 year ago

Selected Answer: B

Option B (Create three Cloud Functions exposed directly) is the best choice in this scenario, as it allows you to create a separate Cloud Function for each API URL path and configure each one to invoke a different function in your code.

Option A (Create one Cloud Function as a backend service exposed using an HTTPS load balancer) and Option D (Create three Cloud Functions as three backend services exposed using an HTTPS load balancer) both involve using an HTTPS load balancer, which adds additional complexity and configuration overhead. These options may be appropriate for more complex scenarios, but in this case, they are not necessary.

Option C (Create one Cloud Function exposed directly) would require all three API URL paths to invoke the same function in your code, which does not meet the requirement of invoking different functions for each URL path.

upvoted 1 times

closer89 1 year ago

B is wrong, in API context you need to map each external url to cloud function url, to do that you need LB

upvoted 1 times

Pime13 1 year, 2 months ago

Selected Answer: D

i choose D

upvoted 1 times

Pime13 1 year, 1 month ago

<https://cloud.google.com/load-balancing/docs/https/setting-up-https-serverless>  
<https://cloud.google.com/load-balancing/docs/serverless-neg-concepts>

upvoted 1 times

mrvergara 1 year, 2 months ago

Selected Answer: B

Each function is defined as an HTTP trigger, which allows it to be triggered by incoming HTTP requests. The endpoint for each function is defined in the function name (e.g. "students", "teachers", "classes").

This means that the APIs would be accessible at the following endpoints:

- <https://yourcompany.com/students>
- <https://yourcompany.com/teachers>
- <https://yourcompany.com/classes>

Note that you would need to configure "yourcompany.com" DNS registry.

In this case, option B, "Create three Cloud Functions exposed directly", would be correct.

upvoted 3 times

mrvergara 1 year, 2 months ago

Using option D, where you create three Cloud Functions as backend services exposed through an HTTPS load balancer, is not necessary in this scenario. An HTTPS load balancer would be useful in scenarios where you need to balance incoming traffic across multiple instances of the backend service to distribute the workload, ensure high availability, and provide failover protection. However, in this case, you only need to map each API URL path to a different function, which can be achieved by creating three separate Cloud Functions, each exposed directly. This would be a simpler and more straightforward solution for this specific use case.

upvoted 1 times

mrvergara 1 year, 3 months ago

Why there is the need of LB?

upvoted 1 times

✉️  **sharath25** 1 year, 4 months ago

**Selected Answer: D**

option D

upvoted 1 times

✉️  **zellck** 1 year, 4 months ago

**Selected Answer: D**

D is the answer.

upvoted 1 times

✉️  **zellck** 1 year, 4 months ago

<https://cloud.google.com/load-balancing/docs/https/setup-global-ext-https-serverless>

upvoted 2 times

✉️  **melisargh** 1 year, 4 months ago

**Selected Answer: D**

D is correct

upvoted 1 times

Question #213

Topic 1

You are deploying a microservices application to Google Kubernetes Engine (GKE). The application will receive daily updates. You expect to deploy a large number of distinct containers that will run on the Linux operating system (OS). You want to be alerted to any known OS vulnerabilities in the new containers. You want to follow Google-recommended best practices. What should you do?

- A. Use the gcloud CLI to call Container Analysis to scan new container images. Review the vulnerability results before each deployment.
- B. Enable Container Analysis, and upload new container images to Artifact Registry. Review the vulnerability results before each deployment.
- C. Enable Container Analysis, and upload new container images to Artifact Registry. Review the critical vulnerability results before each deployment.
- D. Use the Container Analysis REST API to call Container Analysis to scan new container images. Review the vulnerability results before each deployment.

**Correct Answer: D**

*Community vote distribution*

B (90%)

10%

✉️  **zanhsieh** 10 months, 1 week ago

**Selected Answer: B**

B. Actually the tricky part for this question is: Is the Container Analysis enabled by default? Can Container Analysis be called on-demand via REST without specifically enabling it? By default GCP does not enable Container Analysis; that's why D is out.

upvoted 2 times

✉️  **Pime13** 1 year, 2 months ago

**Selected Answer: B**

<https://cloud.google.com/artifact-registry/docs/analysis>

Vulnerability scanning can occur automatically or on-demand:

When automatic scanning is enabled, scanning triggers automatically every time you push a new image to Artifact Registry or Container Registry. Vulnerability information is continuously updated when new vulnerabilities are discovered.

When On-Demand Scanning is enabled, you must run a command to scan a local image or an image in Artifact Registry or Container Registry. On-Demand Scanning gives you more flexibility around when you scan containers. For example, you can scan a locally-built image and remediate vulnerabilities before storing it in a registry.

Scanning results are available for up to 48 hours after the scan is completed, and vulnerability information is not updated after the scan.  
upvoted 1 times

⊕  **TNT87** 1 year, 3 months ago

<https://cloud.google.com/blog/products/application-development/understanding-artifact-registry-vs-container-registry>  
upvoted 1 times

⊕  **TNT87** 1 year, 4 months ago

**Selected Answer: B**

Container Analysis is a service that provides vulnerability scanning and metadata storage for containers. The scanning service performs vulnerability scans on images in Container Registry and Artifact Registry, then stores the resulting metadata and makes it available for consumption through an API. Metadata storage allows storing information from different sources, including vulnerability scanning, other Google Cloud services, and third-party providers.

<https://cloud.google.com/container-analysis/docs/container-analysis>

upvoted 1 times

⊕  **sharath25** 1 year, 4 months ago

**Selected Answer: B**

option B

upvoted 1 times

⊕  **zellick** 1 year, 4 months ago

**Selected Answer: B**

B is the answer.

<https://cloud.google.com/container-analysis/docs/automated-scanning-howto>

upvoted 1 times

⊕  **TNT87** 1 year, 4 months ago

Answer B

If you have done Devops you will understand

upvoted 1 times

⊕  **TNT87** 1 year, 4 months ago

**Selected Answer: B**

Answer B

upvoted 1 times

⊕  **kisswd** 1 year, 4 months ago

**Selected Answer: B**

"Container Analysis REST API" doesn't exist.

<https://cloud.google.com/container-analysis/docs/os-overview> says:

The Container Scanning API allows you to automate OS vulnerability detection, scanning each time you push an image to Container Registry Artifact Registry. Enabling this API also triggers language package scans for Go and Java vulnerabilities (Preview).

upvoted 1 times

⊕  **kisswd** 1 year, 4 months ago

After reviewing the document again, I changed my answer to D.

upvoted 2 times

⊕  **TNT87** 1 year, 4 months ago

It can't be D, that's not how the Container analysis API works

upvoted 1 times

⊕  **TNT87** 1 year, 4 months ago

Do not confuse yourself, there is Container analysis API, it exists. check what the question requires, ok

<https://cloud.google.com/container-analysis/docs/reference/rest>

upvoted 1 times

⊕  **ladannylondo** 1 year, 4 months ago

**Selected Answer: B**

<https://cloud.google.com/container-analysis/docs/enable-container-scanning>

upvoted 1 times

✉️  **melisargh** 1 year, 4 months ago

**Selected Answer: D**

<https://cloud.google.com/container-analysis/docs/os-overview>

upvoted 1 times

✉️  **gardisan18** 1 year, 4 months ago

Answer is B

<https://cloud.google.com/container-analysis/docs/automated-scanning-howto>

upvoted 2 times

✉️  **melisargh** 1 year, 4 months ago

after re review i think B is correct too but im still not sure

upvoted 1 times

Question #214

Topic 1

You are a developer at a large organization. You have an application written in Go running in a production Google Kubernetes Engine (GKE) cluster. You need to add a new feature that requires access to BigQuery. You want to grant BigQuery access to your GKE cluster following Google-recommended best practices. What should you do?

- A. Create a Google service account with BigQuery access. Add the JSON key to Secret Manager, and use the Go client library to access the JSON key.
- B. Create a Google service account with BigQuery access. Add the Google service account JSON key as a Kubernetes secret, and configure the application to use this secret.
- C. Create a Google service account with BigQuery access. Add the Google service account JSON key to Secret Manager, and use an init container to access the secret for the application to use.
- D. Create a Google service account and a Kubernetes service account. Configure Workload Identity on the GKE cluster, and reference the Kubernetes service account on the application Deployment.

**Correct Answer: D**

*Community vote distribution*

D (88%)

13%

✉️  **alpha\_canary** 2 weeks ago

**Selected Answer: D**

"Applications running on GKE might need access to Google Cloud APIs such as Compute Engine API, BigQuery Storage API, or Machine Learning APIs."

[https://cloud.google.com/kubernetes-engine/docs/concepts/workload-identity#what\\_is](https://cloud.google.com/kubernetes-engine/docs/concepts/workload-identity#what_is)

upvoted 1 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: D**

Workload Identity allows a Kubernetes service account in your GKE cluster to act as an IAM service account. Pods that use the configured Kubernetes service account automatically authenticate as the IAM service account when accessing Google Cloud APIs. Using Workload Identity allows you to assign distinct, fine-grained identities and authorization for each application in your cluster.

[https://cloud.google.com/kubernetes-engine/docs/concepts/workload-identity#what\\_is](https://cloud.google.com/kubernetes-engine/docs/concepts/workload-identity#what_is)

upvoted 1 times

 **telp** 1 year, 3 months ago

**Selected Answer: D**

The answer is D because the best practice is to use workload identity

[https://cloud.google.com/kubernetes-engine/docs/concepts/workload-identity#what\\_is](https://cloud.google.com/kubernetes-engine/docs/concepts/workload-identity#what_is)

upvoted 1 times

 **TNT87** 1 year, 3 months ago

[https://cloud.google.com/kubernetes-engine/docs/quickstarts/deploy-app-container-image#deploying\\_to\\_gke](https://cloud.google.com/kubernetes-engine/docs/quickstarts/deploy-app-container-image#deploying_to_gke)

upvoted 1 times

 **TNT87** 1 year, 4 months ago

**Selected Answer: D**

[https://cloud.google.com/kubernetes-engine/docs/concepts/workload-identity#what\\_is](https://cloud.google.com/kubernetes-engine/docs/concepts/workload-identity#what_is)

Answer D

upvoted 1 times

 **sharath25** 1 year, 4 months ago

**Selected Answer: D**

option D

upvoted 1 times

 **jcataluna** 1 year, 4 months ago

**Selected Answer: D**

a go???? no!! D is correct

upvoted 1 times

 **zellck** 1 year, 4 months ago

**Selected Answer: D**

D is the answer.

[https://cloud.google.com/kubernetes-engine/docs/concepts/workload-identity#what\\_is](https://cloud.google.com/kubernetes-engine/docs/concepts/workload-identity#what_is)

Applications running on GKE might need access to Google Cloud APIs such as Compute Engine API, BigQuery Storage API, or Machine Learning APIs.

Workload Identity allows a Kubernetes service account in your GKE cluster to act as an IAM service account. Pods that use the configured Kubernetes service account automatically authenticate as the IAM service account when accessing Google Cloud APIs. Using Workload Identity allows you to assign distinct, fine-grained identities and authorization for each application in your cluster.

upvoted 1 times

 **melisargh** 1 year, 4 months ago

**Selected Answer: A**

vote A because the type of auth supported by bq and the recommended way of auth which is use go libraries

<https://cloud.google.com/bigquery/docs/authorization>

[https://pkg.go.dev/golang.org/x/oauth2/google?utm\\_source=cloud.google.com&utm\\_medium=referral#JWTAccessTokenSourceFromJSON](https://pkg.go.dev/golang.org/x/oauth2/google?utm_source=cloud.google.com&utm_medium=referral#JWTAccessTokenSourceFromJSON)

upvoted 1 times

Question #215

Topic 1

You have an application written in Python running in production on Cloud Run. Your application needs to read/write data stored in a Cloud Storage bucket in the same project. You want to grant access to your application following the principle of least privilege. What should you do?

- A. Create a user-managed service account with a custom Identity and Access Management (IAM) role.
- B. Create a user-managed service account with the Storage Admin Identity and Access Management (IAM) role.

C. Create a user-managed service account with the Project Editor Identity and Access Management (IAM) role.

D. Use the default service account linked to the Cloud Run revision in production.

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **alpha\_canary** 2 weeks ago

**Selected Answer: A**

A. Create a user-managed service account with a custom Identity and Access Management (IAM) role.

upvoted 1 times

 **\_\_rajan\_\_** 7 months ago

**Selected Answer: A**

A is correct.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: A**

principle of least privilege -> custom Identity and Access Management (IAM) role

upvoted 1 times

 **telp** 1 year, 3 months ago

**Selected Answer: A**

Answer is A

The others give too many access

upvoted 2 times

 **zelick** 1 year, 4 months ago

**Selected Answer: A**

A is the answer.

upvoted 2 times

 **TNT87** 1 year, 4 months ago

Answer A

upvoted 1 times

 **gardislan18** 1 year, 4 months ago

**Selected Answer: A**

A - assign the needed permissions, following the least privilege rule

Not B - <https://cloud.google.com/iam/docs/understanding-roles#storage.admin>

C and D gives too many access

upvoted 1 times

Your team is developing unit tests for Cloud Function code. The code is stored in a Cloud Source Repositories repository. You are responsible for implementing the tests. Only a specific service account has the necessary permissions to deploy the code to Cloud Functions. You want to ensure that the code cannot be deployed without first passing the tests. How should you configure the unit testing process?

- A. Configure Cloud Build to deploy the Cloud Function. If the code passes the tests, a deployment approval is sent to you.
- B. Configure Cloud Build to deploy the Cloud Function, using the specific service account as the build agent. Run the unit tests after successful deployment.
- C. Configure Cloud Build to run the unit tests. If the code passes the tests, the developer deploys the Cloud Function.
- D. Configure Cloud Build to run the unit tests, using the specific service account as the build agent. If the code passes the tests, Cloud Build deploys the Cloud Function.

**Correct Answer:** B

*Community vote distribution*

D (90%)

10%

 **\_\_rajan\_\_** 7 months ago

**Selected Answer: D**

D is correct.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: D**

Correct answer is D. First run unit tests and if all pass then deploy as Cloud Func.

upvoted 1 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: D**

i made a midtake, it's d

upvoted 1 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: B**

b) first run test and then deploy

upvoted 1 times

 **Pime13** 1 year, 2 months ago

typo, D

upvoted 1 times

Question #217

Topic 1

Your team detected a spike of errors in an application running on Cloud Run in your production project. The application is configured to read messages from Pub/Sub topic A, process the messages, and write the messages to topic B. You want to conduct tests to identify the cause of the errors. You can use a set of mock messages for testing. What should you do?

- A. Deploy the Pub/Sub and Cloud Run emulators on your local machine. Deploy the application locally, and change the logging level in the application to DEBUG or INFO. Write mock messages to topic A, and then analyze the logs.
- B. Use the gcloud CLI to write mock messages to topic A. Change the logging level in the application to DEBUG or INFO, and then analyze the logs.
- C. Deploy the Pub/Sub emulator on your local machine. Point the production application to your local Pub/Sub topics. Write mock messages to topic A, and then analyze the logs.
- D. Use the Google Cloud console to write mock messages to topic A. Change the logging level in the application to DEBUG or INFO, and then analyze the logs.

**Correct Answer: C**

*Community vote distribution*

A (90%)

10%

 **\_rajan\_** 7 months ago

**Selected Answer: A**

A is correct.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: A**

A is right. Pub-Sub and cloud run emulator to run under local env with mock msgs publish to a topic, INFO and DEBUG logs enabled to see detailed log info.

upvoted 1 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: A**

I choose A. C is against all practices.

upvoted 1 times

 **zellck** 1 year, 4 months ago

**Selected Answer: A**

A is the answer.

upvoted 1 times

 **melisargh** 1 year, 4 months ago

**Selected Answer: A**

going with A because it mentions the 2 points of possible failure and gives you a full scenario to analyse

upvoted 2 times

 **kisswd** 1 year, 4 months ago

**Selected Answer: A**

Run all locally

upvoted 3 times

 **TNT87** 1 year, 4 months ago

**Selected Answer: C**

<https://cloud.google.com/pubsub/docs/emulator>

upvoted 1 times

 **ladannylondo** 1 year, 4 months ago

i think that is better the option A, because can you run all locally and check the logs.

upvoted 4 times

 **swifty512** 1 year, 4 months ago

If production is pointing to your local emulator...your users are in trouble lol...Answer is A

upvoted 2 times

 **TNT87** 1 year, 3 months ago

You want to conduct tests to identify the cause of the errors...this is the core of the question.....

upvoted 1 times

 **TNT87** 1 year, 3 months ago

when emulating you are testing, you have to test, i think you need to read the document first then you will understand what pub/sub emulation is and how it is done. yeah the answer might not be correct because it doesn't include cloud run emulation.... you run all local to test then you can deploy to production

Question #218

Topic 1

You are developing a Java Web Server that needs to interact with Google Cloud services via the Google Cloud API on the user's behalf. Users should be able to authenticate to the Google Cloud API using their Google Cloud identities. Which workflow should you implement in your web application?

- A. 1. When a user arrives at your application, prompt them for their Google username and password.
2. Store an SHA password hash in your application's database along with the user's username.
3. The application authenticates to the Google Cloud API using HTTPS requests with the user's username and password hash in the

Authorization request header.

- B. 1. When a user arrives at your application, prompt them for their Google username and password.
  - 2. Forward the user's username and password in an HTTPS request to the Google Cloud authorization server, and request an access token.
  - 3. The Google server validates the user's credentials and returns an access token to the application.
  - 4. The application uses the access token to call the Google Cloud API.
- C. 1. When a user arrives at your application, route them to a Google Cloud consent screen with a list of requested permissions that prompts the user to sign in with SSO to their Google Account.
  - 2. After the user signs in and provides consent, your application receives an authorization code from a Google server.
  - 3. The Google server returns the authorization code to the user, which is stored in the browser's cookies.
  - 4. The user authenticates to the Google Cloud API using the authorization code in the cookie.
- D. 1. When a user arrives at your application, route them to a Google Cloud consent screen with a list of requested permissions that prompts the user to sign in with SSO to their Google Account.
  - 2. After the user signs in and provides consent, your application receives an authorization code from a Google server.
  - 3. The application requests a Google Server to exchange the authorization code with an access token.
  - 4. The Google server responds with the access token that is used by the application to call the Google Cloud API.

**Correct Answer: C**

*Community vote distribution*

D (100%)

 **\_rajan\_** 7 months ago

**Selected Answer: D**

D is correct.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: D**

D is right. OAuth 2.0 authorization code grant flow is the technique to use Google APIs to access resources servers.

upvoted 1 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: D**

<https://developers.google.com/identity/protocols/oauth2>

upvoted 1 times

 **telp** 1 year, 3 months ago

**Selected Answer: D**

D is the answer

You need to use OAuth of google so A and B are eliminated.

Question #219

Topic 1

You recently developed a new application. You want to deploy the application on Cloud Run without a Dockerfile. Your organization requires that all container images are pushed to a centrally managed container repository. How should you build your container using Google Cloud services? (Choose two.)

- A. Push your source code to Artifact Registry.
- B. Submit a Cloud Build job to push the image.
- C. Use the pack build command with pack CLI.
- D. Include the --source flag with the gcloud run deploy CLI command.
- E. Include the --platform=kubernetes flag with the gcloud run deploy CLI command.

**Correct Answer: CE**

*Community vote distribution*

CD (63%)

AB (19%)

Other

 **wanrltw** 4 months, 2 weeks ago

**Selected Answer: CD**

C: "For example, use buildpacks to build the source code of your Cloud Run service into a container image." - <https://cloud.google.com/docs/buildpacks/build-application>

Also, <https://cloud.google.com/blog/products/containers-kubernetes/google-cloud-now-supports-buildpacks>

D: "If no Dockerfile is present in the source code directory, Google Cloud's buildpacks automatically detects the language you are using and fetches the dependencies of the code to make a production-ready container image, using a secure base image managed by Google." - <https://cloud.google.com/run/docs/deploying-source-code>

upvoted 2 times

 **wanrltw** 4 months, 2 weeks ago

Not A, as it's redundant when using the option D: "You can also deploy directly from source to Cloud Run, which includes automatically creating a container image for your built source and storing the image in Artifact Registry." - <https://cloud.google.com/artifact-registry/docs/integrate-cloud-run>

B & E are irrelevant.

upvoted 1 times

 **82e0b6209c** 4 months, 3 weeks ago

**Selected Answer: BC**

The actual question is "How should you build your container using Google Cloud services?", so it doesn't mention how to deploy it.

Also, if we exclude B, how is the image build in C ending up at the central container repository?

upvoted 1 times

 **purushti** 8 months, 3 weeks ago

**Selected Answer: CD**

C is packeto build pack to create an image. This is a very efficient way of creating images explicitly.

D is through gcloud run command. Not sure what framework cloud build uses to create an image.

upvoted 1 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: CD**

i choose cd

upvoted 1 times

 **mrvergara** 1 year, 2 months ago

**Selected Answer: CD**

pack build [IMAGE-NAME] --builder [BUILDER-IMAGE] --path [APPLICATION-DIRECTORY]

gcloud run deploy [SERVICE-NAME] --image [IMAGE-NAME] --source [APPLICATION-DIRECTORY]

upvoted 1 times

 **mrvergara** 1 year, 2 months ago

**Selected Answer: CD**

<https://cloud.google.com/run/docs/deploying-source-code>

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: AB**

A and B are the correct options because they both involve using Cloud Build to build the container image.

Option A, Push your source code to Artifact Registry, allows you to store the source code of your application in a central location, making it easier to manage and version control.

Option B, Submit a Cloud Build job to push the image, allows you to use Cloud Build to build the container image, which is a recommended method for building container images in a production environment. It allows you to automate the build process, test the image, and push it to container registry.

upvoted 3 times

 **omermahgoub** 1 year, 3 months ago

Option C, Use the pack build command with pack CLI, is not correct because Cloud Run does not support the use of the pack CLI.

Option D, Include the --source flag with the gcloud run deploy CLI command, is not correct because this flag is used to specify the source code location when deploying the application, not building the container.

Option E, Include the --platform=kubernetes flag with the gcloud run deploy CLI command, is not correct because this flag is used to specify the platform when deploying the application on Kubernetes and not Cloud Run.

upvoted 3 times

 **telp** 1 year, 3 months ago

**Selected Answer: CD**

The Cloud run use the buildpacks to automatically build container images from source code but you need to use source code flag so you need to add the --source flag to your command gcloud run deploy --source=/PATH/

Answer C & D

upvoted 1 times

✉  **zellick** 1 year, 4 months ago

**Selected Answer: CD**

CD is the answer.

