- Expert Verified, Online, **Free**.

Custom View Settings

Topic 1 - Single Topic

Question #1 *Topic 1*

You support a Node.js application running on Google Kubernetes Engine (GKE) in production. The application makes several HTTP requests to dependent applications. You want to anticipate which dependent applications might cause performance issues. What should you do?

A. Instrument all applications with Stackdriver Profiler.

B. Instrument all applications with Stackdriver Trace and review inter-service HTTP requests.

C. Use Stackdriver Debugger to review the execution of logic within each application to instrument all applications.

D. Modify the Node.js application to log HTTP request and response times to dependent applications. Use Stackdriver Logging to find dependent applications that are performing poorly.

tdm4649 Highly Voted 4 months, 4 weeks ago
8/7, I failed the exam.. 20/50 were from this dump, ill need new version's 30 questions sets.
upvoted 10 times

tdm4649 4 months ago
OK...I want to say this to guys.
I took the exam 9/11 as my second try, and 48/50 came from this dump. I passed. I don't know that I was just lucky or the new question version will not come up any more ...
upvoted 4 times

Manumj 3 months, 2 weeks ago
this is the first time i am seeing such things happening with ET , i always depended on this site and i cleared my exams , but for this one i am seeing some negative comments .
can some suggest how can i proceed further
upvoted 1 times

karthik0077 3 months, 3 weeks ago
have you submitted exact answers from site ?
upvoted 1 times

WakandaF 3 months, 3 weeks ago
Hi, tdm46.

The reason is simple. The first time that you failed, they assign you another exam 2. All the questions and answers here belong to that exam1.
upvoted 1 times

syslog 3 months, 2 weeks ago
I agree with WakandaF. I passed the exam 22 September, I found 49/50 questions from this dump. When I failed on July, I found only 20 questions.
upvoted 1 times

Aws_guru69 2 months, 4 weeks ago
12/10, 10/50 questions, proceed with caution
upvoted 1 times

Aldo86 Highly Voted 5 months, 3 weeks ago
19th July, Only 20 Questions of 50 from Examtopics... 30 questions totally new... update the questions :)
upvoted 8 times

WakandaF 5 months, 2 weeks ago
I got the same exam, 30 questions new!!! Terraform questions, gcr.io questions.
upvoted 4 times

Aldo86 5 months, 1 week ago
@WakandaF, yes another one that I remember is the delivery proccess of APIs...
upvoted 3 times

syslog 5 months, 1 week ago
I remember also a question on how to speed up the Cloud Build building (with caching on Cloud Storage)
upvoted 4 times

Biden Most Recent 2 days, 6 hours ago
Took my exam on 12/22/2021 (during holidays). 50/50 came from this dump !!
upvoted 1 times

jits1984 1 week, 1 day ago
is this dump still valid?

upvoted 1 times

Biden 4 weeks ago
why are questions 82-88 missing ?
upvoted 2 times

PJ_2021 1 month, 3 weeks ago
Has anyone given the exam in the last 1-2 weeks. Did questions appear from here?
Also if someone is willing to collaborate on questions 55-81
upvoted 4 times

jimrr 1 month, 3 weeks ago
has anyone passed with the stuff from the new section?
upvoted 2 times

Oujsh_1 1 month, 3 weeks ago
any idea?
upvoted 3 times

jimrr 1 month, 3 weeks ago
has anyone passed with the stuff from the nez section?
upvoted 2 times

tee_dee26 1 month, 4 weeks ago
Took the exam twice, on my 1st try (Oct), I failed. I wasn't aware of this dump. I went the questions and literally 99% of the questions I saw in the exam was here. My 2nd try was a couple of days ago, all the questions came from here. All the best to those writing theirs in the nearest time.
Cheers
upvoted 1 times

Manh 2 months ago
Answer is B.

The keyword is "make several requests to dependent app". So you need trace for it.

Cloud Trace
Find performance bottlenecks in production.