<https://cloud.google.com/run/docs/deploying-source-code>

This page describes how to deploy new services and new revisions to Cloud Run directly from source code using a single gcloud CLI command, gcloud run deploy with the --source flag.

Behind the scenes, this command uses Google Cloud's buildpacks and Cloud Build to automatically build container images from your source code without having to install Docker on your machine or set up buildpacks or Cloud Build.

upvoted 1 times

✉  **jcataluna** 1 year, 4 months ago

**Selected Answer: CD**

C & D are correct

upvoted 2 times

✉  **x\_cath** 1 year, 4 months ago

C and D.

C: Google Cloud for buildpacks—an open-source technology that makes it fast and easy for you to create secure, production-ready container images from source code and without a Dockerfile.

<https://cloud.google.com/blog/products/containers-kubernetes/google-cloud-now-supports-buildpacks> (also mentioned by TNT87)

D: Deploying from source code. "This page describes how to deploy new services and new revisions to Cloud Run directly from source code using a single gcloud CLI command, gcloud run deploy with the --source flag."

<https://cloud.google.com/run/docs/deploying-source-code>

A is incorrect because Artifact Registry is for container images, not source code.

B is incorrect because only the built image is needed to be deployed to Cloud Run. "A centrally managed container repository" can be somewhere outside of Google, so as the build tool. It doesn't necessarily have to be built on Cloud Build.

E is irrelevant in this case, as K8S is not involved in this question.

upvoted 4 times

✉  **x\_cath** 1 year, 4 months ago

Finally find something that excludes E as an answer: also in the buildpacks blog post, "these buildpacks produce container images that follow best practices and are suitable for running on all of our container platforms: Cloud Run (fully managed), Anthos, and Google Kubernetes Engine (GKE)"

If it deploys to Cloud Run, it needs to be fully managed. Then the platform cannot be "kubernetes" - use the default value "managed" instead. See <https://cloud.google.com/sdk/gcloud/reference/run/deploy#--platform>

upvoted 1 times

✉  **TNT87** 1 year, 4 months ago

Artifact registry, A

upvoted 1 times

✉  **TNT87** 1 year, 4 months ago

Artifact Registry does not support Docker chunked uploads. Some tools support uploading large images with either chunked upload or a single monolithic upload.

upvoted 1 times

✉  **TNT87** 1 year, 4 months ago

Re-read the question, we simply need a method to deploy the application on Cloud Run without a Dockerfile. That's all

upvoted 1 times

✉  **kisswd** 1 year, 4 months ago

**Selected Answer: BC**

<https://dev.to/alvaradev/gcp-cloud-run-containers-without-dockerfile-2jh3>

upvoted 1 times

✉  **TNT87** 1 year, 4 months ago

B is wrong sir

upvoted 1 times

✉  **TNT87** 1 year, 4 months ago

B, can't be.

upvoted 1 times

 **TNT87** 1 year, 4 months ago

Selected Answer: AC

Answer A

<https://cloud.google.com/run/docs/deploying#images>

Answer C

<https://cloud.google.com/blog/products/containers-kubernetes/google-cloud-now-supports-buildpacks>

upvoted 1 times

 **zellck** 1 year, 4 months ago

"Push your source code to Artifact Registry" -> GAR is not used for source code

upvoted 2 times

 **TNT87** 1 year, 3 months ago

<https://cloud.google.com/artifact-registry/docs/integrate-cloud-run>

upvoted 1 times

 **TNT87** 1 year, 4 months ago

How should you build your container using Google Cloud services?

Its simply A, C

upvoted 1 times

 **zellck** 1 year, 4 months ago

You cannot push source code to Artifact Registry. Cloud Source Repositories stores source code, while GAR stores build artifacts or dependencies.

upvoted 2 times

 **TNT87** 1 year, 4 months ago

Note that source deployments use Artifact Registry to store built containers. If your project doesn't already have an Artifact Registry repository with the name cloud-run-source-deploy in the region you are deploying to, this feature automatically creates an Artifact Registry repository with the name cloud-run-source-deploy.

Red this to understand, i can tell you have never done DevOps at all

<https://cloud.google.com/run/docs/deploying-source-code>

upvoted 1 times

 **TNT87** 1 year, 4 months ago

<https://cloud.google.com/run/docs/deploying#images>

This will help you and if you have done Devops you will understand this

upvoted 1 times

Question #220

*Topic 1*

You work for an organization that manages an online ecommerce website. Your company plans to expand across the world; however, the estore currently serves one specific region. You need to select a SQL database and configure a schema that will scale as your organization grows. You want to create a table that stores all customer transactions and ensure that the customer (CustomerId) and the transaction (TransactionId) are unique. What should you do?

- A. Create a Cloud SQL table that has TransactionId and CustomerId configured as primary keys. Use an incremental number for the TransactionId.
- B. Create a Cloud SQL table that has TransactionId and CustomerId configured as primary keys. Use a random string (UUID) for the TransactionId.
- C. Create a Cloud Spanner table that has TransactionId and CustomerId configured as primary keys. Use a random string (UUID) for the TransactionId.
- D. Create a Cloud Spanner table that has TransactionId and CustomerId configured as primary keys. Use an incremental number for the TransactionId.

**Correct Answer: B**

*Community vote distribution*

C (100%)

 **\_rajan\_** 7 months ago

**Selected Answer: C**

C is correct.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: C**

Requirement is to scale globally. Cloud spanner is the best fit. UUID as a transaction ID is good for security purpose...avoids guessing of next transaction ID.

upvoted 1 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: C**

across the world -> global/multi-region -> spanner

uuid for primary key

upvoted 2 times

 **omermahgoub** 1 year, 3 months ago

C. Create a Cloud Spanner table that has TransactionId and CustomerId configured as primary keys. Use a random string (UUID) for the TransactionId. This will ensure that the combination of CustomerId and TransactionId is unique, even as your organization grows and expands across the world. Cloud Spanner is a highly scalable and globally-distributed SQL database, making it well-suited for this use case. Using a UUID for the TransactionId will ensure that it is unique across all regions and customers.

upvoted 1 times

 **telp** 1 year, 3 months ago

**Selected Answer: C**

Answer C, cloud spanner for multi-region and use primary key to be sure to be unique

upvoted 1 times

 **TNT87** 1 year, 4 months ago

**Selected Answer: C**

[https://cloud.google.com/spanner/docs/schema-design#uuid\\_primary\\_key](https://cloud.google.com/spanner/docs/schema-design#uuid_primary_key)

Answer C

upvoted 1 times

 **sharath25** 1 year, 4 months ago

**Selected Answer: C**

option C

upvoted 1 times

 **x\_cath** 1 year, 4 months ago

**Selected Answer: C**

Globally available --> Cloud Spanner (multi-region). Cloud SQL is a regional service.

upvoted 1 times

 **zellick** 1 year, 4 months ago

**Selected Answer: C**

C is the answer.

upvoted 1 times

- A. Download, install, and start the Snapshot Debugger agent in your VM. Take debug snapshots of the functions that take the longest time. Review the call stack frame, and identify the local variables at that level in the stack.
- B. Import the Cloud Profiler package into your application, and initialize the Profiler agent. Review the generated flame graph in the Google Cloud console to identify time-intensive functions.
- C. Import OpenTelemetry and Trace export packages into your application, and create the trace provider. Review the latency data for your application on the Trace overview page, and identify where bottlenecks are occurring.
- D. Create a Cloud Logging query that gathers the web application's logs. Write a Python script that calculates the difference between the timestamps from the beginning and the end of the application's longest functions to identify time-intensive functions.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **\_rajan\_** 7 months ago

**Selected Answer: B**

B is correct.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: B**

Focus is to find which function is more CPU and Memory intensive. Flame graphs highlights the memory intensive functions in a graphical wa

Question #222

Topic 1

You have a container deployed on Google Kubernetes Engine. The container can sometimes be slow to launch, so you have implemented a liveness probe. You notice that the liveness probe occasionally fails on launch. What should you do?

- A. Add a startup probe.
- B. Increase the initial delay for the liveness probe.
- C. Increase the CPU limit for the container.
- D. Add a readiness probe.

**Correct Answer: D**

*Community vote distribution*

A (55%)	B (36%)	9%
---------	---------	----

CI  
ch  
dei  
ior

 **closer89**  1 year ago

**Selected Answer: A**

<https://kubernetes.io/docs/tasks/configure-pod-container/configure-liveness-readiness-startup-probes/#define-startup-probes>  
The kubelet uses startup probes to know when a container application has started. If such a probe is configured, it disables liveness and readiness checks until it succeeds, making sure those probes don't interfere with the application startup. This can be used to adopt liveness checks on slow starting containers, avoiding them getting killed by the kubelet before they are up and running.

upvoted 6 times

 **Kadhem**  4 months ago

**Selected Answer: A**

"Sometimes, you have to deal with legacy applications that might require an additional startup time on their first initialization. In such cases, it can be tricky to set up liveness probe parameters without compromising the fast response to deadlocks that motivated such a probe. The trick is to set up a startup probe with the same command"

<https://kubernetes.io/docs/tasks/configure-pod-container/configure-liveness-readiness-startup-probes/#define-startup-probes>  
upvoted 2 times

 **\_rajan\_** 7 months ago

**Selected Answer: A**

A startup probe is a probe that Kubernetes uses to determine if a container has started successfully. If the startup probe fails, Kubernetes will restart the container.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: D**

Readiness probe is the right answer. Likeness probe fails if it tries to probe a container not yet ready to serve the traffic. So we need to add readiness probe. There is no such thing called startup probe in kubernetes.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

Typo: Likeness probe... -> Liveness probe

upvoted 1 times

 **flesk** 6 months, 2 weeks ago

Startup probes have been enabled by default since v1.19.

upvoted 1 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: B**

<https://kubernetes.io/docs/tasks/configure-pod-container/configure-liveness-readiness-startup-probes/>

Caution: Liveness probes do not wait for readiness probes to succeed. If you want to wait before executing a liveness probe you should use initialDelaySeconds or a startupProbe.

upvoted 1 times

 **mrvergara** 1 year, 2 months ago

**Selected Answer: B**

A liveness probe checks if the container is running as expected, and if not, it restarts it. If the container is slow to launch, it may take some time for it to fully start up and be able to respond to the liveness probe. Increasing the initial delay for the liveness probe can help mitigate this issue by giving the container more time to start up before the probe begins checking its status. This can help reduce the likelihood of false-positive failures during launch.

upvoted 1 times

 **omermahgoub** 1 year, 3 months ago

**Selected Answer: A**

A. Adding a startup probe is useful for determining when a container has started, but it won't help with the problem of the liveness probe occasionally failing on launch.

B. Increasing the initial delay for the liveness probe might help if the container is taking longer than the delay to start, but it's not a guaranteed solution.

C. Increasing the CPU limit for the container may help if the container is running out of resources, but it may not be necessary if the issue is related to the container's initialization process.

D. A readiness probe can help determine when a container is ready to receive traffic, but it won't help with the problem of the liveness probe occasionally failing on launch.

upvoted 3 times

 **chunker** 1 year, 3 months ago

**Selected Answer: D**

To the people voting B:

The question specifically says that the problem occurs sometimes on launch, so how is the solution not a readiness probe?

upvoted 1 times

 **TNT87** 1 year, 3 months ago

provide a link to cement your argument

upvoted 1 times

 **closer89** 1 year ago

Should be A definitely

<https://kubernetes.io/docs/tasks/configure-pod-container/configure-liveness-readiness-startup-probes/#define-startup-probes>  
Sometimes, you have to deal with legacy applications that might require an additional startup time on their first initialization. In such cases it can be tricky to set up liveness probe parameters without compromising the fast response to deadlocks that motivated such a probe. The trick is to set up a startup probe with the same command, HTTP or TCP check, with a failureThreshold \* periodSeconds long enough to cover the worse case startup time

upvoted 1 times

 **closer89** 1 year ago

Thanks to the startup probe, the application will have a maximum of 5 minutes ( $30 * 10 = 300s$ ) to finish its startup. Once the startup probe has succeeded once, the liveness probe takes over to provide a fast response to container deadlocks. If the startup probe never succeeds, the container is killed after 300s and subject to the pod's restartPolicy.

upvoted 1 times

 **chunker** 1 year, 3 months ago

Changing to A:

The problem is that the liveness probes fires too early, so we need a startup probe to determine when liveness (and potential readiness) probes are valid.

<https://kubernetes.io/docs/tasks/configure-pod-container/configure-liveness-readiness-startup-probes/>

upvoted 2 times

 **TNT87** 1 year, 2 months ago

<https://kubernetes.io/docs/tasks/configure-pod-container/configure-liveness-readiness-startup-probes/>

Answer will remain B

upvoted 1 times

 **zellick** 1 year, 4 months ago

**Selected Answer: B**

B is the answer.

<https://cloud.google.com/blog/products/containers-kubernetes/kubernetes-best-practices-setting-up-health-checks-with-readiness-and-liveness-probes>

upvoted 2 times

 **sharath25** 1 year, 4 months ago

**Selected Answer: B**

option B

<https://kubernetes.io/docs/tasks/configure-pod-container/configure-liveness-readiness-startup-probes/#configure-probes>

upvoted 1 times

 **TNT87** 1 year, 4 months ago

Question #223

Topic 1

You work for an organization that manages an ecommerce site. Your application is deployed behind a global HTTP(S) load balancer. You need to test a new product recommendation algorithm. You plan to use A/B testing to determine the new algorithm's effect on sales in a randomized way. How should you test this feature?

- A. Split traffic between versions using weights.
- B. Enable the new recommendation feature flag on a single instance.
- C. Mirror traffic to the new version of your application.

D. Use HTTP header-based routing.

**Correct Answer: C**

*Community vote distribution*

A (100%)

 **\_\_rajan\_\_** 7 months ago

**Selected Answer: A**

Splitting traffic between versions using weights is a common way to implement A/B testing. To do this, you would create two versions of your application, one with the new recommendation algorithm and one without. You would then configure the load balancer to split traffic between two versions using weights. For example, you could configure the load balancer to send 50% of traffic to the new version and 50% of traffic to the old version.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: A**

Split traffic is the right answer.

upvoted 1 times

 **closer89** 1 year ago

**Selected Answer: A**

in a randomized way - so its A, D otherwise

upvoted 1 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: A**

[https://cloud.google.com/traffic-director/docs/advanced-traffic-management#weight-based\\_traffic\\_splitting\\_for\\_safer\\_deployments](https://cloud.google.com/traffic-director/docs/advanced-traffic-management#weight-based_traffic_splitting_for_safer_deployments)

upvoted 1 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: A**

[https://cloud.google.com/traffic-director/docs/advanced-traffic-management#weight-based\\_traffic\\_splitting\\_for\\_safer\\_deployments](https://cloud.google.com/traffic-director/docs/advanced-traffic-management#weight-based_traffic_splitting_for_safer_deployments)

upvoted 1 times

 **sharath25** 1 year, 4 months ago

**Selected Answer: A**

option A

upvoted 1 times

 **zellck** 1 year, 4 months ago

**Selected Answer: A**

A is the answer.

[https://cloud.google.com/load-balancing/docs/https/traffic-management-global#traffic\\_actions\\_weight-based\\_traffic\\_splitting](https://cloud.google.com/load-balancing/docs/https/traffic-management-global#traffic_actions_weight-based_traffic_splitting)

Deploying a new version of an existing production service generally incurs some risk. Even if your tests pass in staging, you probably don't want to subject 100% of your users to the new version immediately. With traffic management, you can define percentage-based traffic splits across multiple backend services.

For example, you can send 95% of the traffic to the previous version of your service and 5% to the new version of your service. After you've validated that the new production version works as expected, you can gradually shift the percentages until 100% of the traffic reaches the new version of your service. Traffic splitting is typically used for deploying new versions, A/B testing, service migration, and similar processes.

upvoted 1 times

 **kisswd** 1 year, 4 months ago

**Selected Answer: A**

A is the answer

upvoted 1 times

 **TNT87** 1 year, 4 months ago

**Selected Answer: A**

[https://cloud.google.com/traffic-director/docs/advanced-traffic-management#weight-based\\_traffic\\_splitting\\_for\\_safer\\_deployments](https://cloud.google.com/traffic-director/docs/advanced-traffic-management#weight-based_traffic_splitting_for_safer_deployments)  
upvoted 2 times

 **melisargh** 1 year, 4 months ago

**Selected Answer: A**

A is the recommended way to test A/B

<https://cloud.google.com/load-balancing/docs/https/traffic-management-global>

upvoted 2 times

 **TNT87** 1 year, 4 months ago

**Selected Answer: A**

[https://cloud.google.com/architecture/implementing-deployment-and-testing-strategies-on-gke#split\\_the\\_traffic\\_2](https://cloud.google.com/architecture/implementing-deployment-and-testing-strategies-on-gke#split_the_traffic_2)  
[https://cloud.google.com/load-balancing/docs/https/traffic-management-global#traffic\\_actions\\_weight-based\\_traffic\\_splitting](https://cloud.google.com/load-balancing/docs/https/traffic-management-global#traffic_actions_weight-based_traffic_splitting)  
upvoted 1 times

Question #224

*Topic 1*

You plan to deploy a new application revision with a Deployment resource to Google Kubernetes Engine (GKE) in production. The container might not work correctly. You want to minimize risk in case there are issues after deploying the revision. You want to follow Google-recommended best practices. What should you do?

- A. Perform a rolling update with a PodDisruptionBudget of 80%.
- B. Perform a rolling update with a HorizontalPodAutoscaler scale-down policy value of 0.
- C. Convert the Deployment to a StatefulSet, and perform a rolling update with a PodDisruptionBudget of 80%.
- D. Convert the Deployment to a StatefulSet, and perform a rolling update with a HorizontalPodAutoscaler scale-down policy value of 0.

**Correct Answer: D**

*Community vote distribution*

A (100%)

 **\_rajan\_** 7 months ago

**Selected Answer: A**

By performing a rolling update with a PDB of 80%, you can ensure that at least 80% of the Pods are always available during the deployment. This will minimize the risk of downtime in case there are issues with the new revision.

upvoted 2 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: A**

<https://kubernetes.io/docs/tasks/run-application/configure-pdb/#identify-an-application-to-protect>

upvoted 2 times

 **mrvergara** 1 year, 2 months ago

**Selected Answer: A**

A rolling update with a PodDisruptionBudget (PDB) of 80% helps to minimize the risk of issues after deploying a new revision to a production environment in GKE. The PDB specifies the number of pods in a deployment that must remain available during an update, ensuring that there is sufficient capacity to handle any increase in traffic or demand. By setting a PDB of 80%, you ensure that at least 80% of the pods are available during the update, reducing the risk of disruption to your application. This is a recommended best practice by Google for deploying updates to production environments in GKE.

upvoted 1 times

 **TNT87** 1 year, 4 months ago

**Selected Answer: A**

<https://kubernetes.io/docs/tutorials/kubernetes-basics/update/update-intro/>

<https://cloud.google.com/blog/products/containers-kubernetes/ensuring-reliability-and-uptime-for-your-gke-cluster>

Answer A

unvoted 1 times

Question #225

*Topic 1*

Before promoting your new application code to production, you want to conduct testing across a variety of different users. Although this plan is risky, you want to test the new version of the application with production users and you want to control which users are forwarded to the new version of the application based on their operating system. If bugs are discovered in the new version, you want to roll back the newly deployed version of the application as quickly as possible.

What should you do?

- A. Deploy your application on Cloud Run. Use traffic splitting to direct a subset of user traffic to the new version based on the revision tag.
- B. Deploy your application on Google Kubernetes Engine with Anthos Service Mesh. Use traffic splitting to direct a subset of user traffic to the new version based on the user-agent header.
- C. Deploy your application on App Engine. Use traffic splitting to direct a subset of user traffic to the new version based on the IP address.
- D. Deploy your application on Compute Engine. Use Traffic Director to direct a subset of user traffic to the new version based on predefined weights.

**Correct Answer: B**

*Community vote distribution*

B (92%)

8%

 **\_rajan\_** 7 months ago

**Selected Answer: B**

Anthos Service Mesh is a fully managed service that provides a wide range of features for managing microservices, including traffic splitting. Traffic splitting allows you to distribute traffic between different versions of your application based on a variety of factors, such as the user-agent header.

upvoted 2 times

 **purush** 8 months, 3 weeks ago

**Selected Answer: B**

B is perfect. Key is split traffic based on type of OS. So that info can be retrieved with user-agent header.

upvoted 1 times

 **zellck** 1 year, 4 months ago

**Selected Answer: B**

B is the answer.

upvoted 1 times

 **x\_cath** 1 year, 4 months ago

**Selected Answer: B**

The key point for this question is the last two words of this statement "you want to control which users are forwarded to the new version of the application based on their operating system". Operating system. Where could the developers find the OS for a certain user? That's the User-Agent header. Example of a header: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_11\_6 rv:42.0) Gecko/20100101 Firefox/42.0.

- More info about the User-Agent header: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/User-Agent>

upvoted 4 times

 **kisswd** 1 year, 4 months ago

**Selected Answer: B**

The requirement is "you want to control which users are forwarded to the new version of the application based on their operating system". <https://cloud.google.com/traffic-director/docs/ingress-traffic#sending-traffic>

upvoted 3 times

 **TNT87** 1 year, 4 months ago

**Selected Answer: C**

You can use traffic splitting to specify a percentage distribution of traffic across two or more of the versions within a service. Splitting traffic 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/legacy/standard/python/splitting-traffic#ip\\_address\\_splitting](https://cloud.google.com/appengine/docs/legacy/standard/python/splitting-traffic#ip_address_splitting) Answer C

upvoted 1 times

 **zellck** 1 year, 4 months ago

C is based on IP address and not OS, so it cannot be the answer.

upvoted 4 times

Question #226

Topic 1

Your team is writing a backend application to implement the business logic for an interactive voice response (IVR) system that will support a payroll application. The IVR system has the following technical characteristics:

- Each customer phone call is associated with a unique IVR session.
- The IVR system creates a separate persistent gRPC connection to the backend for each session.
- If the connection is interrupted, the IVR system establishes a new connection, causing a slight latency for that call.

You need to determine which compute environment should be used to deploy the backend application. Using current call data, you determine that:

- Call duration ranges from 1 to 30 minutes.
- Calls are typically made during business hours.
- There are significant spikes of calls around certain known dates (e.g., pay days), or when large payroll changes occur.

You want to minimize cost, effort, and operational overhead. Where should you deploy the backend application?

- A. Compute Engine
- B. Google Kubernetes Engine cluster in Standard mode
- C. Cloud Functions
- D. Cloud Run

**Correct Answer: D**

*Community vote distribution*

D (100%)

 rajan\_ 7 months ago

**Selected Answer: D**

D is correct.

upvoted 1 times

 purushi 8 months, 3 weeks ago

**Selected Answer: D**

Cloud Run is more suitable for gRPC communication between micro services.

The key here is "gRPC connection to the backend for each session".

upvoted 1 times

 telp 1 year, 3 months ago

**Selected Answer: D**

Answer D

upvoted 1 times

 zellick 1 year, 4 months ago

**Selected Answer: D**

D is the answer.

upvoted 2 times

 TNT87 1 year, 4 months ago

**Selected Answer: D**

Answer D

This page shows Cloud Run-specific details for developers who want to use gRPC to connect a Cloud Run service with other services, for example, to provide simple, high performance communication between internal microservices. You can use all gRPC types, streaming or unary with Cloud Run.

Possible use cases include:

Communication between internal microservices.

High loads of data (gRPC uses protocol buffers, which are up to seven times faster than REST calls).

Only a simple service definition is needed, you don't want to write a full client library.

Use streaming gRPCs in your gRPC server to build more responsive applications and APIs.

<https://cloud.google.com/run/docs/tutorials/secure-services#:~:text=The%20backend%20service%20is%20private,Google%20Cloud%20except%20where%20necessary>.

upvoted 2 times

You are developing an application hosted on Google Cloud that uses a MySQL relational database schema. The application will have a large volume of reads and writes to the database and will require backups and ongoing capacity planning. Your team does not have time to fully manage the database but can take on small administrative tasks. How should you host the database?

- A. Configure Cloud SQL to host the database, and import the schema into Cloud SQL.
- B. Deploy MySQL from the Google Cloud Marketplace to the database using a client, and import the schema.
- C. Configure Bigtable to host the database, and import the data into Bigtable.
- D. Configure Cloud Spanner to host the database, and import the schema into Cloud Spanner.
- E. Configure Firestore to host the database, and import the data into Firestore.

**Correct Answer: D***Community vote distribution*

A (94%)

6%

**✉️**  \_\_rajan\_\_ 7 months ago**Selected Answer: A**

It is a good choice for applications that require a high volume of reads and writes, as well as regular backups and capacity planning.  
upvoted 1 times

**✉️**  purushi 8 months, 3 weeks ago**Selected Answer: A**

I go with A, since it is a Cloud SQL is a fully managed service that involves less operational overheads.  
upvoted 1 times

**✉️**  closer89 1 year ago**Selected Answer: A**

A or D  
cloud sql ideal for heavy reads and not ideal for heavy writes  
spanner ideal for both reads/writes but more about global  
anyway both are extremely fast - then go for A  
upvoted 3 times

**✉️**  Pime13 1 year, 2 months ago**Selected Answer: A**

<https://cloud.google.com/sql/docs/mysql> -> no time to manage DB therefore use a manage service  
upvoted 1 times

✉  **omermahgoub** 1 year, 3 months ago

The best option to host the MySQL relational database schema on Google Cloud while minimizing management overhead and maximizing the ability to handle a large volume of reads and writes, backups and ongoing capacity planning would be:

A. Configure Cloud SQL to host the database, and import the schema into Cloud SQL.

Cloud SQL is a fully-managed service that makes it easy to set up, maintain, manage, and administer your relational databases on Google Cloud. It is specifically designed for MySQL, so it is a good fit for this use case. With Cloud SQL, you can automatically backup your data, and perform capacity planning, so you don't have to worry about managing the infrastructure. Additionally, Cloud SQL provides high availability, automatic failover and easy scaling.

Option D and E are not correct since Cloud Spanner is a NoSQL database and Firestore is a document-based database and not suitable for Relational Database.

upvoted 1 times

✉  **omermahgoub** 1 year, 3 months ago

Option C is not the best option to host the MySQL relational database schema because Bigtable is not a relational database. It is a NoSQL wide-column store database that is designed to handle large amounts of data with low latency. It is not a good fit for this use case because it does not provide the same level of support for relational data structures and SQL queries that a relational database like MySQL would.

Additionally, Bigtable is not designed for handling large volumes of reads and writes, backups and ongoing capacity planning.

upvoted 1 times

✉  **telp** 1 year, 3 months ago

**Selected Answer: A**

A, cloud SQL is easy to put in place from another relational database

upvoted 1 times

✉  **x\_cath** 1 year, 4 months ago

**Selected Answer: A**

The answer A is more likely to be the correct one. Although Cloud Spanner is also a relational DB service (and has certain advantages over Cloud SQL), migrating from MySQL to Cloud Spanner is not as trivial as "import the schema" (stating by the answer D). If D has been excluded, the relational DB option in the answers is A: Cloud SQL.

<https://cloud.google.com/spanner/docs/migrating-mysql-to-spanner#migration-process>

upvoted 2 times

✉  **zellck** 1 year, 4 months ago

**Selected Answer: A**

A is the answer.

<https://cloud.google.com/sql/docs/mysql>

Cloud SQL for MySQL is a fully-managed database service that helps you set up, maintain, manage, and administer your MySQL relational databases on Google Cloud Platform.

upvoted 2 times

✉  **TNT87** 1 year, 4 months ago

**Selected Answer: A**

Cloud SQL: Cloud SQL is a web service that allows you to create, configure, and use relational databases that live in Google's cloud. It is a fully managed service that maintains, manages, and administers your databases, allowing you to focus on your applications and services.

Answer A

upvoted 3 times

✉  **TNT87** 1 year, 4 months ago

**Selected Answer: C**

a large volume of reads and writes to the database and will require backups and ongoing capacity planning. That's Bigtable. Changing my answer to C

upvoted 1 times

✉  **TNT87** 1 year, 4 months ago

But Bigtable doesn't use MySQL.... aiili will stick to A

upvoted 1 times

✉  **TNT87** 1 year, 4 months ago

**Selected Answer: A**

Answer A

upvoted 1 times

You are developing a new web application using Cloud Run and committing code to Cloud Source Repositories. You want to deploy new code in the most efficient way possible. You have already created a Cloud Build YAML file that builds a container and runs the following command: gcloud run deploy. What should you do next?

- A. Create a Pub/Sub topic to be notified when code is pushed to the repository. Create a Pub/Sub trigger that runs the build file when an event is published to the topic.
- B. Create a build trigger that runs the build file in response to a repository code being pushed to the development branch.
- C. Create a webhook build trigger that runs the build file in response to HTTP POST calls to the webhook URL.
- D. Create a Cron job that runs the following command every 24 hours: gcloud builds submit.

**Correct Answer: B**

*Community vote distribution*

B (100%)

✉️  **edoo** 2 months, 2 weeks ago

**Selected Answer: B**

<https://cloud.google.com/build/docs/automating-builds/create-manage-triggers>  
upvoted 1 times

✉️  **\_rajan\_\_** 7 months ago

**Selected Answer: B**

B is correct.  
upvoted 1 times

✉️  **purushi** 8 months, 3 weeks ago

**Selected Answer: B**

I go with B.  
Code commit to the repository should trigger the build process.  
C is complicated because of webhook POST Url  
upvoted 1 times

✉️  **Pime13** 1 year, 2 months ago

**Selected Answer: B**

<https://cloud.google.com/build/docs/triggers>  
upvoted 1 times

✉️  **zellick** 1 year, 4 months ago

**Selected Answer: B**

B is the answer.

<https://cloud.google.com/build/docs/triggers>  
Cloud Build uses build triggers to enable CI/CD automation. You can configure triggers to listen for incoming events, such as when a new commit is pushed to a repository or when a pull request is initiated, and then automatically execute a build when new events come in. You can also configure triggers to build code on any changes to your source repository or only on changes that match certain criteria.

upvoted 1 times

✉️  **TNT87** 1 year, 4 months ago

**Selected Answer: B**

Cloud Build enables you to build the container image, store the built image in Container Registry, and then deploy the image to Cloud Run.  
upvoted 1 times

✉️  **TNT87** 1 year, 4 months ago

**Selected Answer: B**

[https://cloud.google.com/build/docs/automating-builds/create-manage-triggers#connect\\_repo](https://cloud.google.com/build/docs/automating-builds/create-manage-triggers#connect_repo)  
Answer B  
upvoted 1 times

Question #229

Topic 1

You are a developer at a large organization. You are deploying a web application to Google Kubernetes Engine (GKE). The DevOps team has built a CI/CD pipeline that uses Cloud Deploy to deploy the application to Dev, Test, and Prod clusters in GKE. After Cloud Deploy successfully deploys the application to the Dev cluster, you want to automatically promote it to the Test cluster. How should you configure this process following Google-recommended best practices?

- A. 1. Create a Cloud Build trigger that listens for SUCCEEDED Pub/Sub messages from the clouddesploy-operations topic.  
2. Configure Cloud Build to include a step that promotes the application to the Test cluster.
- B. 1. Create a Cloud Function that calls the Google Cloud Deploy API to promote the application to the Test cluster.  
2. Configure this function to be triggered by SUCCEEDED Pub/Sub messages from the cloud-builds topic.

- C. 1. Create a Cloud Function that calls the Google Cloud Deploy API to promote the application to the Test cluster.
  2. Configure this function to be triggered by SUCCEEDED Pub/Sub messages from the clouddesign-operations topic.
- D. 1. Create a Cloud Build pipeline that uses the gke-deploy builder.
  2. Create a Cloud Build trigger that listens for SUCCEEDED Pub/Sub messages from the cloud-builds topic.
  3. Configure this pipeline to run a deployment step to the Test cluster.

**Correct Answer: D**

*Community vote distribution*

C (58%)

A (42%)

 **Kadhem** 3 months, 4 weeks ago

**Selected Answer: C**

C in answer. A cannot be the answer as it mention "cloud build" and the question talk about cloud deploy.  
upvoted 3 times

 **\_\_rajan\_\_** 7 months ago

**Selected Answer: C**

I think it should be C.  
upvoted 1 times

 **purush** 8 months, 3 weeks ago

**Selected Answer: A**

Its either A or D. A is better since the topic is clouddesign-operations. Once the msg is being published to this topic that means deployment has been done successfully to the environment, so the next step is to deploy the containers in the test cluster. So I go with option A.  
upvoted 1 times

 **closer89** 1 year ago

**Selected Answer: A**

<https://cloud.google.com/functions/docs/calling/pubsub>  
[https://cloud.google.com/deploy/docs/integrating#integrating\\_with\\_automated\\_testing](https://cloud.google.com/deploy/docs/integrating#integrating_with_automated_testing)  
 cloud deploy sends message  
 cloud build reads this message  
 upvoted 1 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: A**

[https://cloud.google.com/build/docs/automate-builds-pubsub-events#console\\_2](https://cloud.google.com/build/docs/automate-builds-pubsub-events#console_2)  
 upvoted 1 times

 **Pime13** 1 year, 2 months ago

Cloud Build Pub/Sub triggers enable you to execute builds in response to Google Cloud events published over Pub/Sub. You can use information from a Pub/Sub event to parameterize your build and to decide if a build should execute in response to the event. Pub/Sub triggers can be configured to listen to any Pub/Sub topic.  
 upvoted 1 times

 **TNT87** 1 year, 2 months ago

**Selected Answer: C**

<https://cloud.google.com/functions/docs/calling/pubsub>  
 upvoted 1 times

mrvergara 1 year, 2 months ago

Selected Answer: C

This option (C) is recommended because it follows the best practice of using a serverless function, specifically Cloud Functions, for triggering automated tasks in response to events. In this case, the function will be triggered by a SUCCEEDED message from the clouddesploy-operations topic, indicating that the deployment to the Dev cluster has completed successfully. The function will then use the Google Cloud Deploy API to promote the application to the Test cluster.

Using a Cloud Function in this way allows for a scalable, event-driven architecture and reduces the amount of infrastructure required to manage the deployment process.

upvoted 2 times

mrvergara 1 year, 2 months ago

Option A is not better than Option C because it involves using Cloud Build instead of Cloud Functions for the deployment promotion process. While Cloud Build is a powerful tool for building and testing applications, it is generally not recommended for triggering automated tasks in response to events like the successful deployment of an application to a cluster.

In Option A, the Cloud Build trigger listens for SUCCEEDED Pub/Sub messages from the clouddesploy-operations topic, and then promotes the application to the Test cluster as part of the Cloud Build pipeline. This approach involves using a more complex and less scalable infrastructure than using a serverless function like Cloud Functions.

On the other hand, Option C uses a Cloud Function to promote the application, which is a more streamlined, scalable, and event-driven solution. Cloud Functions are designed specifically for triggering automated tasks in response to events, making them a better choice for this type of use case.

upvoted 3 times

TNT87 1 year, 2 months ago

Your explanation is not from the documentation sir, kindly provide a link to your answer. Do you also understand what and when to use cloud build??

upvoted 2 times

TNT87 1 year, 2 months ago

Selected Answer: A

[https://cloud.google.com/deploy/docs/integrating#integrating\\_with\\_automated\\_testing](https://cloud.google.com/deploy/docs/integrating#integrating_with_automated_testing)  
[https://cloud.google.com/deploy/docs/integrating#before\\_you\\_begin](https://cloud.google.com/deploy/docs/integrating#before_you_begin)

upvoted 2 times

TNT87 1 year, 2 months ago

<https://cloud.google.com/functions/docs/calling/pubsub>  
mhh i see why it could be C

upvoted 1 times

Question #230

Topic 1

Your application is running as a container in a Google Kubernetes Engine cluster. You need to add a secret to your application using a secure approach. What should you do?

- A. Create a Kubernetes Secret, and pass the Secret as an environment variable to the container.
- B. Enable Application-layer Secret Encryption on the cluster using a Cloud Key Management Service (KMS) key.
- C. Store the credential in Cloud KMS. Create a Google service account (GSA) to read the credential from Cloud KMS. Export the GSA as a .json file, and pass the .json file to the container as a volume which can read the credential from Cloud KMS.

D. Store the credential in Secret Manager. Create a Google service account (GSA) to read the credential from Secret Manager. Create a Kubernetes service account (KSA) to run the container. Use Workload Identity to configure your KSA to act as a GSA.

**Correct Answer: A**

*Community vote distribution*

D (64%)

A (36%)

 **examprof** 4 months, 3 weeks ago

Alternative D is correct.

Problem I see with alternative A is that storing secrets in Kubernetes Secrets in plain text format is not aligned with best practices, as such secrets are base64 encoded but not encrypted at rest. If a malicious agent gains access to the cluster, secrets can be easily decoded and captured.

upvoted 1 times

 **\_rajan\_** 7 months ago

Question #231

*Topic 1*

You are a developer at a financial institution. You use Cloud Shell to interact with Google Cloud services. User data is currently stored on an ephemeral disk; however, a recently passed regulation mandates that you can no longer store sensitive information on an ephemeral disk. You need to implement a new storage solution for your user data. You want to minimize code changes. Where should you store your user data?

su

- A. Store user data on a Cloud Shell home disk, and log in at least every 120 days to prevent its deletion.
- B. Store user data on a persistent disk in a Compute Engine instance.
- C. Store user data in a Cloud Storage bucket.
- D. Store user data in BigQuery tables.

**Correct Answer: C**

*Community vote distribution*

B (100%)

 **purushi** 8 months, 3 weeks ago

**Selected Answer: B**

Persistent disk is the right option to store sensitive info in this case. ( Obviously in the general sense, we should store user data in the data stc  
Key points:

- 1) You use Cloud Shell to interact with Google Cloud services
- 2) You want to minimize code changes

upvoted 1 times

 **rich\_maverick** 1 year, 2 months ago

C is best answer:

Using gsfuse: <https://github.com/GoogleCloudPlatform/gcsfuse> you can have Cloud Shell interact with Cloud Storage directly as a drive. You don't need to redesign or recode or move your app from Cloud Shell. This is the same approach that dataproc uses to leverage GCS as a storage solution.

upvoted 3 times

 **TNT87** 1 year, 2 months ago

No , kindly read the documentation about cloud shell and what it is them you will know why B is the answer

upvoted 1 times

 **mrvergara** 1 year, 2 months ago

**Selected Answer: B**

Store user data in a Cloud Storage bucket is a good option for storing large amounts of data, but if you need to minimize code changes, using persistent disk in a Compute Engine instance may be a better fit as it provides a more direct replacement for an ephemeral disk with similar access patterns, which will likely require fewer changes to your existing code. Storing user data in a Cloud Storage bucket would likely require more significant changes to how your application interacts with the data.

upvoted 4 times

 **TNT87** 1 year, 2 months ago

**Selected Answer: B**

[https://cloud.google.com/shell/docs/how-cloud-shell-works#persistent\\_disk\\_storage](https://cloud.google.com/shell/docs/how-cloud-shell-works#persistent_disk_storage)

How Cloud Shell works

bookmark\_border

Cloud Shell provisions a Compute Engine virtual machine running a Debian-based Linux operating system for your temporary use. This virtual machine is owned and managed by Google Cloud, so will not appear within any of your GCP projects.

<https://cloud.google.com/shell/docs/how-cloud-shell-works>

upvoted 1 times

Question #232

Topic 1

You recently developed a web application to transfer log data to a Cloud Storage bucket daily. Authenticated users will regularly review logs from the prior two weeks for critical events. After that, logs will be reviewed once annually by an external auditor. Data must be stored for a period of no less than 7 years. You want to propose a storage solution that meets these requirements and minimizes costs. What should you do? (Choose two.)

- A. Use the Bucket Lock feature to set the retention policy on the data.
- B. Run a scheduled job to set the storage class to Coldline for objects older than 14 days.
- C. Create a JSON Web Token (JWT) for users needing access to the Coldline storage buckets.
- D. Create a lifecycle management policy to set the storage class to Coldline for objects older than 14 days.
- E. Create a lifecycle management policy to set the storage class to Nearline for objects older than 14 days.

**Correct Answer: BE**

*Community vote distribution*

AD (100%)

 **purushi** 8 months, 3 weeks ago

**Selected Answer: AD**

A -> Data must be stored for a period of no less than 7 years.

D -> Authenticated users will regularly review logs from the prior two weeks for critical events. After that, logs will be reviewed once annually by an external auditor.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

D. Create a lifecycle management policy to set the storage class to Coldline for objects older than 14 days

This should be like setting the storage class to Archival for objects older than 14 days, since logs will be reviewed once annually by an external auditor. But the close answer is Coldline in Option D.

upvoted 1 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: AD**

lock to avoid deletion before 7 years

lifecycle policy to change to coldline (since it will be accessed annually) after 14 days.

upvoted 1 times

 **mrvergara** 1 year, 2 months ago

**Selected Answer: AD**

The requirement of storing data for a period of no less than 7 years can be met by setting the retention policy for the data in the Cloud Storage bucket. This can be done using the Bucket Lock feature (A) or a lifecycle management policy (D), which can be set to retain the objects for the required period of 7 years.

upvoted 3 times

 **TNT87** 1 year, 2 months ago

**Selected Answer: AD**

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

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

upvoted 1 times

- A. Create a new Cloud Function that is triggered when Cloud Audit Logs detects the cloudfunctions.functions.sourceCodeSet operation in the original Cloud Function. Send mock requests to the new function to evaluate the functionality.
- B. Make a copy of the Cloud Function, and rewrite the code to be HTTP-triggered. Edit and test the new version by triggering the HTTP endpoint. Send mock requests to the new function to evaluate the functionality.
- C. Install the Functions Frameworks library, and configure the Cloud Function on localhost. Make a copy of the function, and make edits to the new version. Test the new version using curl.
- D. Make a copy of the Cloud Function in the Google Cloud console. Use the Cloud console's in-line editor to make source code changes to the new function. Modify your web application to call the new function, and test the new version in production

**Correct Answer: B**

*Community vote distribution*

C (67%)

B (33%)

braska 5 months, 1 week ago

Selected Answer: C

Making a copy of the function for edits ensures that your changes do not affect the original function in production. It provides a controlled environment for development and testing.  
curl Testing:

Testing the new version using curl is a simple and effective way to send mock requests and evaluate the functionality of your Cloud Function locally.

Using the Functions Frameworks library and local testing provides a development environment that is both efficient and aligned with Google-recommended best practices for Cloud Functions development.

upvoted 1 times

purushi 8 months, 3 weeks ago

Selected Answer: C

Option C is well suited for testing cloud functions in the local environment.  
<https://cloud.google.com/functions/docs/running/function-frameworks>

upvoted 1 times

AlizCert 9 months ago

Not B because

"Local testing"

Many development paradigms depend on being able to test your code relatively quickly.

Because testing code on Cloud Functions itself involves waiting for deployed code and log entries to become available, running and testing your function on your development machine can make the testing process (and, in turn, the development process) significantly faster."

C because: <https://cloud.google.com/functions/docs/running/function-frameworks>

upvoted 1 times

closer89 1 year ago

Selected Answer: C

[https://cloud.google.com/functions/docs/running/calling#cloudevent\\_functions](https://cloud.google.com/functions/docs/running/calling#cloudevent_functions)

upvoted 1 times

Pime13 1 year, 2 months ago

Selected Answer: C

[https://cloud.google.com/functions/docs/running/overview#choosing\\_an\\_abstraction\\_layer](https://cloud.google.com/functions/docs/running/overview#choosing_an_abstraction_layer)

<https://cloud.google.com/functions/docs/running/function-frameworks>

<https://cloud.google.com/functions/docs/running/calling#cloudevent-function-curl-tabs-storage>

upvoted 1 times

TNT87 1 year, 2 months ago

Selected Answer: B

<https://cloud.google.com/functions/docs/writing/write-event-driven-functions>

<https://cloud.google.com/functions/docs/calling/storage>

upvoted 2 times

TNT87 1 year, 2 months ago

<https://firebase.google.com/docs/functions/gcp-storage-events>

upvoted 1 times

Your team is setting up a build pipeline for an application that will run in Google Kubernetes Engine (GKE). For security reasons, you only want images produced by the pipeline to be deployed to your GKE cluster. Which combination of Google Cloud services should you use?