Cloud Profiler
Continuous CPU and heap profiling to improve performance and reduce costs.
upvoted 4 times

SuperDevops 2 months ago
The exam real is different.
upvoted 1 times

TNT87 2 months ago
what are you saying?
upvoted 1 times

satz1234 2 months, 1 week ago
This dump is valid and and passed the exam on 1st Nov
upvoted 5 times

TNT87 2 months, 1 week ago
Help answer the questions please , like from n number 56 -81
upvoted 3 times

Alaaelanwr 2 months, 1 week ago
can you please help with the correct Answer
upvoted 2 times

jits1984 2 months, 1 week ago
Hi, how many questions did you get from this dump?
upvoted 1 times

NXD 2 months, 1 week ago
There're only 81 questions, not 88 as advertised.
upvoted 1 times

Nik22 2 months, 2 weeks ago
Lot of new questions have been added.
upvoted 2 times

TNT87 2 months, 2 weeks ago
I sent them an email last week begging them to..and they surely did
upvoted 2 times

jits1984 2 months, 1 week ago

please let us know how many questions you got from this dump in your actual exam?

upvoted 1 times

Alaaelanwr 2 months, 2 weeks ago

Hi, guys
May anyone tell me how many questions do I need to answer correctly in order to pass the exam?

upvoted 1 times

TNT87 2 months, 1 week ago

Unfortunately Google doesnt reveal anything ,even after passing the exam ,they just say pass,they dnt give you marks. Only Google knows that secret

upvoted 1 times

imperial_max 2 months, 2 weeks ago

26oct i gave exam, just 1 day back i can see more 30 questions got added wherefrom 80% of the questions are there in the exam. Unfortunately those were not discussed from the community perspective and the answers mentioned seems to be incorrect which i followed and most of it are tricky. I failed the exam. Will try again. Everyone please try to give expert opinion for the new questions from 51-81

upvoted 4 times

TNT87 2 months, 2 weeks ago

OK...i want to write the exam soon,....last week i sent them an email to update the exam and surely they did... lets try and asnwer all questions fro 56-88

upvoted 1 times

TNT87 2 months, 3 weeks ago

which dump can i use to get the latest and relevant questions?

upvoted 4 times

Question #2 Topic 1

You created a Stackdriver chart for CPU utilization in a dashboard within your workspace project. You want to share the chart with your Site Reliability Engineering
(SRE) team only. You want to ensure you follow the principle of least privilege. What should you do?

A. Share the workspace Project ID with the SRE team. Assign the SRE team the Monitoring Viewer IAM role in the workspace project.

B. Share the workspace Project ID with the SRE team. Assign the SRE team the Dashboard Viewer IAM role in the workspace project.

C. Click ג€Share chart by URLג€ and provide the URL to the SRE team. Assign the SRE team the Monitoring Viewer IAM role in the workspace project.

D. Click ג€Share chart by URLג€ and provide the URL to the SRE team. Assign the SRE team the Dashboard Viewer IAM role in the workspace project.

syslog Highly Voted 7 months, 1 week ago
I think it's C, because dashboard viewer "Read-only access to dashboard configurations."
SRE team wants to view data, not configurations.
upvoted 13 times

akg001 7 months, 1 week ago
correct there is no such role - "dashboard viewer" the correct name is monitoring dashboard configuration viewer (and the permission is - Read-only access to dashboard configurations).

so correct answer should be - C
upvoted 5 times

gcpengineer 5 months ago
but it gives access to all list in monitoring of the project.
upvoted 1 times

francisco_guerra Highly Voted 6 months, 3 weeks ago
Ans: C
this question is kind of weird because the role is: roles/monitoring.dashboardViewer "Monitoring Dashboard Configuration Viewer" but monitoring viewer its too much access so I tested in console

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

with Dashboard Viewer I would´nt be allowed to see the chart URL
with monitoring works fine

Dashboard Viewer Provides read-only access to get and list information about all monitoring data and configurations.
upvoted 5 times

gcpz Most Recent 1 week ago
Selected Answer: C
voted c
upvoted 1 times

TNT87 2 weeks ago
The answer is C...not D, do not confuse the 2 and there is no role called dashboard viewer
upvoted 1 times

azuretestingpoc 1 month, 2 weeks ago
Selected Answer: C
its Cccccccc
upvoted 1 times

TNT87 1 month, 2 weeks ago
https://cloud.google.com/monitoring/access-control#mon_roles_desc
upvoted 2 times

giammydell 2 months, 2 weeks ago
the question is: If you share a URL link containing the chart the SRE team can see the chart without knowing the workspace and the project-ID associated to the workspace
upvoted 1 times

TNT87 2 months, 2 weeks ago
Ans A,you dnt share the link,but the ID...
upvoted 2 times

maddy94 3 months, 1 week ago

why not A?
we dont have an option for sharing the chart url by clicking on share chart by URL

upvoted 1 times

sticky 3 months, 1 week ago

monitoring viewer is correct. - C

upvoted 1 times

MF2C 4 months ago

is there share chart provided by GCP dashboard? if not, A is correct

upvoted 1 times

TNT87 4 months, 1 week ago

therenis no role called dasboard viewer.

upvoted 1 times

pondai 4 months, 1 week ago

I think answer is C . I try to give user dashboard viewer and share url, but user can't watch content .If I give user Monitor Viewer and share url can watch.So I pick C

upvoted 2 times

danchoif2 4 months, 2 weeks ago

I did a test and see that:

The valid roles are: Monitoring Viewer and Monitoring Dashboard Configuration Viewer.
You can only share chart by URL using Metrics explorer.