- A. Cloud Build, Cloud Storage, and Binary Authorization
- B. Google Cloud Deploy, Cloud Storage, and Google Cloud Armor
- C. Google Cloud Deploy, Artifact Registry, and Google Cloud Armor
- D. Cloud Build, Artifact Registry, and Binary Authorization

**Correct Answer: C**

*Community vote distribution*

D (100%)

 **alpha\_canary** 2 weeks, 5 days ago

**Selected Answer: D**

<https://cloud.google.com/architecture/app-development-and-delivery-with-cloud-code-gcb-cd-and-gke#architecture>  
upvoted 1 times

 **\_\_rajan\_\_** 7 months ago

**Selected Answer: D**

D is correct.  
upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: D**

D is the right option.  
Cloud Build: To build code and push image into Artifactory  
Artifact Registry: A store for built images  
Binary Authorization: Approval for deployment  
upvoted 1 times

 **bober86** 1 year, 2 months ago

**Selected Answer: D**

<https://cloud.google.com/binary-authorization/docs/cloud-build>  
upvoted 2 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: D**

i choose D  
upvoted 1 times

 **TNT87** 1 year, 2 months ago

**Selected Answer: D**

I'd go with D  
<https://cloud.google.com/architecture/app-development-and-delivery-with-cloud-code-gcb-cd-and-gke#objectives>  
upvoted 1 times

You are supporting a business-critical application in production deployed on Cloud Run. The application is reporting HTTP 500 errors that are affecting the usability of the application. You want to be alerted when the number of errors exceeds 15% of the requests within a specific time window. What should you do?

WINDOW. What should you do?

- A. Create a Cloud Function that consumes the Cloud Monitoring API. Use Cloud Scheduler to trigger the Cloud Function daily and alert you if the number of errors is above the defined threshold.
- B. Navigate to the Cloud Run page in the Google Cloud console, and select the service from the services list. Use the Metrics tab to visualize the number of errors for that revision, and refresh the page daily.
- C. Create an alerting policy in Cloud Monitoring that alerts you if the number of errors is above the defined threshold.
- D. Create a Cloud Function that consumes the Cloud Monitoring API. Use Cloud Composer to trigger the Cloud Function daily and alert you if the number of errors is above the defined threshold.

**Correct Answer: A**

*Community vote distribution*

C (78%)

A (22%)

 **Tusky4u** 3 months, 3 weeks ago  
C is 100% correct answer, practically used  
upvoted 1 times

 **\_rajan\_** 7 months ago  
**Selected Answer: C**  
C is correct.  
upvoted 1 times

Question #236

Topic 1

You need to build a public API that authenticates, enforces quotas, and reports metrics for API callers. Which tool should you use to complete this architecture?



- A. App Engine
- B. Cloud Endpoints
- C. Identity-Aware Proxy
- D. GKE Ingress for HTTP(S) Load Balancing

**Correct Answer: D**

*Community vote distribution*  
B (100%)

 **xiaofeng\_0226** 5 months, 2 weeks ago

**Selected Answer: B**  
B is correct  
upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: B**  
Cloud endpoints is the right answer.  
[cloud.google.com/endpoints/docs/frameworks/quotas-configure](https://cloud.google.com/endpoints/docs/frameworks/quotas-configure)  
upvoted 1 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: B**  
<https://cloud.google.com/endpoints>  
upvoted 2 times

 **TNT87** 1 year, 2 months ago

**Selected Answer: B**  
<https://cloud.google.com/endpoints/docs/openapi/quotas-overview>  
upvoted 1 times

Question #237

Topic 1

You noticed that your application was forcefully shut down during a Deployment update in Google Kubernetes Engine. Your application didn't close the database connection before it was terminated. You want to update your application to make sure that it completes a graceful shutdown. What

should you do?

- A. Update your code to process a received SIGTERM signal to gracefully disconnect from the database.
- B. Configure a PodDisruptionBudget to prevent the Pod from being forcefully shut down.
- C. Increase the terminationGracePeriodSeconds for your application.
- D. Configure a PreStop hook to shut down your application.

**Correct Answer: B**

*Community vote distribution*

A (89%)

11%

✉  **\_\_rajan\_\_** 7 months ago

**Selected Answer: A**

This is the most direct and effective way to ensure that your application completes a graceful shutdown. When your application receives a SIGTERM signal, it should use this signal as a trigger to disconnect from the database and complete any other necessary tasks before terminating.

upvoted 1 times

✉  **purushi** 8 months, 3 weeks ago

**Selected Answer: A**

A is right. After caching the SIGTERM event that raised by Pod shutdown, we need to release the DB connection.

upvoted 1 times

✉  **closer89** 1 year ago

**Selected Answer: A**

A is a best practice

<https://cloud.google.com/blog/products/containers-kubernetes/kubernetes-best-practices-terminating-with-grace>

upvoted 2 times

✉  **Pime13** 1 year, 2 months ago

**Selected Answer: A**

<https://cloud.google.com/blog/products/containers-kubernetes/kubernetes-best-practices-terminating-with-grace>

upvoted 1 times

✉  **Pime13** 1 year, 2 months ago

**Selected Answer: A**

i would choose A

upvoted 1 times

✉  **mrvergara** 1 year, 2 months ago

**Selected Answer: A**

While a PodDisruptionBudget can help protect a Pod from being forcibly terminated during a deployment update, it does not ensure a graceful shutdown of the application. Option A, updating the code to handle SIGTERM signals, is the recommended way to ensure a graceful shutdown in the event of a termination.

upvoted 2 times

✉  **mrvergara** 1 year, 2 months ago

Here's a link to the official Kubernetes documentation on the SIGTERM signal:

<https://kubernetes.io/docs/concepts/containers/container-lifecycle-hooks/#container-hooks>

And here's a link to the official Kubernetes documentation on how to handle the SIGTERM signal in your application:

<https://kubernetes.io/docs/tasks/configure-pod-container/configure-liveness-readiness-startup-probes/#define-a-graceful-shutdown-for-your-application>

upvoted 1 times

✉  **TNT87** 1 year, 2 months ago

Selected Answer: B

<https://kubernetes.io/docs/concepts/workloads/pods/disruptions/#pod-disruption-budgets>

<https://cloud.google.com/blog/products/containers-kubernetes/kubernetes-best-practices-terminating-with-grace>

upvoted 1 times

✉  **mrvergara** 1 year, 2 months ago

Option B, Configuring a PodDisruptionBudget, is used to control the number of replicas of a pod that can be down simultaneously. It prevents voluntary disruption of the pods, but it does not prevent forced termination of the pods. When a pod is terminated forcefully, for example, during a node failure, the PodDisruptionBudget does not come into play. In this scenario, you need to handle the termination gracefully in your application code, as described in option A.

upvoted 3 times

✉  **TNT87** 1 year, 2 months ago

As i said i passed my exam already

upvoted 1 times

✉  **mrvergara** 1 year, 2 months ago

And you don't want other people passing the exam? Because this option B seems to be wrong to me

upvoted 7 times

✉  **TNT87** 1 year, 2 months ago

According to you and who are you?? stay away from baseless arguments they don't benefit you with anything

upvoted 2 times

✉  **wanrltw** 4 months, 1 week ago

Have you passed the exam scoring 100% and it has had this particular question? Cause if not, you're just talking smack - GCP exams do not show where exactly you were wrong, so even if you passed it successfully it doesn't mean that you're right in this exact question.

upvoted 1 times

✉  **NewComer200** 12 months ago

I think Mr. TNT87 is very exceed person, because I know he answered very excellent answer in other questions.

But this question's demand is

"You want to update your application to make sure that it completes a graceful shutdown.".

It's not about avoiding shutdown.

I think the answer is what you should do in occurring shutdown.

So me too, I think "to prevent the Pod from being forcefully shut down." doesn't answer for demand.

I think also right answer is A.

upvoted 3 times

You are a lead developer working on a new retail system that runs on Cloud Run and Firestore in Datastore mode. A web UI requirement is for the system to display a list of available products when users access the system and for the user to be able to browse through all products. You have implemented this requirement in the minimum viable product (MVP) phase by returning a list of all available products stored in Firestore.

A few months after go-live, you notice that Cloud Run instances are terminated with HTTP 500: Container instances are exceeding memory limits errors during busy times. This error coincides with spikes in the number of Datastore entity reads. You need to prevent Cloud Run from crashing and decrease the number of Datastore entity reads. You want to use a solution that optimizes system performance. What should you do?

- A. Modify the query that returns the product list using integer offsets.
- B. Modify the query that returns the product list using limits.
- C. Modify the Cloud Run configuration to increase the memory limits.
- D. Modify the query that returns the product list using cursors.

**Correct Answer: C***Community vote distribution*

D (82%)

Other

✉️  **wanrltw** 4 months, 1 week ago

**Selected Answer: D**

[https://cloud.google.com/datastore/docs/concepts/queries#cursors\\_limits\\_and\\_offsets](https://cloud.google.com/datastore/docs/concepts/queries#cursors_limits_and_offsets)  
upvoted 2 times

✉️  **\_rajan\_** 7 months ago

**Selected Answer: D**

Cursors allow you to paginate through the results of a Firestore query. This can be useful for queries that return a large number of results, such as the query that returns the list of all available products.  
upvoted 1 times

✉️  **purushi** 8 months, 3 weeks ago

**Selected Answer: D**

D is correct.  
Use pagination and return only results in batch/limits when querying for the list of products. This is called lazy loading.  
upvoted 1 times

✉️  **bober86** 1 year, 2 months ago

**Selected Answer: D**

<https://cloud.google.com/datastore/docs/best-practices#queries>  
upvoted 1 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: A**

Note: To conserve memory and improve performance, a query should, whenever possible, specify a limit on the number of results returned.

[https://cloud.google.com/datastore/docs/concepts/queries#cursors\\_limits\\_and\\_offsets](https://cloud.google.com/datastore/docs/concepts/queries#cursors_limits_and_offsets)

upvoted 1 times

 **Pime13** 1 year, 2 months ago

it's D, not a, wrongly selected

upvoted 1 times

 **Pime13** 1 year, 2 months ago

Although Datastore mode databases support integer offsets, you should avoid using them. Instead, use cursors. Using an offset only avoids returning the skipped entities to your application, but these entities are still retrieved internally. The skipped entities do affect the latency of the query, and your application is billed for the read operations required to retrieve them. Using cursors instead of offsets lets you avoid all these costs

upvoted 1 times

 **mrvergara** 1 year, 2 months ago

**Selected Answer: D**

While increasing the memory limits of Cloud Run instances could help alleviate the issue temporarily, it would not address the root cause of the problem, which is the high number of Datastore entity reads during busy times. Over time, as more products are added to the system, this problem would only become more severe, and you would have to continually increase the memory limits to prevent Cloud Run from crashing.

Using cursors to paginate the results and retrieve a limited number of products at a time is a more sustainable solution as it reduces the amount of data that needs to be read from Datastore and decreases the memory usage of your Cloud Run instances. This way, you can maintain the performance of the system and prevent it from crashing, even as more products are added over time.

upvoted 4 times

 **TNT87** 1 year, 2 months ago

**Selected Answer: C**

The issue is with the memory limits.

<https://cloud.google.com/run/docs/configuring/memory-limits#optimizing>

<https://cloud.google.com/run/docs/configuring/memory-limits#optimizing>

upvoted 1 times

 **mrvergara** 1 year, 2 months ago

<https://cloud.google.com/datastore/docs/concepts/queries#cursors>

Cursors allow you to paginate through query results efficiently, which can help reduce the number of Datastore entity reads and prevent Cloud Run instances from crashing due to exceeding memory limits. By using cursors, you can retrieve only a portion of the query results at a time instead of retrieving all results in one go, which can help optimize system performance.

upvoted 4 times

 **mrvergara** 1 year, 2 months ago

Option C, increasing the memory limits of Cloud Run, may provide a temporary solution to the issue, but it does not address the root cause of the problem. The root cause is that too many Datastore entities are being read in one go, which is causing Cloud Run instances to exceed their memory limits and crash. Increasing the memory limits simply allows the instances to handle more data in memory, but it does not address the issue of retrieving too much data in one go.

Using cursors to paginate through query results, as in option D, is a better solution because it allows you to retrieve only the necessary data at a time, which can help reduce the number of Datastore entity reads and prevent Cloud Run instances from crashing.

upvoted 3 times

 **NewComer200** 12 months ago

I agree with Mr. mrvergara

If I would image I'm actually creating the code for this program code, I would think current program isn't very good. I'll think I should improve this program better than now firstly. If it's possible, I wouldn't like to add resources.

upvoted 2 times

You need to deploy an internet-facing microservices application to Google Kubernetes Engine (GKE). You want to validate new features using the A/B testing method. You have the following requirements for deploying new container image releases:

- There is no downtime when new container images are deployed.
- New production releases are tested and verified using a subset of production users.

What should you do?

1. Configure your CI/CD pipeline to update the Deployment manifest file by replacing the container version with the latest version.
  2. Recreate the Pods in your cluster by applying the Deployment manifest file.
  3. Validate the application's performance by comparing its functionality with the previous release version, and roll back if an issue arises.
1. Create a second namespace on GKE for the new release version.
  2. Create a Deployment configuration for the second namespace with the desired number of Pods.
  3. Deploy new container versions in the second namespace.
  4. Update the Ingress configuration to route traffic to the namespace with the new container versions.
1. Install the Anthos Service Mesh on your GKE cluster.
  2. Create two Deployments on the GKE cluster, and label them with different version names.
  3. Implement an Istio routing rule to send a small percentage of traffic to the Deployment that references the new version of the application.
1. Implement a rolling update pattern by replacing the Pods gradually with the new release version.
  2. Validate the application's performance for the new subset of users during the rollout, and roll back if an issue arises.

**Correct Answer: D**

*Community vote distribution*

C (65%)

B (29%)

6%

✉️  **Pime13**  1 year, 2 months ago

**Selected Answer: C**

[https://cloud.google.com/architecture/implementing-deployment-and-testing-strategies-on-gke#perform\\_an\\_ab\\_test](https://cloud.google.com/architecture/implementing-deployment-and-testing-strategies-on-gke#perform_an_ab_test)

i would say C:

To try this pattern, you perform the following steps:

Deploy the current version of the application (app:current) on the GKE cluster.

Deploy a new version of the application (app:new) alongside the current version.

Use Istio to route incoming requests that have the username test in the request's cookie to app:new. All other requests are routed to app:current.

✉️  **\_\_rajan\_\_**  7 months ago

**Selected Answer: C**

C is correct.

upvoted 1 times

✉️  **purushi** 8 months, 3 weeks ago

**Selected Answer: C**

C looks good since "send a small percentage of traffic to the Deployment that references the new version of the application" for A/B testing.  
D is close but not perfect for the said requirements.

upvoted 1 times

✉️  **zanhsieh** 10 months, 3 weeks ago

**Selected Answer: C**

C. The keywords, "A/B testing", "verified using a subset of production users", mean we need canary deployment.  
A: No. In-place deployment.  
B: No. This is Blue/Green deployment, but Ingress config (=manifest) does not have way to specify subset of traffic routing to different namespace.  
C: Yes.  
D: No, there's no mechanism on Ingress / Services manifests that can specify a subset of users, plus this is rolling update (=in-place deployment)

upvoted 2 times

✉️  **NewComer200** 12 months ago

**Selected Answer: C**

I couldn't find the wrong point in Option C.

And it's cool way.

I think in option B, some accidents possibly occur in the case the communication occurred between some microservices including new container.

upvoted 1 times

✉️  **TNT87** 1 year, 2 months ago

**Selected Answer: B**

Actually according to this link , its B

[https://cloud.google.com/kubernetes-engine/docs/tutorials/hello-app#deploying\\_a\\_new\\_version\\_of\\_the\\_sample\\_app](https://cloud.google.com/kubernetes-engine/docs/tutorials/hello-app#deploying_a_new_version_of_the_sample_app)

upvoted 1 times

✉️  **mrvergara** 1 year, 2 months ago

**Selected Answer: B**

This approach allows you to deploy new container images without downtime, as the traffic is only being redirected to the new namespace once the Deployment is ready. This also allows you to test and verify the new production release using a subset of production users by routing only a portion of the traffic to the new namespace.

upvoted 4 times

✉️  **mrvergara** 1 year, 2 months ago

Option D, which implements a rolling update pattern, can result in some downtime as Pods are gradually replaced with the new release version. While this approach can minimize the impact of any issues with the new release, it does not meet the requirement of "no downtime when new container images are deployed." Option D would be a suitable approach for situations where downtime is acceptable and can be managed, but it does not meet the requirements specified in this scenario.

upvoted 2 times

✉️  **TNT87** 1 year, 2 months ago

**Selected Answer: D**

<https://auth0.com/blog/deployment-strategies-in-kubernetes/>

Rolling updates are ideal because they allow you to deploy an application slowly with minimal overhead, minimal performance impact, and minimal

upvoted 1 times

Question #240

Topic 1

Your team manages a large Google Kubernetes Engine (GKE) cluster. Several application teams currently use the same namespace to develop microservices for the cluster. Your organization plans to onboard additional teams to create microservices. You need to configure multiple environments while ensuring the security and optimal performance of each team's work. You want to minimize cost and follow Google-recommended best practices. What should you do?

- A. Create new role-based access controls (RBAC) for each team in the existing cluster, and define resource quotas.
- B. Create a new namespace for each environment in the existing cluster, and define resource quotas.

- C. Create a new GKE cluster for each team.
- D. Create a new namespace for each team in the existing cluster, and define resource quotas.

**Correct Answer: A**

*Community vote distribution*

D (35%)

A (35%)

B (29%)

 **alpha\_canary** 2 weeks, 5 days ago

**Selected Answer: D**

D: Creating a new namespace for each team within the existing cluster and defining resource quotas is a good way to provide isolation, manage resources, and maintain security without incurring the cost of additional clusters.

Rejected:

- A: While RBAC can help manage access control, it doesn't provide the same level of resource isolation and management as using namespaces.
- B: Creating a namespace for each environment doesn't account for multiple teams working in the same environment.
- C: Creating a new GKE cluster for each team could lead to higher costs and complexity. It's more efficient to use namespaces within a single cluster for team isolation.

upvoted 1 times

 **edoo** 2 months, 1 week ago

**Selected Answer: D**

I'd like to say A, but namespacing is too important to be left aside.

I say D.

upvoted 2 times

 **\_rajan\_** 7 months ago

**Selected Answer: D**

I will go with D.

upvoted 1 times

 **kapara** 7 months, 3 weeks ago

**Selected Answer: B**

B is correct

upvoted 1 times

 **purush** 8 months, 3 weeks ago

**Selected Answer: A**

I go with A. Because of Security, low cost and Google-recommended best practices. I hope there is no need to create additional namespaces since several application teams are already use the same namespace to develop microservices for the cluster.

upvoted 1 times

 **phil\_thain** 10 months, 2 weeks ago

**Selected Answer: B**

Option B is the only one which addresses the part of the question that says 'You need to configure multiple environments'

upvoted 4 times

 **kapara** 7 months, 3 weeks ago

This is the correct answer as its the only one which addresses the question: "You need to configure multiple environments"

upvoted 1 times

 **NewComer200** 12 months ago

**Selected Answer: A**

I worried A or D.

I judged these teams are creating a microservice for each function on a large same application by the explain of "to develop microservices for the cluster".

If it's true, you don't need to separate using namespace.

I think the thing you should protect is resources, for example the spanner for development environment, the spanner for release environment and forbidden other team's spanner access.

In the case I think like that, I think this Q's answer is A.

upvoted 1 times

 closer89 1 year ago

**Selected Answer: A**

security

upvoted 1 times

 guruguru 1 year, 1 month ago

**Selected Answer: D**

for each team, hence need namespaces and quota

upvoted 2 times

 NewComer200 12 months ago

You could give the Role to user or user group.

upvoted 1 times

 Pime13 1 year, 2 months ago

**Selected Answer: A**

To configure more granular access to Kubernetes resources at the cluster level or within Kubernetes namespaces, you use Role-Based Access Control (RBAC). RBAC allows you to create detailed policies that define which operations and resources you allow users and service account access. With RBAC, you can control access for Google Accounts, Google Cloud service accounts, and Kubernetes service accounts. T

upvoted 2 times

 TNT87 1 year, 2 months ago

**Selected Answer: A**

<https://cloud.google.com/kubernetes-engine/docs/best-practices/rbac>

upvoted 1 times

Question #241

Topic 1

You have deployed a Java application to Cloud Run. Your application requires access to a database hosted on Cloud SQL. Due to regulatory requirements, your connection to the Cloud SQL instance must use its internal IP address. How should you configure the connectivity while following Google-recommended best practices?

- A. Configure your Cloud Run service with a Cloud SQL connection.
- B. Configure your Cloud Run service to use a Serverless VPC Access connector.
- C. Configure your application to use the Cloud SQL Java connector.
- D. Configure your application to connect to an instance of the Cloud SQL Auth proxy.

**Correct Answer: C**

*Community vote distribution*

B (86%)

14%

✉️  **alpha\_canary** 2 weeks, 5 days ago

**Selected Answer: B**

<https://cloud.google.com/sql/docs/mysql/connect-run#private-ip>

upvoted 1 times

✉️  **\_rajan\_** 7 months ago

**Selected Answer: B**

B is correct.

upvoted 1 times

✉️  **Maddyricky** 1 year, 2 months ago

**Selected Answer: B**

It should be B, EI faced this exact challenge in one of my projects

upvoted 3 times

✉️  **mrvergara** 1 year, 2 months ago

**Selected Answer: B**

Option B, using a Serverless VPC Access connector, is the recommended best practice for accessing a Cloud SQL instance from Cloud Run because it provides a secure and scalable way to connect to your internal resources.

With this option, you can connect your Cloud Run service to your internal VPC network, allowing it to access resources such as Cloud SQL instances that have internal IP addresses. This eliminates the need for a public IP address or a public network connection to your database, which can increase security and regulatory compliance.

upvoted 1 times

✉️  **mrvergara** 1 year, 2 months ago

Option A, configuring a Cloud SQL connection, is not possible because Cloud Run does not support direct connections to Cloud SQL instances.

Option C, using the Cloud SQL Java connector, is a valid way to connect to a Cloud SQL instance but does not provide the secure and scalable VPC connectivity that is recommended by Google.

Option D, connecting to an instance of the Cloud SQL Auth proxy, is a valid way to connect to a Cloud SQL instance, but it requires additional setup and maintenance, and may not be the most secure or scalable option, especially for large-scale deployments.

upvoted 1 times

✉️  **TNT87** 1 year, 2 months ago

**Selected Answer: C**

<https://cloud.google.com/sql/docs/mysql/connect-connectors#setup-and-usage>

If your application is written in Java you can skip this step, since you do this in the Java Cloud SQL Connector

upvoted 1 times

✉️  **mrvergara** 1 year, 2 months ago

<https://cloud.google.com/sql/docs/mysql/connect-run#vpc-access>

In this documentation, Google recommends using a Serverless VPC Access connector to connect to the internal IP address of a Cloud SQL instance, which is a secure and scalable way to access resources in a VPC network.

upvoted 2 times

✉️  **mrvergara** 1 year, 2 months ago

Option C, "Configure your application to use the Cloud SQL Java connector," is a valid option, but it is not recommended by Google as best practice. The Cloud SQL Java connector is designed to work with external IP addresses, and using it with an internal IP address can result in increased latency and potential security vulnerabilities.

Using a Serverless VPC Access connector to connect to the internal IP address, as suggested by option B, provides a more secure and performant solution. This method allows you to access the internal IP address of your Cloud SQL instance from a private network, bypassing the public internet, and avoiding exposure to security threats.

upvoted 3 times

✉️  **mathieu89** 1 year, 2 months ago

According doc tnt87 sent - SQL connectors can't provide a network path to a Cloud SQL instance if one is not already present.

upvoted 1 times

Your application stores customers' content in a Cloud Storage bucket, with each object being encrypted with the customer's encryption key. The key for each object in Cloud Storage is entered into your application by the customer. You discover that your application is receiving an HTTP 4xx error when reading the object from Cloud Storage. What is a possible cause of this error?

- A. You attempted the read operation on the object with the customer's base64-encoded key.
- B. You attempted the read operation without the base64-encoded SHA256 hash of the encryption key.
- C. You entered the same encryption algorithm specified by the customer when attempting the read operation.
- D. You attempted the read operation on the object with the base64-encoded SHA256 hash of the customer's key.

**Correct Answer: D***Community vote distribution*

B (65%)

C (24%)

12%

**molntamas** Highly Voted 1 year, 2 months ago**Selected Answer: B**

According to the documentation the SHA256 is needed in the REST API -> B  
<https://cloud.google.com/storage/docs/encryption/using-customer-supplied-keys#rest-csek-download-object>  
upvoted 5 times

**Kadhem** Most Recent 4 months ago**Selected Answer: B**

as some guys said, in the link <https://cloud.google.com/storage/docs/encryption/customer-supplied-keys#response> we understand why B is correct  
upvoted 1 times

**mohammeddigital** 4 months ago**Selected Answer: B**

B is correct.  
upvoted 1 times

**\_\_rajan\_\_** 7 months ago**Selected Answer: B**

B is correct.  
upvoted 1 times

**purushi** 8 months, 3 weeks ago**Selected Answer: B**

4xx is for Bad request, resource forbidden, not found and many more.  
If we want to read the object of Cloud storage bucket programmatically, then we need to pass the same customer key that was used for encrypting the object.

The request we need to send with Base64Encode ( SHA256 Hash (customer-key) )  
The key set for object is SHA256 Hash (customer-key) and while reading the Base64decode of the key will happen and comparing the Hash of the keys. If Hash are equal, then read access is permitted.

upvoted 1 times

👤 **Pime13** 1 year, 1 month ago  
took my exam yesterday (01-03-2023) and this question was there  
upvoted 2 times

👤 **markware** 10 months, 3 weeks ago  
what was the answer? did you pass?  
upvoted 1 times

👤 **markware** 10 months, 3 weeks ago  
I think its A  
upvoted 1 times

👤 **anukulk** 1 year, 2 months ago  
<https://cloud.google.com/storage/docs/encryption/customer-supplied-keys>  
upvoted 3 times

👤 **mrvergara** 1 year, 2 months ago

**Selected Answer: D**

Option D is a possible cause of an HTTP 4xx error when reading an object from Cloud Storage because it is incorrect to use the base64-encoded SHA256 hash of the customer's encryption key to read an encrypted object. To read an encrypted object, you need to use the original encryption key, not its hash. The HTTP 4xx error could be a result of an incorrect or unsupported key format, or a key mismatch. On the other hand, using the base64-encoded key (Option A), the encryption algorithm (Option C), or the base64-encoded SHA256 hash of the encryption key (Option B) without the original encryption key would not allow the object to be decrypted and read.

upvoted 2 times

👤 **mrvergara** 1 year, 2 months ago

The Google Cloud Storage documentation explains how to access objects in a bucket, including the use of an encryption key. The encryption key must be base64-encoded, and it is recommended to use the base64-encoded SHA256 hash of the encryption key for secure access to the objects.

Here's the link to the Google Cloud Storage documentation: <https://cloud.google.com/storage/docs/access-control/using-encryption-keys#using-base64-encoded-sha256-hashes-to-authenticate>

upvoted 1 times

👤 **Pime13** 1 year, 2 months ago

link do not exists :/  
upvoted 1 times

👤 **TNT87** 1 year, 2 months ago

**Selected Answer: B**

Answer B, made a mistake  
upvoted 2 times

👤 **TNT87** 1 year, 2 months ago

**Selected Answer: C**

You receive an HTTP 400 error in the following cases:

1. You upload an object using a customer-supplied encryption key, and you attempt to perform another operation on the object (other than requesting or updating most metadata or deleting the object) without providing the key.
2. You upload an object using a customer-supplied encryption key, and you attempt to perform another operation on the object with an incorrect key.
3. You upload an object without providing a customer-supplied encryption key, and you attempt to perform another operation on the object with a customer-supplied encryption key.
4. You specify an encryption algorithm, key, or SHA256 hash that is not valid.

Point number 2 has the answer

<https://cloud.google.com/storage/docs/encryption/customer-supplied-keys#response>

upvoted 4 times

👤 **TNT87** 1 year, 2 months ago

typo , its B not C  
upvoted 1 times

You have two Google Cloud projects, named Project A and Project B. You need to create a Cloud Function in Project A that saves the output in a Cloud Storage bucket in Project B. You want to follow the principle of least privilege. What should you do?

- A. 1. Create a Google service account in Project B.  
2. Deploy the Cloud Function with the service account in Project A.  
3. Assign this service account the roles/storage.objectCreator role on the storage bucket residing in Project B.
- B. 1. Create a Google service account in Project A  
2. Deploy the Cloud Function with the service account in Project A.  
3. Assign this service account the roles/storage.objectCreator role on the storage bucket residing in Project B.
- C. 1. Determine the default App Engine service account (PROJECT\_ID@appspot.gserviceaccount.com) in Project A.  
2. Deploy the Cloud Function with the default App Engine service account in Project A.  
3. Assign the default App Engine service account the roles/storage.objectCreator role on the storage bucket residing in Project B.
- D. 1. Determine the default App Engine service account (PROJECT\_ID@appspot.gserviceaccount.com) in Project B.  
2. Deploy the Cloud Function with the default App Engine service account in Project A.  
3. Assign the default App Engine service account the roles/storage.objectCreator role on the storage bucket residing in Project B.

**Correct Answer: C***Community vote distribution*

B (75%)

A (17%)

8%

 **alpha\_canary** 2 weeks, 5 days ago

**Selected Answer: B**

quite straightforward  
upvoted 1 times

 **\_rajan\_** 7 months ago

**Selected Answer: B**

B is correct.  
upvoted 1 times

 **\_rajan\_** 7 months ago

**Selected Answer: B**

B is correct.  
upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: B**

B is correct. Simple and straight forward.  
Create SA in Project A, Assign SA the role of object creator to push objects to Cloud bucket in Project B.  
upvoted 1 times

 **Pime13** 1 year, 1 month ago

took my exam yesterday (01-03-2023) and this question was there  
upvoted 4 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: B**

it's B.

<https://articles.wesisionary.team/multi-project-account-service-account-in-gcp-ba8f8821347e>

upvoted 2 times

 **mrvergara** 1 year, 2 months ago

**Selected Answer: B**

A is not correct because you cannot run a Cloud Function with a service account that is not in the same Google Cloud project.  
B is correct because it follows the least privilege principle and for a Cloud Function, the service account must be created in the same project where the function is getting executed.

upvoted 3 times

 **anukulk** 1 year, 2 months ago

option B is right. We have permissions to object creation in project for the SA created in project A. <https://www.youtube.com/watch?v=ctACCk80H-w>

upvoted 2 times

 **mrvergara** 1 year, 2 months ago

**Selected Answer: A**

In option B, a service account is created in Project A, but this service account would have access to all the resources within Project A, which is more than is necessary for the task of saving output to a storage bucket in Project B.

Options C and D use the default App Engine service account, which would have more permissions than necessary, as it would have access to App Engine resources within Project A or B, rather than just the permissions needed for the task of saving output to a storage bucket in Project B.

upvoted 2 times

 **TNT87** 1 year, 2 months ago

No it can't be A, check the link provided below please. It can't be A, there is no way

upvoted 1 times

 **mrvergara** 1 year, 2 months ago

[https://cloud.google.com/docs/authentication/production#providing\\_credentials\\_to\\_your\\_application](https://cloud.google.com/docs/authentication/production#providing_credentials_to_your_application)

In this guide, it explains the best practice for providing authentication credentials to your application. By creating a separate Google service account in the project that owns the resource you want to access (in this case, Project B), and then using that service account to perform actions on the resource (writing to the Cloud Storage bucket in Project B), you are following the principle of least privilege. This means that you are granting the minimum permissions necessary to perform the desired action.

upvoted 1 times

 **TNT87** 1 year, 2 months ago

Anyway I passed my exam last week

upvoted 1 times

 **mrvergara** 1 year, 2 months ago

Congrats, this time you are right. The answer is option B

upvoted 1 times

 **mrvergara** 1 year, 2 months ago

It is the B option

upvoted 1 times

 **TNT87** 1 year, 2 months ago

**Selected Answer: C**

Question #244

Topic 1

A governmental regulation was recently passed that affects your application. For compliance purposes, you are now required to send a duplicate of specific application logs from your application's project to a project that is restricted to the security team. What should you do?

- A. Create user-defined log buckets in the security team's project. Configure a Cloud Logging sink to route your application's logs to log buckets in the security team's project.

- B. Create a job that copies the logs from the \_Required log bucket into the security team's log bucket in their project.
- C. Modify the \_Default log bucket sink rules to reroute the logs into the security team's log bucket.
- D. Create a job that copies the System Event logs from the \_Required log bucket into the security team's log bucket in their project.

**Correct Answer: B**

*Community vote distribution*

A (100%)

 **\_\_rajan\_\_** 7 months ago

**Selected Answer: A**

A is correct.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: A**

I go with A.

This question is to test Cloud Logging Sink feature.

upvoted 1 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: A**

i also choose A. <https://cloud.google.com/architecture/security-log-analytics>

upvoted 2 times

 **mrvergara** 1 year, 2 months ago

**Selected Answer: A**

I choose option A because it provides a direct and automated solution for duplicating the specific application logs and sending them to the security team's project. This method uses Cloud Logging's sink feature, which is a powerful tool for routing logs to other destinations, such as log buckets or Pub/Sub topics. By using a sink, you can ensure that the duplication of logs is performed in real-time and automatically, which would minimize manual intervention and minimize the risk of errors.

upvoted 3 times

You plan to deploy a new Go application to Cloud Run. The source code is stored in Cloud Source Repositories. You need to configure a fully managed, automated, continuous deployment pipeline that runs when a source code commit is made. You want to use the simplest deployment solution. What should you do?

- A. Configure a cron job on your workstations to periodically run gcloud run deploy --source in the working directory.
- B. Configure a Jenkins trigger to run the container build and deploy process for each source code commit to Cloud Source Repositories.
- C. Configure continuous deployment of new revisions from a source repository for Cloud Run using buildpacks.
- D. Use Cloud Build with a trigger configured to run the container build and deploy process for each source code commit to Cloud Source Repositories.

**Correct Answer: D**

*Community vote distribution*

D (83%)

C (17%)

 **\_\_rajan\_\_** 7 months ago

**Selected Answer: D**

D is correct.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: D**

D is more suitable since we need "simplest deployment solution".

C is close but it is limited to only building the image and pushing that into artifact registry. It donot take part in deployment.

B is also close but it takes more work than D.

upvoted 1 times

Question #246

Topic 1

Your team has created an application that is hosted on a Google Kubernetes Engine (GKE) cluster. You need to connect the application to a legacy REST service that is deployed in two GKE clusters in two different regions. You want to connect your application to the target service in a way that is resilient. You also want to be able to run health checks on the legacy service on a separate port. How should you set up the connection? (Choose two.)

- A. Use Traffic Director with a sidecar proxy to connect the application to the service.
- B. Use a proxyless Traffic Director configuration to connect the application to the service.
- C. Configure the legacy service's firewall to allow health checks originating from the proxy.
- D. Configure the legacy service's firewall to allow health checks originating from the application.
- E. Configure the legacy service's firewall to allow health checks originating from the Traffic Director control plane.

**Correct Answer: AC**

*Community vote distribution*

AC (100%)

 **\_\_rajan\_\_** 7 months ago

**Selected Answer: AC**

AC are correct.

upvoted 1 times

 **Pime13** 1 year, 1 month ago

took my exam yesterday (01-03-2023) and this question was there

upvoted 3 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: AC**

i agree, AC

upvoted 1 times

 **mrvergara** 1 year, 2 months ago

**Selected Answer: AC**

A. Using Traffic Director with a sidecar proxy can provide resilience for your application by allowing for failover to the secondary region in the event of an outage. The sidecar proxy can route traffic to the legacy service in either of the two GKE clusters, ensuring high availability.

Question #247

Topic 1

You have an application running in a production Google Kubernetes Engine (GKE) cluster. You use Cloud Deploy to automatically deploy your application to your production GKE cluster. As part of your development process, you are planning to make frequent changes to the application's source code and need to select the tools to test the changes before pushing them to your remote source code repository. Your toolset must meet the following requirements:

- Test frequent local changes automatically.
- Local deployment emulates production deployment.

Which tools should you use to test building and running a container on your laptop using minimal resources?

A. Docker Compose and dockerd

B. Terraform and kubeadm

C. Minikube and Skaffold

D. kaniko and Tekton

**Correct Answer: C**

*Community vote distribution*

C (100%)

✉️  **tesix79748** 5 months ago

How is this even related to GCP

upvoted 2 times

✉️  **\_rajan\_** 7 months ago

**Selected Answer: C**

Minikube is a tool for running Kubernetes locally on your laptop. Skaffold is a tool for scaffolding, building, and deploying Kubernetes applications.

upvoted 1 times

✉️  **purushি** 8 months, 3 weeks ago

**Selected Answer: C**

C is the correct choice. Since GKE local environment is required, Minikube and scaffold are right choices.

upvoted 1 times

✉️  **purushি** 8 months, 3 weeks ago

Tilt and Octant are also very good local development tools to test K8S applications.

upvoted 1 times

✉️  **Pime13** 1 year, 1 month ago

took my exam yesterday (01-03-2023) and this question was there

upvoted 4 times

✉️  **mrvergara** 1 year, 2 months ago

**Selected Answer: C**

Minikube is a tool that runs a single-node Kubernetes cluster locally on your laptop, allowing you to test and run your application on a simulated production environment. Skaffold is a command line tool that automates the process of building and deploying your application to a local or remote Kubernetes cluster.

Together, Minikube and Skaffold allow you to test your frequent changes locally, with a deployment that emulates a production environment, using minimal resources. Minikube provides the simulated production environment, while Skaffold takes care of building and deploying your application, making the development process smoother and more efficient.

upvoted 3 times

✉️  **TNT87** 1 year, 2 months ago

**Selected Answer: C**

Answer C

Minikube is a lightweight Kubernetes implementation that creates a VM on your local machine and deploys a simple cluster containing only one node. Minikube is available for Linux, macOS, and Windows systems.

Skaffold is a tool that handles the workflow for building, pushing and deploying your application. You can use Skaffold to easily configure a local development workspace, streamline your inner development loop, and integrate with other tools such as Kustomize and Helm to help manage your Kubernetes manifests

upvoted 1 times

Question #248

Topic 1

You are deploying a Python application to Cloud Run using Cloud Source Repositories and Cloud Build. The Cloud Build pipeline is shown below:

```
steps:
- name: python
  entrypoint: pip
  args: ["install", "-r", "requirements.txt", "--user"]

- name: 'gcr.io/cloud-builders/docker'
  args: ['build', '-t',
         'us-central1-docker.pkg.dev/${PROJECT_ID}/${_REPO_NAME}/myimage:${SHORT_SHA}',

...]
```

```

'.']

- name: 'gcr.io/cloud-builders/docker'
  args: ['push', 'us-central1-'
docker.pkg.dev/${PROJECT_ID}/${_REPO_NAME}/myimage:${SHORT_SHA}']

- name: google/cloud-sdk
  args: ['gcloud', 'run', 'deploy', 'helloworld-${SHORT_SHA}',
         '--image=us-central1-'
docker.pkg.dev/${PROJECT_ID}/${_REPO_NAME}/myimage:${SHORT_SHA}',
         '--region', 'us-central1', '--platform', 'managed',
         '--allow-unauthenticated']

```

You want to optimize deployment times and avoid unnecessary steps. What should you do?

- A. Remove the step that pushes the container to Artifact Registry.
- B. Deploy a new Docker registry in a VPC, and use Cloud Build worker pools inside the VPC to run the build pipeline.
- C. Store image artifacts in a Cloud Storage bucket in the same region as the Cloud Run instance.
- D. Add the --cache-from argument to the Docker build step in your build config file.

**Correct Answer: D**

*Community vote distribution*

D (100%)

✉  **\_\_rajan\_\_** 7 months ago

**Selected Answer: D**

D is correct.

upvoted 1 times

✉  **purushi** 8 months, 3 weeks ago

**Selected Answer: D**

Use local cached image to save build time.

upvoted 1 times

✉  **Pime13** 1 year, 2 months ago

**Selected Answer: D**

[https://cloud.google.com/build/docs/optimize-builds/speeding-up-builds#using\\_a\\_cached\\_docker\\_image](https://cloud.google.com/build/docs/optimize-builds/speeding-up-builds#using_a_cached_docker_image)

upvoted 1 times

✉  **mrvergara** 1 year, 2 months ago

**Selected Answer: D**

Option D, adding the --cache-from argument to the Docker build step in the build config file, would be the best option to optimize deployment times.

The --cache-from argument allows you to specify a list of images that Docker should use as a cache source when building the image. If a layer in the current build matches a layer in one of the cache source images, Docker uses the cached layer instead of building it again, reducing the build time.

Options A and C may not have a significant impact on deployment times, and option B would likely add complexity and increase deployment times, as it would require deploying and managing a new Docker registry and using a VPC-based Cloud Build worker pool.

upvoted 1 times

✉  **TNT87** 1 year, 2 months ago

**Selected Answer: D**

[https://cloud.google.com/build/docs/optimize-builds/speeding-up-builds#using\\_a\\_cached\\_docker\\_image](https://cloud.google.com/build/docs/optimize-builds/speeding-up-builds#using_a_cached_docker_image)

upvoted 1 times

You are developing an event-driven application. You have created a topic to receive messages sent to Pub/Sub. You want those messages to be processed in real time. You need the application to be independent from any other system and only incur costs when new messages arrive. How should you configure the architecture?

- A. Deploy the application on Compute Engine. Use a Pub/Sub push subscription to process new messages in the topic.
- B. Deploy your code on Cloud Functions. Use a Pub/Sub trigger to invoke the Cloud Function. Use the Pub/Sub API to create a pull subscription to the Pub/Sub topic and read messages from it.
- C. Deploy the application on Google Kubernetes Engine. Use the Pub/Sub API to create a pull subscription to the Pub/Sub topic and read messages from it.
- D. Deploy your code on Cloud Functions. Use a Pub/Sub trigger to handle new messages in the topic.

**Correct Answer: B**

*Community vote distribution*

B (50%)

D (50%)

✉  **alpha\_canary** 2 weeks, 4 days ago

**Selected Answer: D**

D: Deploying your code on Cloud Functions and using a Pub/Sub trigger to handle new messages in the topic allows for a real-time, event-driven architecture. Cloud Functions only incur costs when invoked, which aligns with the requirement to only incur costs when new messages arrive.

B: With Cloud Functions, there's no need to manually create a pull subscription. The Pub/Sub trigger handles the message retrieval.  
upvoted 1 times

✉  **JonathanSJ** 2 months, 3 weeks ago

**Selected Answer: D**

I will go for D.

upvoted 1 times

✉  **examprof** 4 months, 3 weeks ago

Alternative D is correct.

A "push subscription" (not "pull") is more suitable when messages must be processed in real-time. Message ingested in the Pub/Sub topic, message pushed and retried recurrently until acknowledged.

upvoted 1 times

✉  **Raghunanda** 6 months, 3 weeks ago

**Selected Answer: D**

Not sure why we are complicating!! D is the right option

upvoted 1 times

✉  **\_\_rajan\_\_** 7 months ago

**Selected Answer: D**

I would go with D.

upvoted 1 times

✉  **purushi** 8 months, 3 weeks ago

**Selected Answer: B**

B is a very detailed answer and it is a right choice.

D is missing info like cloud function to subscribe pub sub topic to handle new messages.

upvoted 2 times

✉️  **NewComer200** 12 months ago

**Selected Answer: D**

Selected Answer:D

<https://cloud.google.com/functions/docs/calling/pubsub>

We selected D based on our experience with Cloud Functions and the material at the URL above.

Since messages can be obtained from Cloud Functions arguments, we are not aware of the description of Subscription.

"only incur costs when new messages arrive." so it's OK to process on the trigger.

I don't think real time means so strictly.

For the life of me, I can't find any reason why D is wrong, and it seems to me that B is an error because of the extra processing.

upvoted 4 times

✉️  **NewComer200** 12 months ago

Selected Answer:D

<https://cloud.google.com/functions/docs/calling/pubsub>

We selected D based on our experience with Cloud Functions and the material at the URL above.

Since messages can be obtained from Cloud Functions arguments, we are not aware of the description of Subscription.

upvoted 2 times

✉️  **Pime13** 1 year, 1 month ago

took my exam yesterday (01-03-2023) and this question was there

upvoted 3 times

✉️  **imiu** 4 months, 4 weeks ago

and what is the answer? option D?

upvoted 1 times

✉️  **mrvergara** 1 year, 2 months ago

**Selected Answer: B**

Option D is not ideal because using a Pub/Sub trigger to handle new messages in a topic is not the most efficient way to process messages in real time. In a trigger-based architecture, Cloud Functions are invoked only when new messages are available, so there is a possibility of delay processing.

On the other hand, Option B provides a more efficient architecture for real-time processing. A Cloud Function is invoked for each message received in the Pub/Sub topic, providing immediate processing as messages arrive. This way, the application is independent from any other system and incurs costs only when new messages arrive, fulfilling the requirements stated in the question.

upvoted 4 times

✉️  **TNT87** 1 year, 2 months ago

**Selected Answer: B**

<https://cloud.google.com/solutions/event-driven-architecture-pubsub>

upvoted 2 times

Question #250

Topic 1

You have an application running on Google Kubernetes Engine (GKE). The application is currently using a logging library and is outputting to standard output. You need to export the logs to Cloud Logging, and you need the logs to include metadata about each request. You want to use the simplest method to accomplish this. What should you do?

- A. Change your application's logging library to the Cloud Logging library, and configure your application to export logs to Cloud Logging.
- B. Update your application to output logs in JSON format, and add the necessary metadata to the JSON.
- C. Update your application to output logs in CSV format, and add the necessary metadata to the CSV.
- D. Install the Fluent Bit agent on each of your GKE nodes, and have the agent export all logs from /var/log.

**Correct Answer: C**

*Community vote distribution*

A (67%)

B (25%)

8%

✉️  **aldi22** Highly Voted 1 year ago

The answer is B since GKE is integrated with Cloud Logging by default.

"By default, GKE clusters are natively integrated with Cloud Logging (and Monitoring). When you create a GKE cluster, both Monitoring and Cloud Logging are enabled by default."

"GKE deploys a per-node logging agent that reads container logs, adds helpful metadata, and then sends the logs to the logs router, which sends the logs to Cloud Logging and any of the Logging sink destinations that you have configured. Cloud Logging stores logs for the duration that you specify or 30 days by default. Because Cloud Logging automatically collects standard output and error logs for containerized processes you can start viewing your logs as soon as your application is deployed."

Source: <https://cloud.google.com/blog/products/management-tools/using-logging-your-apps-running-kubernetes-engine>  
upvoted 12 times

✉️  **JonathanSJ** Most Recent 2 months, 3 weeks ago

**Selected Answer: B**

I will go for B.

In Google Kubernetes Engine (GKE), the standard output (stdout) of containers is automatically sent to Cloud Logging. This means that if your application in GKE prints logs to standard output, these logs will be captured and can be viewed in Cloud Logging without additional configuration.

And if the logs are in JSON is better for processing.

Option A is irrelevant because the logs have been sent already to cloud logging via standard output.

upvoted 2 times

✉️  **Kadhem** 4 months ago

**Selected Answer: A**

since we need to update the application, the best solution between A, B and C is A.

upvoted 1 times

✉️  **82e0b6209c** 4 months, 3 weeks ago

**Selected Answer: B**

B for me: we're looking for the simplest method and I feel it's easier to configure the existing library to output JSON and include some context metadata rather than changing every log statement to use Cloud Logging library.

upvoted 1 times

✉️  **purush** 8 months, 3 weeks ago

**Selected Answer: A**

The key here is "use the simplest method to accomplish this...", using Cloud logging library is a very simple and straight forward solution. If the app is running on the single and multiple VMs in a instance group, then installing the cloud logging agent must be the correct answer. This environment is GKE cluster and separate some normal VM workflow.

upvoted 1 times

✉️  **82e0b6209c** 4 months, 3 weeks ago

How is it simpler to change every logging statement to use a different library rather than configuring the existing one to output in JSON and automatically append context metadata? I'd go for B

upvoted 1 times

✉️  **closer89** 1 year ago

**Selected Answer: A**

to log request metadata

[https://cloud.google.com/logging/docs/reference/libraries#write\\_request\\_logs](https://cloud.google.com/logging/docs/reference/libraries#write_request_logs)

upvoted 1 times

✉️  **Pime13** 1 year, 1 month ago

took my exam yesterday (01-03-2023) and this question was there

upvoted 2 times

✉️  **Pime13** 1 year, 2 months ago

**Selected Answer: A**

When you write logs from your service or job, they will be picked up automatically by Cloud Logging so long as the logs are written to any of these locations:

Standard output (stdout) or standard error (stderr) streams

Any files under the /var/log directory

syslog (/dev/log)

Logs written using Cloud Logging client libraries, which are available for many popular languages

<https://cloud.google.com/run/docs/logging#container-logs>

upvoted 1 times

✉️  **Pime13** 1 year, 2 months ago

[https://cloud.google.com/stackdriver/docs/solutions/gke/managing-logs#what\\_logs](https://cloud.google.com/stackdriver/docs/solutions/gke/managing-logs#what_logs)

upvoted 1 times

✉️  **mrvergara** 1 year, 2 months ago

**Selected Answer: A**

Option D, installing the Fluent Bit agent on each of your GKE nodes, is not the most straightforward method for exporting logs to Cloud Logging as it requires manual configuration and management of the Fluent Bit agent. While Fluent Bit can be used to collect and forward logs to Cloud Logging, it is typically used for more complex logging scenarios where custom log processing is required.

Using the Cloud Logging library, as described in Option A, is a simpler and more direct method for exporting logs to Cloud Logging, as it eliminates the need to manage an additional log agent and provides a more integrated solution for logging in a GKE environment.

upvoted 4 times

✉️  **TNT87** 1 year, 2 months ago

<https://cloud.google.com/blog/products/management-tools/using-logging-your-apps-running-kubernetes-engine>

upvoted 1 times

✉️  **TNT87** 1 year, 2 months ago

**Selected Answer: D**

<https://cloud.google.com/run/docs/logging#container-logs>

upvoted 1 times

✉️  **TNT87** 1 year, 2 months ago

Answer A not D

upvoted 2 times

Question #251

Topic 1

You are working on a new application that is deployed on Cloud Run and uses Cloud Functions. Each time new features are added, new Cloud Functions and Cloud Run services are deployed. You use ENV variables to keep track of the services and enable interservice communication, but the maintenance of the ENV variables has become difficult. You want to implement dynamic discovery in a scalable way. What should you do?

- A. Configure your microservices to use the Cloud Run Admin and Cloud Functions APIs to query for deployed Cloud Run services and Cloud Functions in the Google Cloud project.
- B. Create a Service Directory namespace. Use API calls to register the services during deployment, and query during runtime.
- C. Rename the Cloud Functions and Cloud Run services endpoint using a well-documented naming convention.
- D. Deploy Hashicorp Consul on a single Compute Engine instance. Register the services with Consul during deployment, and query during runtime.

**Correct Answer: C**

*Community vote distribution*

B (100%)

 **\_rajan\_** 7 months ago

**Selected Answer: B**

B is correct.

upvoted 1 times

 **purushি** 8 months, 3 weeks ago

**Selected Answer: B**

Creating a service registry is a right choice. B is correct.

One more way is to write the new service urls to the config server registry so that other application/services can fetch those urls dynamically & and when required.

upvoted 1 times

 **purushি** 8 months, 3 weeks ago

One example of creating service directory to use in subsequent MS calls is seen in Microservice Orchestration Design principles and patte

upvoted 1 times

 **Pime13** 1 year, 1 month ago

took my exam yesterday (01-03-2023) and this question was there

upvoted 2 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: B**

service directory for registration and discovery of services

upvoted 2 times

 **mrvergara** 1 year, 2 months ago

**Selected Answer: B**

Service Directory provides a scalable way to manage the registration and discovery of services. By creating a namespace, you can use API calls to register your Cloud Run and Cloud Functions services, and query them during runtime. This allows for dynamic discovery and eliminates the need for manually updating environment variables. Service Directory also provides features such as service health checks and metadata, which can be used to further improve the reliability and scalability of your application.

upvoted 2 times

 **TNT87** 1 year, 2 months ago

**Selected Answer: B**

<https://medium.com/google-cloud/fine-grained-cloud-dns-iam-via-service-directory-446058b4362e>

<https://cloud.google.com/service-directory/docs/overview>

upvoted 2 times

You work for a financial services company that has a container-first approach. Your team develops microservices applications. A Cloud Build pipeline creates the container image, runs regression tests, and publishes the image to Artifact Registry. You need to ensure that only containers that have passed the regression tests are deployed to Google Kubernetes Engine (GKE) clusters. You have already enabled Binary Authorization on the GKE clusters. What should you do next?

- A. Create an attester and a policy. After a container image has successfully passed the regression tests, use Cloud Build to run Kritis Signer to create an attestation for the container image.
- B. Deploy Voucher Server and Voucher Client components. After a container image has successfully passed the regression tests, run Voucher Client as a step in the Cloud Build pipeline.
- C. Set the Pod Security Standard level to Restricted for the relevant namespaces. Use Cloud Build to digitally sign the container images that have passed the regression tests.
- D. Create an attester and a policy. Create an attestation for the container images that have passed the regression tests as a step in the Cloud Build pipeline.

**Correct Answer: A**

*Community vote distribution*

A (64%)

D (27%)

9%

 **JonathanSJ** 2 months, 3 weeks ago

**Selected Answer: D**

I will go for D.

D: The next step, after enable Binary Auth, is creating an attester and a policy and then configure the attestation step in the cloud build pipeline.

Not A because when you use kritis to sign an image you must provide the private key file from the attester. And for that you must save the prikey when you create the attester for it later use. Its more complicated.

Not C because pod security standard level to restricted don't enforce the use of signed images.

upvoted 3 times

 **JonathanSJ** 2 months, 3 weeks ago

With option D the cloud build step could looks like:

```
- name: 'gcr.io/cloud-builders/gcloud'
entrypoint: 'bash'
args: [ '-c', 'gcloud container binauthz create-signature --artifact-url gcr.io/<PROJECT_ID>/<IMAGE_NAME>:signed --attestor
<ATTESTOR_NAME> --keyversion <KEY_VERSION> --project <PROJECT_ID>' ]
upvoted 1 times
```

 **\_\_rajan\_\_** 7 months ago

**Selected Answer: A**

A is correct.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: A**

I go with A since it is detailed and more specific about Kritis digital signature.

upvoted 1 times

zanhsieh 10 months, 3 weeks ago

Selected Answer: A

A. For folks wonder what differences between Kritis Signer and Voucher Server Voucher Client, I asked Google Bard about it. Bard stated Kritis Signer is a command-line tools, whereas Voucher Server Voucher Client is a web-based tool. I then tried to verify that with Google search and Google image search (search "voucher server voucher client" then click Images). It seems Bard report correctly. Someone even wrote a Kritis Signer integrated pipeline with terraform (<https://xebia.com/blog/how-to-automate-the-kritis-signer-on-google-cloud-platform/>). Also, yes, both Kritis Signer and Voucher Server Voucher Client have Google official documentations. However, if you look carefully on Voucher Server Voucher Client Google official doc, they use curl to the Voucher Server address, which indirectly prove Voucher Server Voucher Client is a web-based tool.

upvoted 1 times

closer89 1 year ago

Selected Answer: C

question is not about checking vulnerabilities.

its not A. The Kritis Signer is a command-line utility to check whether an image violates the policy on security vulnerabilities.  
its not a voucher too.

upvoted 1 times

closer89 1 year ago

its D definitely

<https://cloud.google.com/binary-authorization/docs/cloud-build>

upvoted 2 times

Pime13 1 year, 1 month ago

took my exam yesterday (01-03-2023) and this question was there

upvoted 3 times

Pime13 1 year, 2 months ago

info on voucher server: <https://cloud.google.com/binary-authorization/docs/creating-attestations-voucher>

upvoted 2 times

Pime13 1 year, 2 months ago

Selected Answer: A

Kritis Signer is an open source command-line tool that can create Binary Authorization attestations based on a policy that you configure. You also use Kritis Signer to create attestations after checking an image for vulnerabilities identified by Container Analysis.

<https://cloud.google.com/binary-authorization/docs/creating-attestations-kritis>

upvoted 1 times

mrvergara 1 year, 2 months ago

Selected Answer: A

Binary Authorization in GKE provides a way to enforce that only verified container images are deployed in a cluster. In this scenario, to ensure that only containers that have passed the regression tests are deployed, you would create an attester and a policy in Binary Authorization, and use Kritis Signer to create an attestation for the container image after it has passed the tests. The attestation verifies that the image meets the policy's criteria and is authorized to be deployed. This provides a secure and automated way to enforce that only containers that have passed the required tests are deployed in the cluster.

upvoted 1 times

mrvergara 1 year, 2 months ago

Kritis Signer is a component of the Kritis project, which is an open-source implementation of Binary Authorization for Kubernetes. Kritis Signer is used to sign container images and create attestations, which verify that the image meets the criteria specified in a Binary Authorization policy. These attestations can be used to enforce that only authorized containers are deployed in a cluster, providing an additional layer of security for your containerized applications.

upvoted 2 times

TNT87 1 year, 2 months ago

Selected Answer: A

<https://cloud.google.com/binary-authorization/docs/creating-attestations-kritis>

upvoted 2 times

You are reviewing and updating your Cloud Build steps to adhere to best practices. Currently, your build steps include:

1. Pull the source code from a source repository.
2. Build a container image
3. Upload the built image to Artifact Registry.

You need to add a step to perform a vulnerability scan of the built container image, and you want the results of the scan to be available to your deployment pipeline running in Google Cloud. You want to minimize changes that could disrupt other teams' processes. What should you do?

- A. Enable Binary Authorization, and configure it to attest that no vulnerabilities exist in a container image.
- B. Upload the built container images to your Docker Hub instance, and scan them for vulnerabilities.
- C. Enable the Container Scanning API in Artifact Registry, and scan the built container images for vulnerabilities.
- D. Add Artifact Registry to your Aqua Security instance, and scan the built container images for vulnerabilities.

**Correct Answer: D**

*Community vote distribution*

C (86%)

14%

 **wanrltw** 4 months, 1 week ago

**Selected Answer: A**

I'm not so sure about C because the task is to add a STEP to our Cloud Build pipeline to perform the vulnerability scan, whereas C implies me doing the job via Cloud Console. Why would we enable the Container Scanning API in Artifact Registry every time we run the pipeline?

This scenario is similar to what we have in question #252. I'd go with A:  
<https://cloud.google.com/binary-authorization/docs/creating-attestations-kritis>

upvoted 1 times

 **\_rajan\_** 7 months ago

**Selected Answer: C**

C is correct.

upvoted 1 times

 **purushti** 8 months, 3 weeks ago

**Selected Answer: C**

C is right. Requirement is to perform a vulnerability scan of the built container image.

C states Enable the Container Scanning API in Artifact Registry, and scan the built container images for vulnerabilities. Further steps for better security would be to follow option A.

upvoted 1 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: C**

i choose C

upvoted 2 times

 **mrvergara** 1 year, 2 months ago

**Selected Answer: C**

Enabling the Container Scanning API in Artifact Registry and scanning the built container images is a best practice because it allows you to perform security scans within the same environment where the built images are stored. This helps minimize the changes that could disrupt other teams' processes, as the images are already in Artifact Registry, and the scanning results can be easily accessed by the deployment pipeline Google Cloud. Additionally, the Container Scanning API integrates with Google Cloud security and governance tools, allowing you to enforce security policies and manage vulnerabilities in a centralized and automated way.

upvoted 1 times

 **TNT87** 1 year, 2 months ago

**Selected Answer: C**

<https://cloud.google.com/container-analysis/docs/automated-scanning#automating-the-image-vulnerability-scan>

Question #254

Topic 1

You are developing an online gaming platform as a microservices application on Google Kubernetes Engine (GKE). Users on social media are complaining about long loading times for certain URL requests to the application. You need to investigate performance bottlenecks in the application and identify which HTTP requests have a significantly high latency span in user requests. What should you do?

- A. Configure GKE workload metrics using kubectl. Select all Pods to send their metrics to Cloud Monitoring. Create a custom dashboard of application metrics in Cloud Monitoring to determine performance bottlenecks of your GKE cluster.
- B. Update your microservices to log HTTP request methods and URL paths to STDOUT. Use the logs router to send container logs to Cloud Logging. Create filters in Cloud Logging to evaluate the latency of user requests across different methods and URL paths.
- C. Instrument your microservices by installing the OpenTelemetry tracing package. Update your application code to send traces to Trace for inspection and analysis. Create an analysis report on Trace to analyze user requests.
- D. Install tcpdump on your GKE nodes. Run tcpdump to capture network traffic over an extended period of time to collect data. Analyze the data files using Wireshark to determine the cause of high latency.

**Correct Answer: A**

*Community vote distribution*

C (80%)

A (20%)

 **alpha\_canary** 2 weeks, 4 days ago

**Selected Answer: C**

<https://cloud.google.com/trace/docs/setup/python-ot>

upvoted 1 times

 **\_rajan\_\_** 7 months ago

**Selected Answer: C**

This approach allows you to update your application code to send traces to Trace for inspection and analysis. You can then create an analysis report on Trace to analyze user requests. This will help you identify which HTTP requests have a significantly high latency span in user requests which seems to be the main concern according to the complaints from users on social media.

upvoted 1 times

 **purushi** 8 months, 3 weeks ago

**Selected Answer: C**

There is no best fit other than C here.

upvoted 1 times

 **Writer** 1 year ago

**Selected Answer: C**

This is the best way to investigate performance bottlenecks in a microservices application. By using OpenTelemetry, you can collect traces from all of your microservices and analyze them in Trace. This will allow you to identify which requests are taking the longest and where the bottlenecks are occurring.

upvoted 2 times

 **Pime13** 1 year, 1 month ago

took my exam yesterday (01-03-2023) and this question was there

upvoted 2 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: C**

correcting my choice

upvoted 1 times

 **Pime13** 1 year, 2 months ago

**Selected Answer: A**

question clearly says: performance bottlenecks and which step is having latency ---> Cloud Trace

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

upvoted 1 times

 **Pime13** 1 year, 2 months ago

i selected the wrong, it's C

upvoted 1 times

 **TNT87** 1 year, 2 months ago

**Selected Answer: C**

<https://cloud.google.com/trace/docs/setup#when-to-instrument>

upvoted 1 times

 **mrvergara** 1 year, 2 months ago

**Selected Answer: C**

Instrumenting your microservices with the OpenTelemetry tracing package, updating your application code to send traces to Trace for inspection and analysis, and creating an analysis report on Trace would be the recommended solution for investigating performance bottlenecks in the application and identifying HTTP requests with high latency. This would allow you to visualize and analyze the complete request-response cycle and identify specific parts of the application that might be contributing to long loading times.

upvoted 1 times

 **TNT87** 1 year, 2 months ago

**Selected Answer: A**

<https://cloud.google.com/stackdriver/docs/solutions/gke/workload-metrics>

upvoted 1 times

You need to load-test a set of REST API endpoints that are deployed to Cloud Run. The API responds to HTTP POST requests. Your load tests must meet the following requirements:

- Load is initiated from multiple parallel threads.
- User traffic to the API originates from multiple source IP addresses.
- Load can be scaled up using additional test instances.

You want to follow Google-recommended best practices. How should you configure the load testing?

- A. Create an image that has cURL installed, and configure cURL to run a test plan. Deploy the image in a managed instance group, and run one instance of the image for each VM.
- B. Create an image that has cURL installed, and configure cURL to run a test plan. Deploy the image in an unmanaged instance group, and run one instance of the image for each VM.
- C. Deploy a distributed load testing framework on a private Google Kubernetes Engine cluster. Deploy additional Pods as needed to initiate more traffic and support the number of concurrent users.
- D. Download the container image of a distributed load testing framework on Cloud Shell. Sequentially start several instances of the container on Cloud Shell to increase the load on the API.

**Correct Answer: D**

*Community vote distribution*

C (75%)

D (25%)

✉️  **JonathanSJ** 2 months, 3 weeks ago

**Selected Answer: C**

I will go for C.

upvoted 1 times

✉️  **purushi** 8 months, 3 weeks ago

**Selected Answer: C**

Requirements are very clear. Load testing with concurrent users/threads + Multiple source origins/IP address, C is the best choice.

upvoted 1 times

✉️  **purushi** 8 months, 3 weeks ago

Option D is closer but we cannot instantiate the mutliple requests with different IP addresses.

upvoted 1 times

✉️  **NewComer200** 11 months, 3 weeks ago

**Selected Answer: D**

It's normal to launch some compute engine from cloud shell.

I think we can increase right load by increasing Compute Engine which do load-test from Cloud Shell step by step.

Can the test from GKE cover the condition which is "from multiple source IP addresses.".

upvoted 1 times

✉️  **NewComer200** 11 months, 3 weeks ago

I feel that load testing from the Compute Engine is more accurate than load testing from the Pod.

I'm not sure what to think.

Is it possible that GKE's engress is a bottleneck and load testing is not possible?

upvoted 1 times

✉  **mrvergara** 1 year, 2 months ago

**Selected Answer: C**

Option D, which involves starting several instances of a load testing framework container on Cloud Shell, may not be a recommended approach for several reasons:

Cloud Shell is a shell environment for managing resources hosted on Google Cloud and does not provide a scalable infrastructure for running load tests.

Starting several instances of a container on Cloud Shell is not a highly available or scalable solution for load testing, and may not provide sufficient parallelism or control over the source IP addresses of the traffic.

Using a private Google Kubernetes Engine cluster to deploy a distributed load testing framework allows for scaling up the load testing by deploying additional Pods, which can provide more control over the number of concurrent users and the source IP addresses of the traffic, and can provide a more robust and scalable infrastructure for load testing.

upvoted 3 times

✉  **NewComer200** 11 months, 3 weeks ago

"Cloud Shell is a shell environment for managing resources hosted on Google Cloud and does not provide a scalable infrastructure for running load tests."

I agree with this explanation.

But

"Starting several instances of a container on Cloud Shell is not a highly available or scalable solution for load testing, and may not provide sufficient parallelism or control over the source IP addresses of the traffic."

I can't agree with this explanation.

Please teach me where this explanation is written.

It's normal to launch some compute engine from cloud shell.

I think we can increase right load by increasing Compute Engine which do load-test from Cloud Shell step by step.

Can the test from GKE cover the condition which is "from multiple source IP addresses".

I think this question's answer is D.

upvoted 1 times

✉  **TNT87** 1 year, 2 months ago

**Selected Answer: D**

nope Answer is D....not C

upvoted 1 times

✉  **TNT87** 1 year, 2 months ago

<https://cloud.google.com/run/docs/about-load-testing>

upvoted 1 times

✉  **TNT87** 1 year, 2 months ago

**Selected Answer: C**

To deploy the load testing tasks, you do the following:

Deploy a load testing master.

Deploy a group of load testing workers. With these load testing workers, you can create a substantial amount of traffic for testing purposes.

<https://cloud.google.com/run/docs/about-load-testing>

[https://cloud.google.com/architecture/distributed-load-testing-using-gke#build\\_the\\_container\\_image](https://cloud.google.com/architecture/distributed-load-testing-using-gke#build_the_container_image)

Answer

upvoted 1 times

✉  **TNT87** 1 year, 2 months ago

This tutorial explains how to use Google Kubernetes Engine (GKE) to deploy a distributed load testing framework that uses multiple containers to create traffic for a simple REST-based API. This tutorial load-tests a web application deployed to App Engine that exposes REST-style endpoints to respond to incoming HTTP POST requests.

upvoted 1 times



Your team is creating a serverless web application on Cloud Run. The application needs to access images stored in a private Cloud Storage bucket. You want to give the application Identity and Access Management (IAM) permission to access the images in the bucket, while also securing the services using Google-recommended best practices. What should you do?

- A. Enforce signed URLs for the desired bucket. Grant the Storage Object Viewer IAM role on the bucket to the Compute Engine default service account.
- B. Enforce public access prevention for the desired bucket. Grant the Storage Object Viewer IAM role on the bucket to the Compute Engine default service account.
- C. Enforce signed URLs for the desired bucket. Create and update the Cloud Run service to use a user-managed service account. Grant the Storage Object Viewer IAM role on the bucket to the service account.
- D. Enforce public access prevention for the desired bucket. Create and update the Cloud Run service to use a user-managed service account. Grant the Storage Object Viewer IAM role on the bucket to the service account.

**Correct Answer: B***Community vote distribution*

D (100%)

**✉️**  **JonathanSJ** 2 months, 3 weeks ago**Selected Answer: D**

I will go for D.

Option C sounds good, but as the service account only have the Storage Object Viewer role it can't generate signed URLs for files from bucket because need storage.object.get, then it's incorrect.

upvoted 1 times

**✉️**  **\_\_rajan\_\_** 7 months ago**Selected Answer: D**

This approach allows you to secure your Cloud Storage bucket by enforcing public access prevention, which prevents data from being accidentally shared with the public. By creating and updating the Cloud Run service to use a user-managed service account, you can ensure only this service has access to the bucket. Granting the Storage Object Viewer IAM role on the bucket to the service account allows the service to read objects stored in the bucket.

upvoted 1 times

**✉️**  **purushi** 8 months, 3 weeks ago**Selected Answer: D**

D is right.

- 1) Create service account with role of viewing the objects under Cloud storage bucket
- 2) Create policies to prevent public access to the bucket.

A and C: Neither of these are close to the solution.

B is somewhat closer but the statement "Grant the Storage Object Viewer IAM role on the bucket to the Compute Engine default service account" is wrong since we need to create service account for the application and not for VM.

upvoted 2 times

**✉️**  **Wrter** 1 year ago**Selected Answer: D**

most secure and efficient way to give the application Identity and Access Management (IAM) permission to access the images in the bucket.

upvoted 2 times

You are using Cloud Run to host a global ecommerce web application. Your company's design team is creating a new color scheme for the web app. You have been tasked with determining whether the new color scheme will increase sales. You want to conduct testing on live production traffic. How should you design the study?

- A. Use an external HTTP(S) load balancer to route a predetermined percentage of traffic to two different color schemes of your application. Analyze the results to determine whether there is a statistically significant difference in sales.
- B. Use an external HTTP(S) load balancer to route traffic to the original color scheme while the new deployment is created and tested. After testing is complete, reroute all traffic to the new color scheme. Analyze the results to determine whether there is a statistically significant difference in sales.
- C. Use an external HTTP(S) load balancer to mirror traffic to the new version of your application. Analyze the results to determine whether there is a statistically significant difference in sales.
- D. Enable a feature flag that displays the new color scheme to half of all users. Monitor sales to see whether they increase for this group of users.

**Correct Answer: C**

*Community vote distribution*

A (90%)

10%

✉️  **theereechee** Highly Voted 11 months, 3 weeks ago

**Selected Answer: A**

Correct answer is A. This is classic A/B testing. Since you already have a new version, built into an image, all you need do is to use the load balancer to split traffic going to old version and new version. See: [https://cloud.google.com/load-balancing/docs/l7-internal/traffic-management#traffic\\_actions\\_weight-based\\_traffic\\_splitting](https://cloud.google.com/load-balancing/docs/l7-internal/traffic-management#traffic_actions_weight-based_traffic_splitting). Note that global load balancers can route to serverless services. <https://cloud.google.com/load-balancing/docs/https/setting-up-https-serverless>

upvoted 6 times

✉️  **plutonians123** Most Recent 4 months, 3 weeks ago

**Selected Answer: A**

Considering the importance of traffic analysis and the need for precise control over traffic distribution for a global ecommerce web application Option A is likely the better choice. This option allows for detailed monitoring and analysis of user interactions with different color schemes, offering clear insights into which version performs better in terms of sales. The use of an external HTTP(S) load balancer for traffic routing provides a more controlled environment for conducting such a study.

upvoted 1 times

✉️  **\_rajan\_** 7 months ago

**Selected Answer: A**

A is correct.

upvoted 1 times

✉️  **purush** 8 months, 3 weeks ago

**Selected Answer: A**

A is right. D is specifying 50% of the users which is not correct. In reality the traffic split is 80-20 or 75-25 ratio. This is a specialized version of canary deployments.

upvoted 1 times

✉️  **Writer** 1 year ago

**Selected Answer: D**

This is the best way to test the new color scheme on live production traffic. By enabling a feature flag, you can display the new color scheme subset of users while keeping the old color scheme for the rest of the users. This will allow you to compare sales between the two groups of users and determine whether the new color scheme has a statistically significant impact on sales.

upvoted 1 times

Question #258

*Topic 1*

You are a developer at a large corporation. You manage three Google Kubernetes Engine clusters on Google Cloud. Your team's developers need to switch from one cluster to another regularly without losing access to their preferred development tools. You want to configure access to these multiple clusters while following Google-recommended best practices. What should you do?

- A. Ask the developers to use Cloud Shell and run gcloud container clusters get-credential to switch to another cluster.
- B. In a configuration file, define the clusters, users, and contexts. Share the file with the developers and ask them to use kubectl config to add cluster, user, and context details.
- C. Ask the developers to install the gcloud CLI on their workstation and run gcloud container clusters get-credentials to switch to another cluster.
- D. Ask the developers to open three terminals on their workstation and use kubectl config to configure access to each cluster.

**Correct Answer:** C

*Community vote distribution*

B (78%)

11%

11%

 **wanrltw** 4 months, 1 week ago

**Selected Answer: B**

B 100%

<https://kubernetes.io/docs/tasks/access-application-cluster/configure-access-multiple-clusters/>

upvoted 1 times

 **wanrltw** 4 months, 1 week ago

**Selected Answer: D**

D 100%

<https://kubernetes.io/docs/tasks/access-application-cluster/configure-access-multiple-clusters/>

upvoted 1 times

 **wanrltw** 4 months, 1 week ago

Typo - B\*

upvoted 1 times

 **\_\_rajan\_\_** 7 months ago

**Selected Answer: C**

This approach allows developers to switch between different Google Kubernetes Engine clusters directly from their local workstation<sup>1</sup>. The gcloud container clusters get-credentials command configures kubectl with the credentials of the specified cluster<sup>1</sup>, making it easy for developers to switch contexts and interact with different clusters.

upvoted 1 times

 **purush** 8 months, 3 weeks ago

**Selected Answer: B**

<https://kubernetes.io/docs/tasks/access-application-cluster/configure-access-multiple-clusters/>

Command used: kubectl config use-context

upvoted 3 times

 **phil\_thain** 10 months, 2 weeks ago

**Selected Answer: B**

<https://kubernetes.io/docs/tasks/access-application-cluster/configure-access-multiple-clusters/>

upvoted 1 times

 **Writer** 1 year ago

**Selected Answer: B**

Option B is the best solution because it is secure, convenient, and time-efficient. By using a configuration file, you can define the clusters, user, and contexts that you want to use. You can then share the file with the developers, who can use it to add the cluster, user, and context details to their kubeconfig file. Once the developers have added the cluster, user, and context details to their kubeconfig file, they can switch to another cluster by using the following command: kubectl config use <context-name>

upvoted 2 times

You are a lead developer working on a new retail system that runs on Cloud Run and Firestore. A web UI requirement is for the user to be able to browse through all products. A few months after go-live, you notice that Cloud Run instances are terminated with HTTP 500: Container instances are exceeding memory limits errors during busy times. This error coincides with spikes in the number of Firestore queries.

You need to prevent Cloud Run from crashing and decrease the number of Firestore queries. You want to use a solution that optimizes system performance. What should you do?

- A. Modify the query that returns the product list using cursors with limits.
- B. Create a custom index over the products.
- C. Modify the query that returns the product list using integer offsets.
- D. Modify the Cloud Run configuration to increase the memory limits.

**Correct Answer: C***Community vote distribution*

A (100%)

**✉️**  \_\_rajan\_\_ 7 months ago**Selected Answer: A**

A is correct.

upvoted 1 times

**✉️**  purushi 8 months, 3 weeks ago**Selected Answer: A**

A is Best. Using pagination with limit on the size. This is called Lazy loading of data.

upvoted 1 times

**✉️**  Writer 1 year ago**Selected Answer: A**

A cursor is a pointer to a specific location in a Firestore database. By using cursors with limits, you can control the number of documents that returned in a query. This can help to reduce the number of Firestore queries that are made, which can improve performance and prevent Cloud Run from crashing.

upvoted 4 times

You are a developer at a large organization. Your team uses Git for source code management (SCM). You want to ensure that your team follows Google-recommended best practices to manage code to drive higher rates of software delivery. Which SCM process should your team use?

- A. Each developer commits their code to the main branch before each product release, conducts testing, and rolls back if integration issues are detected.
- B. Each group of developers copies the repository, commits their changes to their repository, and merges their code into the main repository before each product release.
- C. Each developer creates a branch for their own work, commits their changes to their branch, and merges their code into the main branch daily.
- D. Each group of developers creates a feature branch from the main branch for their work, commits their changes to their branch, and merges their code into the main branch after the change advisory board approves it.

**Correct Answer: C***Community vote distribution*

D (88%)

13%

**wanrltw** 4 months, 1 week ago**Selected Answer: D**

It's D

upvoted 1 times

**kapara** 4 months, 2 weeks ago

I don't get it why everybody here said D?

IMHO Option D is FALSE bc - Creating feature branches for groups of developers and waiting for a change advisory board's approval can slow down the development process and might not align with the principles of agile and continuous delivery.

upvoted 1 times

**wanrltw** 4 months, 1 week ago

As they say, better safe than sorry. When you rush, you're more prone to make a mistake and it often takes more time to fix a mistake than prevent it. Also, check out the 4-eyes principle.

upvoted 1 times

**\_rajan\_** 7 months ago**Selected Answer: D**

D is correct.

upvoted 1 times

**purushi** 8 months, 3 weeks ago**Selected Answer: D**

The defacto SCM process is described in option D.

Advisory board approves it means approving the PR raised by developer before merging into develop/master branch.

upvoted 1 times

**zanhsieh** 10 months, 3 weeks ago**Selected Answer: B**

B. Put all commits inside a single repo would place lots of burden on branching and commit history. This not only makes checkout slower but also hard to manage - think about a small-mid size team (10 developers) creating 200 commits per day, roughly equals to 156,000 for 3 months. The maintainers of a repo would have a hard time to chase down and merge 156,000 commits. Not to mention the repo permission management would be a nightmare if the repo extends to enterprise level (200 - 500 developers / SRE / qa / SA). Forking repo as opt B would be a better choice. Each developer deals with his fork. PR merge and squash once ready. In fact, all famous OSS software, such as Kubernetes, Grafana, Prometheus, etc., use this approach.

upvoted 1 times

**Writer** 1 year ago**Selected Answer: D**

Use a centralized repository. A centralized repository is a single location where all of your team's code is stored. This makes it easy for everyone to access the latest code, and it also helps to prevent conflicts.

Use branches. Branches are a way to create a separate version of the code for development purposes. This allows developers to work on new features or bug fixes without affecting the main branch of the code.

upvoted 2 times

**closer89** 1 year ago**Selected Answer: D**

You are a developer at a large organization

upvoted 2 times

You have a web application that publishes messages to Pub/Sub. You plan to build new versions of the application locally and want to quickly test Pub/Sub integration for each new build. How should you configure local testing?

- A. Install Cloud Code on the integrated development environment (IDE). Navigate to Cloud APIs, and enable Pub/Sub against a valid Google Project ID. When developing locally, configure your application to call pubsub.googleapis.com.
- B. Install the Pub/Sub emulator using gcloud, and start the emulator with a valid Google Project ID. When developing locally, configure your application to use the local emulator with \${gcloud beta emulators pubsub env-init}.
- C. In the Google Cloud console, navigate to the API Library, and enable the Pub/Sub API. When developing locally, configure your application to call pubsub.googleapis.com.
- D. Install the Pub/Sub emulator using gcloud, and start the emulator with a valid Google Project ID. When developing locally, configure your application to use the local emulator by exporting the PUBSUB\_EMULATOR\_HOST variable.

**Correct Answer: A**

*Community vote distribution*

B (67%)

D (33%)

 **alpha\_canary** 2 weeks, 4 days ago

**Selected Answer: B**

Here we have only single machine, so just using the terminal command is OK, no need to export ENV variables  
[https://cloud.google.com/pubsub/docs/emulator#automatically\\_setting\\_the\\_variables](https://cloud.google.com/pubsub/docs/emulator#automatically_setting_the_variables)

upvoted 1 times

 **examprof** 4 months, 3 weeks ago

Alternative B is correct. Link: <https://cloud.google.com/pubsub/docs/emulator#env>

Executing "gcloud beta emulators pubsub env-init" is required for local testing when the application and the emulator run either on the same machine or on different machines. The export of the PUBSUB\_EMULATOR\_HOST variable is an additional step required only in the latter case (when the application and the emulator run on different machines).

upvoted 1 times

 **plutonian123** 4 months, 3 weeks ago

**Selected Answer: B**

Based on the common steps for implementing the Pub/Sub emulator, the best choice for configuring local testing of your web application's Pub/Sub integration would be:

Option B: Install the Pub/Sub emulator using gcloud, and start the emulator with a valid Google Project ID. When developing locally, configure your application to use the local emulator with \${gcloud beta emulators pubsub env-init}.

This option covers the essential steps for both scenarios (same machine or different machines) and provides a clear path for setting up and utilizing the Pub/Sub emulator effectively for local development and testing.

upvoted 1 times

 **\_rajan\_** 7 months ago

**Selected Answer: D**

This approach allows you to test your application's integration with Pub/Sub without making actual calls to the Pub/Sub service, which can be time-consuming and may incur costs. Instead, your application interacts with the local emulator, which mimics the behavior of the actual Pub/Sub service. This makes it a fast and cost-effective solution for local testing. Remember to set the PUBSUB\_EMULATOR\_HOST environment variable to point your application to the local emulator.

upvoted 1 times

✉️ GoReplyGCPExam 10 months, 3 weeks ago

Selected Answer: B

[https://cloud.google.com/pubsub/docs/emulator#automatically\\_setting\\_the\\_variables](https://cloud.google.com/pubsub/docs/emulator#automatically_setting_the_variables)

If your application and the emulator run on the same machine, you can set the environment variables automatically with:  
1) \$(gcloud beta emulators pubsub env-init)

If your application and the emulator run on different machines, set the environment variables manually with:

- 1) Run the env-init command: gcloud beta emulators pubsub env-init
- 2) On the machine that runs your application, set the PUBSUB\_EMULATOR\_HOST

upvoted 3 times

✉️ sbonessi 11 months, 1 week ago

Selected Answer: B

I agree with B as the correct answer.

[https://cloud.google.com/pubsub/docs/emulator#automatically\\_setting\\_the\\_variables](https://cloud.google.com/pubsub/docs/emulator#automatically_setting_the_variables)

You can run gcloud beta emulators pubsub env-init in your own localhost within if your application and the emulator run on the same machine

upvoted 1 times

✉️ Writer 1 year ago

Selected Answer: D

Answer: D

upvoted 1 times

✉️ Writer 1 year ago

Answer: D

upvoted 1 times

✉️ closer89 1 year ago

Selected Answer: D

gcloud beta emulators pubsub start --project=my-project-id

export PUBSUB\_EMULATOR\_HOST=localhost:8085

export GOOGLE\_CLOUD\_PROJECT=my-project-id

upvoted 1 times

✉️ closer89 1 year ago

its B

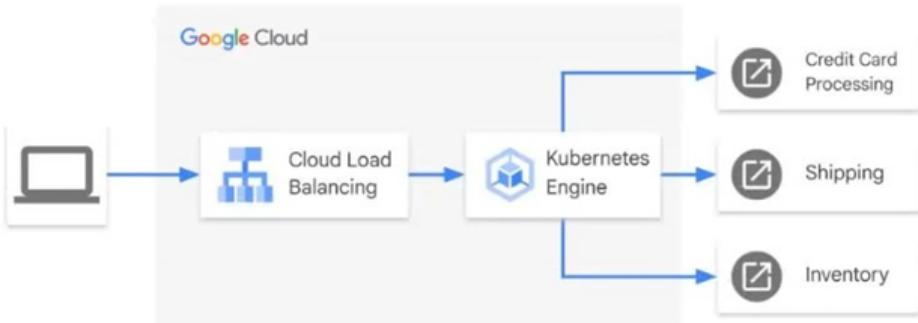
[https://cloud.google.com/pubsub/docs/emulator#automatically\\_setting\\_the\\_variables](https://cloud.google.com/pubsub/docs/emulator#automatically_setting_the_variables)

upvoted 4 times

Question #262

Topic 1

Your ecommerce application receives external requests and forwards them to third-party API services for credit card processing, shipping, and inventory management as shown in the diagram.



Your customers are reporting that your application is running slowly at unpredictable times. The application doesn't report any metrics. You need to determine the cause of the inconsistent performance. What should you do?

- A. Install the OpenTelemetry library for your respective language, and instrument your application.
- B. Install the Ops Agent inside your container and configure it to gather application metrics.
- C. Modify your application to read and forward the X-Cloud-Trace-Context header when it calls the downstream services.
- D. Enable Managed Service for Prometheus on the Google Kubernetes Engine cluster to gather application metrics.

**Correct Answer: C**

*Community vote distribution*

A (80%)

D (20%)

 **plutonians123** 4 months, 3 weeks ago

**Selected Answer: A**

The key part of the question prompting the use of OpenTelemetry over Prometheus is: "Your customers are reporting that your application is running slowly at unpredictable times. The application doesn't report any metrics." This indicates a need for detailed instrumentation to trace and diagnose performance issues across various external service interactions. OpenTelemetry, with its comprehensive APIs and SDKs for collecting a wide range of telemetry data (traces, metrics, logs), is well-suited for this task. It allows for tracing the application's workflow and identifying bottlenecks, which is essential for understanding the root cause of the inconsistent performance.

upvoted 1 times

 **\_rajan\_** 7 months ago

**Selected Answer: A**

Question #263

Topic 1

You are developing a new application. You want the application to be triggered only when a given file is updated in your Cloud Storage bucket. Your trigger might change, so your process must support different types of triggers. You want the configuration to be simple so that multiple team members can update the triggers in the future. What should you do?

- A. Configure Cloud Storage events to be sent to Pub/Sub, and use Pub/Sub events to trigger a Cloud Build job that executes your application.
- B. Create an Eventarc trigger that monitors your Cloud Storage bucket for a specific filename, and set the target as Cloud Run.
- C. Configure a Cloud Function that executes your application and is triggered when an object is updated in Cloud Storage.
- D. Configure a Firebase function that executes your application and is triggered when an object is updated in Cloud Storage.

**Correct Answer: C**

*Community vote distribution*

C (67%)

B (33%)

 **alpha\_canary** 2 weeks, 4 days ago

**Selected Answer: C**

<https://cloud.google.com/functions/docs/calling/storage>

upvoted 1 times

 **imiu** 4 months, 3 weeks ago

**Selected Answer: C**

<https://cloud.google.com/functions/docs/calling>

upvoted 1 times

 **plutonians123** 4 months, 3 weeks ago

**Selected Answer: C**

I change my answer to C, the choice of Option C ("Configure a Cloud Function that executes your application and is triggered when an object updated in Cloud Storage") is strongly supported by the sentence "You want the configuration to be simple so that multiple team members can update the triggers in the future." Cloud Functions provide a more straightforward and user-friendly approach for setting up and managing triggers, making it easier for various team members to work with and update the configuration as needed. This simplicity aligns well with the requirement for an easily manageable and modifiable trigger process.

upvoted 1 times

Question #264

*Topic 1*

You are defining your system tests for an application running in Cloud Run in a Google Cloud project. You need to create a testing environment that is isolated from the production environment. You want to fully automate the creation of the testing environment with the least amount of effort and execute automated tests. What should you do?

- A. Using Cloud Build, execute Terraform scripts to create a new Google Cloud project and a Cloud Run instance of your application in the Google Cloud project.
- B. Using Cloud Build, execute a Terraform script to deploy a new Cloud Run revision in the existing Google Cloud project. Use traffic splitting to send traffic to your test environment.
- C. Using Cloud Build, execute gcloud commands to create a new Google Cloud project and a Cloud Run instance of your application in the Google Cloud project.
- D. Using Cloud Build, execute gcloud commands to deploy a new Cloud Run revision in the existing Google Cloud project. Use traffic splitting to send traffic to your test environment.

**Correct Answer: C**

*Community vote distribution*

A (86%)

14%

 **kapara** 4 months ago

**Selected Answer: A**

fully automate == terraform.  
and new separate env == new project  
therefore i vote A.

upvoted 3 times

 **Kadhem** 4 months ago

**Selected Answer: C**

C is simpler than A!

upvoted 1 times

 **kapara** 4 months ago

you right, but the part of the requirements is "You want to \*fully automate\* the creation of the testing environment"

upvoted 4 times

 **Kadhem** 3 months, 4 weeks ago

oh you right, i didn't make attention for this detail.

upvoted 1 times

 **wanrltw** 4 months, 1 week ago

A is correct

<https://cloud.google.com/docs/terraform/resource-management/managing-infrastructure-as-code>

upvoted 1 times

 **imiu** 4 months, 3 weeks ago

**Selected Answer: A**

<https://cloud.google.com/docs/terraform/best-practices-for-terraform>

upvoted 1 times

 **vmst** 5 months, 1 week ago

**Selected Answer: A**

A is correct

upvoted 1 times

 **xiaofeng\_0226** 5 months, 2 weeks ago

**Selected Answer: A**

A is correct

upvoted 1 times

Question #265

Topic 1

You are a cluster administrator for Google Kubernetes Engine (GKE). Your organization's clusters are enrolled in a release channel. You need to be informed of relevant events that affect your GKE clusters, such as available upgrades and security bulletins. What should you do?

- A. Configure cluster notifications to be sent to a Pub/Sub topic.
- B. Execute a scheduled query against the google\_cloud\_release\_notes BigQuery dataset.
- C. Query the GKE API for available versions.
- D. Create an RSS subscription to receive a daily summary of the GKE release notes.

**Correct Answer: B**

*Community vote distribution*

A (63%)

D (38%)

👤 **wanrltw** 4 months, 1 week ago

**Selected Answer: A**

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

upvoted 1 times

👤 **kapara** 4 months, 2 weeks ago

**Selected Answer: A**

After i read

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

and

<https://cloud.google.com/kubernetes-engine/docs/concepts/release-channels#channels>

i choose A, the two of the answer is correct, but i think how wrote this question according the text, mean to option A. the question and what write here - is literally same words as here:

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

upvoted 1 times

👤 **imiu** 5 months ago

**Selected Answer: A**

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

upvoted 3 times

👤 **examprof** 4 months, 3 weeks ago

Agree with A.

upvoted 1 times

👤 **AlexA\_94** 5 months, 1 week ago

**Selected Answer: D**

<https://cloud.google.com/kubernetes-engine/docs/concepts/release-channels#channels>

upvoted 3 times

👤 **wanrltw** 4 months, 1 week ago

In this link it's said that "you can subscribe to upgrade notifications to be informed of newly available versions".

The correct answer is A: <https://cloud.google.com/kubernetes-engine/docs/concepts/cluster-notifications>

upvoted 1 times

You are tasked with using C++ to build and deploy a microservice for an application hosted on Google Cloud. The code needs to be containerized and use several custom software libraries that your team has built. You do not want to maintain the underlying infrastructure of the application. How should you deploy the microservice?

- A. Use Cloud Functions to deploy the microservice.
- B. Use Cloud Build to create the container, and deploy it on Cloud Run.
- C. Use Cloud Shell to containerize your microservice, and deploy it on a Container-Optimized OS Compute Engine instance.
- D. Use Cloud Shell to containerize your microservice, and deploy it on standard Google Kubernetes Engine.

**Correct Answer: D***Community vote distribution*

B (100%)

✉️  **JonathanSJ** 2 months, 3 weeks ago

**Selected Answer: B**

I will go for B. Fully managed and well suited for c++  
upvoted 1 times

✉️  **imiu** 4 months, 3 weeks ago

Can you provide some documentation that prove B is the right choice?  
upvoted 1 times

✉️  **kapara** 4 months, 2 weeks ago

Option A, using Cloud Functions, is not suitable for your scenario because Cloud Functions primarily supports Node.js, Python, Go, Java, .NET, Ruby, and PHP runtimes. It does not natively support C++ applications. Therefore, for a microservice written in C++, Cloud Function would not be an appropriate choice as it would require significant workarounds or a complete rewrite of your application in a supported language.

and C ,D is OS and GKE so you need to setup the infra.  
therefore the answer is B.  
upvoted 5 times

✉️  **vmst** 5 months, 1 week ago

**Selected Answer: B**

It's B  
upvoted 2 times

✉️  **xiaofeng\_0226** 5 months, 2 weeks ago

**Selected Answer: B**

For me is B  
upvoted 3 times

You need to containerize a web application that will be hosted on Google Cloud behind a global load balancer with SSL certificates. You don't have the time to develop authentication at the application level, and you want to offload SSL encryption and management from your application. You want to configure the architecture using managed services where possible. What should you do?

- A. Host the application on Google Kubernetes Engine, and deploy an NGINX Ingress Controller to handle authentication.
- B. Host the application on Google Kubernetes Engine, and deploy cert-manager to manage SSL certificates.
- C. Host the application on Compute Engine, and configure Cloud Endpoints for your application.
- D. Host the application on Google Kubernetes Engine, and use Identity-Aware Proxy (IAP) with Cloud Load Balancing and Google-managed certificates.

**Correct Answer: B***Community vote distribution*

D (100%)

**✉️**  **plutonians123** 4 months, 3 weeks ago**Selected Answer: D**

IAP provides a way to control access to applications running on GCP without the need for traditional VPNs. It works by verifying a user's identity and determining if that user should be allowed access to the application. This is especially useful since you do not have the time to develop authentication at the application level. IAP can handle this for you.

upvoted 1 times

**✉️**  **diegodoal** 5 months, 2 weeks ago**Selected Answer: D**

It should be D

upvoted 1 times

**✉️**  **vspringe** 5 months, 2 weeks ago

D. provides a comprehensive, managed solution that fulfills all the requirements: containerized application hosting on GKE, simplified authentication with IAP, SSL offloading and management with Cloud Load Balancing and Google-managed certificates.

upvoted 1 times

You manage a system that runs on stateless Compute Engine VMs and Cloud Run instances. Cloud Run is connected to a VPC, and the ingress setting is set to Internal. You want to schedule tasks on Cloud Run. You create a service account and grant it the roles/run.invoker Identity and Access Management (IAM) role. When you create a schedule and test it, a 403 Permission Denied error is returned in Cloud Logging. What should you do?

- A. Grant the service account the roles/run.developer IAM role.
- B. Configure a cron job on the Compute Engine VMs to trigger Cloud Run on schedule.
- C. Change the Cloud Run ingress setting to 'Internal and Cloud Load Balancing.'
- D. Use Cloud Scheduler with Pub/Sub to invoke Cloud Run.

**Correct Answer: A***Community vote distribution*

D (100%)

 **plutoniants123** 4 months, 3 weeks ago

**Selected Answer: D**

Cloud Scheduler can trigger Cloud Run services, but in this case, where the ingress is set to 'Internal', direct invocation might not work. Instead you can use Cloud Scheduler in combination with Pub/Sub. Cloud Scheduler can create a Pub/Sub message on a schedule, and this Pub/Sub message can then trigger the Cloud Run service. This approach is commonly used for invoking services with restricted network access.

upvoted 2 times

 **plutoniants123** 4 months, 3 weeks ago

**Selected Answer: D**

Cloud Scheduler can trigger Cloud Run services, but in this case, where the ingress is set to 'Internal', direct invocation might not work. Instead you can use Cloud Scheduler in combination with Pub/Sub. Cloud Scheduler can create a Pub/Sub message on a schedule, and this Pub/Sub message can then trigger the Cloud Run service. This approach is commonly used for invoking services with restricted network access.

upvoted 1 times

 **diegodoal** 5 months, 2 weeks ago

**Selected Answer: D**

D. When setting PubSub subscription, use type push and use the service account with the invoker role as authentication. A. no need more permissions. B. it could work if the vms are in the same VPC, but it is not best practice. C. That setting is only for connecting to load balancer

upvoted 1 times

 **vspringe** 5 months, 2 weeks ago

D. is the best solution because it effectively circumvents the limitation of the Internal ingress setting of Cloud Run. This setting restricts external access, which is likely causing the 403 error. By using Cloud Scheduler to trigger a Pub/Sub topic, and then having Pub/Sub trigger the Cloud Run service, you maintain internal access security while enabling external scheduling. This method is both secure and adheres to the internal-only access requirements, leveraging managed services for scalability and reliability.

upvoted 1 times

Question #269

Topic 1

You work on an application that relies on Cloud Spanner as its main datastore. New application features have occasionally caused performance regressions. You want to prevent performance issues by running an automated performance test with Cloud Build for each commit made. If multiple commits are made at the same time, the tests might run concurrently. What should you do?

- A. Create a new project with a random name for every build. Load the required data. Delete the project after the test is run.
- B. Create a new Cloud Spanner instance for every build. Load the required data. Delete the Cloud Spanner instance after the test is run.
- C. Create a project with a Cloud Spanner instance and the required data. Adjust the Cloud Build build file to automatically restore the data to its previous state after the test is run.
- D. Start the Cloud Spanner emulator locally. Load the required data. Shut down the emulator after the test is run.

**Correct Answer:** *B*

*Community vote distribution*

B (71%)

D (29%)

 **wanrltw** 4 months, 1 week ago

Selected Answer: B

Question #270

Topic 1

Your company's security team uses Identity and Access Management (IAM) to track which users have access to which resources. You need to create a version control system that can integrate with your security team's processes. You want your solution to support fast release cycles and frequent merges to your main branch to minimize merge conflicts. What should you do?

- A. Create a Cloud Source Repositories repository, and use trunk-based development.
- B. Create a Cloud Source Repositories repository, and use feature-based development.
- C. Create a GitHub repository, mirror it to a Cloud Source Repositories repository, and use trunk-based development.
- D. Create a GitHub repository, mirror it to a Cloud Source Repositories repository, and use feature-based development.

**Correct Answer: C**

*Community vote distribution*

A (50%)

C (50%)

 **JonathanSJ** 2 months, 3 weeks ago

**Selected Answer: A**

I will go for A instead of C because it's more simple and straightforward.

There isn't a requirement to have PR's or something like that to choose to have GitHub.

upvoted 1 times

 **wanrltw** 4 months, 1 week ago

**Selected Answer: A**

I choose A.

Question #271

Topic 1

You recently developed an application that monitors a large number of stock prices. You need to configure Pub/Sub to receive messages and update the current stock price in an in-memory database. A downstream service needs the most up-to-date prices in the in-memory database to perform stock trading transactions. Each message contains three pieces of information:

- Stock symbol
- Stock price
- Timestamp for the update

How should you set up your Pub/Sub subscription?

- A. Create a push subscription with exactly-once delivery enabled.
- B. Create a pull subscription with both ordering and exactly-once delivery turned off.
- C. Create a pull subscription with ordering enabled, using the stock symbol as the ordering key.
- D. Create a push subscription with both ordering and exactly-once delivery turned off.

**Correct Answer: A**

*Community vote distribution*

A (67%)

C (33%)

 **alpha\_canary** 2 weeks, 2 days ago

**Selected Answer: A**

iven the requirement that the downstream service needs the most up-to-date prices, you don't need to order the messages. In this case, a pu subscription would be suitable as it delivers messages as they arrive, ensuring the downstream service receives the latest stock prices prompt. Exactly-once delivery can prevent the same message from being processed multiple times, which could be beneficial in this scenario.

upvoted 1 times

✉️  **JonathanSJ** 2 months, 3 weeks ago

**Selected Answer: A**

I will go for A.

B and C aren't good because you need to receive the prices in real time as they come.

Between A and D:

D with exactly-once delivery turned off you can process the same message many times and it isn't good for financial systems.

upvoted 1 times

✉️  **JonathanSJ** 2 months, 3 weeks ago

I change my mind.

I will go for D, because the question says "A downstream service needs the most up-to-date prices".

The pull subscriptions introduce the possibility of latency between the time a message is published and when it's pulled by the app. Then B and C are discarded.

Between A and D, A is not correct because the exactly-once delivery feature is only for pull subscriptions.

Also, this questions is a duplicate from Question #271.

upvoted 2 times

✉️  **pbrvg!** 4 months, 3 weeks ago

A is correct (I am not a contributor, so unable to vote). Rationale:

1. The downstream application needs only the most up-to-date value for a stock price. There's no need of historical values from a time series "ordering" does not make any sense in this scenario. This eliminates alternatives B, C and D. In addition, in alternative C, "using the stock symbol as the ordering key" has no practical effect, once "ordering" is not necessary.

2. About "push" and "pull": in a "push" subscription, whenever the topic is fed with a new value, it will keep pushing it to the application until acknowledgement is received. Latency is lower in this case. In a "pull" subscription, there's an additional burden on the application to keep pulling from the topic. This increases latency. A "push" subscription is recommended in such scenarios.

upvoted 4 times

✉️  **vspringe** 5 months, 2 weeks ago

**Selected Answer: C**

Pull Subscription for Controlled Processing: A pull subscription gives you control over when and how messages are processed. This can be particularly important for maintaining the integrity of the in-memory database, as it allows for more deliberate handling of message backlogs at peak loads.

Message Ordering Is Crucial: The ordering of stock price updates is critical. Using the stock symbol as the ordering key ensures that updates for a specific stock are processed in the order they were sent. This is vital to ensure the accuracy of stock price data, as prices must be updated in the sequence they were received to reflect the true market conditions.

No Need for Exactly-Once Delivery: In most financial data scenarios, the latest data supersedes the old. If a message is delivered more than once, the last update for a given timestamp will leave the database in the correct state. Therefore, exactly-once delivery, which can add

Question #272

Topic 1

You are a developer at a social media company. The company runs their social media website on-premises and uses MySQL as a backend to store user profiles and user posts. Your company plans to migrate to Google Cloud, and you learn will migrate user profile information to Firestore. You are tasked with designing the Firestore collections. What should you do?

- A. Create one root collection for user profiles, and create one root collection for user posts.
- B. Create one root collection for user profiles, and create one subcollection for each user's posts.
- C. Create one root collection for user profiles, and store each user's post as a nested list in the user profile document.
- D. Create one root collection for user posts, and create one subcollection for each user's profile.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **alpha\_canary** 2 weeks, 2 days ago

**Selected Answer: B**

B: The best practice for this scenario would be to create one root collection for user profiles and one subcollection for each user's posts. This allows for easy retrieval of all posts for a given user and aligns well with the hierarchical data model of Firestore. It also provides good isolation of data as each user's posts are stored separately.

upvoted 1 times

 **JonathanSJ** 2 months, 3 weeks ago

**Selected Answer: B**

I will go for B.

upvoted 1 times

 **Kadhem** 4 months ago

**Selected Answer: B**

B is more appropriate

upvoted 1 times

 **kapara** 4 months, 2 weeks ago

**Selected Answer: B**

For migrating user profile information to Firestore in your social media company, the best approach is:

B. Create one root collection for user profiles, and create one subcollection for each user's posts.

This structure offers better scalability, efficient data retrieval, and clearer organization, while also simplifying access control and data modeling. Options A, C, and D are less optimal due to potential performance issues, complex querying, and counterintuitive data relationships.

upvoted 1 times

Your team recently deployed an application on Google Kubernetes Engine (GKE). You are monitoring your application and want to be alerted when the average memory consumption of your containers is under 20% or above 80%. How should you configure the alerts?

- A. Create a Cloud Function that consumes the Monitoring API. Create a schedule to trigger the Cloud Function hourly and alert you if the average memory consumption is outside the defined range.
- B. In Cloud Monitoring, create an alerting policy to notify you if the average memory consumption is outside the defined range.
- C. Create a Cloud Function that runs on a schedule, executes kubectl top on all the workloads on the cluster, and sends an email alert if the average memory consumption is outside the defined range.
- D. Write a script that pulls the memory consumption of the instance at the OS level and sends an email alert if the average memory consumption is outside the defined range.

**Correct Answer: D**

*Community vote distribution*

B (100%)

 **JonathanSJ** 2 months, 3 weeks ago

**Selected Answer: B**

I will go for B.

upvoted 1 times

 **plutonian123** 4 months, 2 weeks ago

**Selected Answer: B**

To monitor average memory consumption of containers in Google Kubernetes Engine (GKE), the best approach is to use Cloud Monitoring. You can create an alerting policy in Cloud Monitoring to notify you if the average memory consumption is outside the defined range. This method leverages Google Cloud's built-in capabilities for efficient and accurate monitoring.

For detailed instructions, please refer to:

Google Cloud Documentation: <https://cloud.google.com/monitoring>

upvoted 1 times

 **dar\_gor** 4 months, 2 weeks ago

**Selected Answer: B**

No need to use CloudFunction in this case and the custom script is overengineering. Answer B fits the needs.

upvoted 1 times

 **plutonian123** 4 months, 3 weeks ago

**Selected Answer: B**

Cloud Monitoring provides a user-friendly interface to create complex alerting policies. You can set up thresholds for specific metrics, like memory consumption, and receive notifications if these thresholds are exceeded or undercut. This feature negates the need for custom script functions to monitor these metrics.

upvoted 1 times

 **MoanaMacknzy** 5 months ago

**Selected Answer: B**

B is the right answer, alert in the cloud monitoring

upvoted 1 times

 **vspringe** 5 months, 2 weeks ago

B. using Cloud Monitoring to create an alerting policy is the most efficient, reliable, and straightforward method to monitor and be alerted about the memory consumption of your containers in GKE.

upvoted 2 times

You manage a microservice-based ecommerce platform on Google Cloud that sends confirmation emails to a third-party email service provider using a Cloud Function. Your company just launched a marketing campaign, and some customers are reporting that they have not received order confirmation emails. You discover that the services triggering the Cloud Function are receiving HTTP 500 errors. You need to change the way emails are handled to minimize email loss. What should you do?

- A. Increase the Cloud Function's timeout to nine minutes.
- B. Configure the sender application to publish the outgoing emails in a message to a Pub/Sub topic. Update the Cloud Function configuration to consume the Pub/Sub queue.
- C. Configure the sender application to write emails to Memorystore and then trigger the Cloud Function. When the function is triggered, it reads the email details from Memorystore and sends them to the email service.
- D. Configure the sender application to retry the execution of the Cloud Function every one second if a request fails.

**Correct Answer: C***Community vote distribution*

B (100%)

**plutonians123** 4 months, 3 weeks ago**Selected Answer: B**

This is a robust and scalable approach. By decoupling the email sending process using Pub/Sub, you introduce a queueing mechanism. This ensures that even if the Cloud Function encounters an issue, the email messages are not lost but remain in the queue. Additionally, Pub/Sub can handle high throughput and provides retry mechanisms.

upvoted 3 times

**MoanaMacknzy** 5 months ago**Selected Answer: B**

B is the right answer

upvoted 1 times

**diegodoal** 5 months, 2 weeks ago**Selected Answer: B**

B. With pub sub you can scale the load of sending emails to the Cloud Function. Also can configure exponential backoff if errors arise in the third-party service and ensure the email is delivered

upvoted 1 times

**vspringe** 5 months, 2 weeks ago

B. the most effective solution would be B. - using Pub/Sub to queue email messages and having the Cloud Function process these messages is a robust, scalable, and reliable way to handle email sending in your ecommerce platform, especially during high load conditions.

upvoted 1 times

You have a web application that publishes messages to Pub/Sub. You plan to build new versions of the application locally and need to quickly test Pub/Sub integration for each new build. How should you configure local testing?

- A. In the Google Cloud console, navigate to the API Library, and enable the Pub/Sub API. When developing locally configure your application to call pubsub.googleapis.com.
- B. Install the Pub/Sub emulator using gcloud, and start the emulator with a valid Google Project ID. When developing locally, configure your application to use the local emulator by exporting the PUBSUB\_EMULATOR\_HOST variable.
- C. Run the gcloud config set api\_endpoint\_overrides/pubsub https://pubsubemulator.googleapis.com command to change the Pub/Sub endpoint prior to starting the application.
- D. Install Cloud Code on the integrated development environment (IDE). Navigate to Cloud APIs, and enable Pub/Sub against a valid Google Project ID. When developing locally, configure your application to call pubsub.googleapis.com.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **plutonian123** 4 months, 2 weeks ago

**Selected Answer: B**

For local testing of Pub/Sub integration in a web application, installing and using the Pub/Sub emulator is the most efficient approach. The emulator can be installed via gcloud and started with a valid Google Project ID. Configuring your application to use the emulator locally is done by setting the PUBSUB\_EMULATOR\_HOST environment variable.

For more details on setting up and using the Pub/Sub emulator, visit:  
Google Cloud Documentation: <https://cloud.google.com/pubsub/docs/emulator>

upvoted 2 times

 **MFay** 4 months, 3 weeks ago

**Selected Answer: B**

For local testing of Pub/Sub integration, the most suitable option is B. You'd install the Pub/Sub emulator via gcloud, initiate it with a valid Google Project ID, and configure your application to utilize the local emulator by setting the PUBSUB\_EMULATOR\_HOST variable. This method replicates the Pub/Sub environment locally for efficient testing.

upvoted 3 times

You recently developed an application that monitors a large number of stock prices. You need to configure Pub/Sub to receive a high volume of messages and update the current stock price in a single large in-memory database. A downstream service needs the most up-to-date prices in the in-memory database to perform stock trading transactions. Each message contains three pieces of information:

- Stock symbol
- Stock price
- Timestamp for the update

How should you set up your Pub/Sub subscription?

- A. Create a pull subscription with exactly-once delivery enabled.

- B. Create a push subscription with both ordering and exactly-once delivery turned off.
- C. Create a push subscription with exactly-once delivery enabled.
- D. Create a pull subscription with both ordering and exactly-once delivery turned off.

**Correct Answer: B**

*Community vote distribution*

C (75%)

A (25%)

 **Kadhem** 4 months ago

**Selected Answer: C**

i go for C : push subscription + exactly once delivery so ordering is guaranteed  
upvoted 2 times

 **Adpese\_1** 4 months, 1 week ago

<https://cloud.google.com/pubsub/docs/exactly-once-delivery>

Question #277

Topic 1

Your team has created an application that is hosted on a Google Kubernetes Engine (GKE) cluster. You need to connect the application to a legacy REST service that is deployed in two GKE clusters in two different regions. You want to connect your application to the legacy service in a way that is resilient and requires the fewest number of steps. You also want to be able to run probe-based health checks on the legacy service on a separate port. How should you set up the connection? (Choose two.)

- A. Use Traffic Director with a sidecar proxy to connect the application to the service.
- B. Set up a proxyless Traffic Director configuration for the application.
- C. Configure the legacy service's firewall to allow health checks originating from the sidecar proxy.
- D. Configure the legacy service's firewall to allow health checks originating from the application.
- E. Configure the legacy service's firewall to allow health checks originating from the Traffic Director control plane.

**Correct Answer: AC**

*Community vote distribution*

AC (100%)

 **alpha\_canary** 2 weeks, 2 days ago

**Selected Answer: AC**

repeat of question 246  
upvoted 1 times

 **JonathanSJ** 2 months, 3 weeks ago

**Selected Answer: AC**

I will go for AC.  
upvoted 1 times

 **Kadhem** 4 months ago

**Selected Answer: AC**

Answer AC  
Question is duplicated : 246  
upvoted 1 times

 **plutonians123** 4 months, 2 weeks ago

**Selected Answer: AC**

For connecting a GKE-hosted application to a legacy REST service across two regions, using Traffic Director with a sidecar proxy and config the legacy service's firewall for health checks offers a resilient and efficient solution. More details can be found at: <https://thenewstack.io/google-traffic-director-and-the-l7-internal-load-balancer-intermingles-cloud-native-and-legacy-workloads/>  
upvoted 1 times

 **MFay** 4 months, 4 weeks ago

**Selected Answer: AC**

1. Use Traffic Director with a sidecar proxy (Option A): This enables reliable communication between your application and the legacy service. The sidecar proxy can manage traffic routing, load balancing, and resilience.

2. Configure the legacy service's firewall to allow health checks originating from the sidecar proxy (Option C): By allowing health checks from the sidecar proxy, you ensure that the health checks, which are necessary for ensuring service availability, are permitted by the firewall.

upvoted 2 times