With only Monitoring Dashboard Configuration Viewer role, user cannot see anything in Monitoring page.

I create a custom role from Monitoring Dashboard Configuration Viewer role and add resourcemanager.projects.get permission.

Now user can see list of custom dashboards and the charts in these custom dashboards. User cannot see standard GCP dashboards.

User cannot see the the chart in Metrics explorer (using the shared URL).
Opening the URL, user will see errors: "Invalid resource type" and "Invalid metric type".

So even if I ignore the typo of Dashboard Viewer role in B and D, they are still incorrect answers.

So only A and C are valid. But I think C is better because the question is: "You want to share the chart" not the whole dashboard.

upvoted 4 times

skm4690 5 months, 3 weeks ago

I think it should be C
https://cloud.google.com/monitoring/access-control
dashboard viewer role is for dashboard configuration.
monitoring viewer for monitoring.

upvoted 2 times

Charun 6 months, 2 weeks ago

I have submitted D answer

upvoted 4 times

> **TNT87** 2 weeks ago
>
> The answer is C...not D , there is no role called dashboard viwer.
>
> upvoted 1 times
>
> **WakandaF** 6 months, 2 weeks ago
>
> Have you done the exam?
>
> upvoted 1 times
>
> > **Charun** 6 months, 1 week ago
> >
> > Yes mate on 28th, passed
> >
> > upvoted 1 times

JuanitoNN 6 months, 4 weeks ago

the rol Dashboard Viewer doesn't exist in the GCP, the real name is monitoring dashboard configuration viewer, so in this case I think is C or the anwser is not correct with the rol name

upvoted 2 times

Question #3 *Topic 1*

Your organization wants to implement Site Reliability Engineering (SRE) culture and principles. Recently, a service that you support had a limited outage. A manager on another team asks you to provide a formal explanation of what happened so they can action remediations. What should you do?

A. Develop a postmortem that includes the root causes, resolution, lessons learned, and a prioritized list of action items. Share it with the manager only.

B. Develop a postmortem that includes the root causes, resolution, lessons learned, and a prioritized list of action items. Share it on the engineering organization's document portal.

C. Develop a postmortem that includes the root causes, resolution, lessons learned, the list of people responsible, and a list of action items for each person. Share it with the manager only.

D. Develop a postmortem that includes the root causes, resolution, lessons learned, the list of people responsible, and a list of action items for each person. Share it on the engineering organization's document portal.

devopsbatch Highly Voted 7 months, 1 week ago
B it could be based on this In order to maintain a healthy postmortem culture within an organization, it’s important to share postmortems as widely as possible.
upvoted 16 times

akg001 7 months, 1 week ago
agree with you for B based on blameless postmortem culture.
C and D promote blame by adding people responsible.
upvoted 3 times

alaahakim Most Recent 1 month ago
Ans: B
upvoted 1 times

Charun 6 months, 2 weeks ago
I have submitted B answer
upvoted 3 times

Question #4 *Topic 1*

You have a set of applications running on a Google Kubernetes Engine (GKE) cluster, and you are using Stackdriver Kubernetes Engine Monitoring. You are bringing a new containerized application required by your company into production. This application is written by a third party and cannot be modified or reconfigured. The application writes its log information to /var/log/app_messages.log, and you want to send these log entries to Stackdriver Logging. What should you do?

A. Use the default Stackdriver Kubernetes Engine Monitoring agent configuration.

B. Deploy a Fluentd daemonset to GKE. Then create a customized input and output configuration to tail the log file in the application's pods and write to Stackdriver Logging.

C. Install Kubernetes on Google Compute Engine (GCE) and redeploy your applications. Then customize the built-in Stackdriver Logging configuration to tail the log file in the application's pods and write to Stackdriver Logging.

D. Write a script to tail the log file within the pod and write entries to standard output. Run the script as a sidecar container with the application's pod. Configure a shared volume between the containers to allow the script to have read access to /var/log in the application container.

Charun Highly Voted 6 months, 2 weeks ago
B 100%
upvoted 11 times

alaahakim Most Recent 1 month ago
Ans: B
upvoted 1 times

syslog 1 month, 1 week ago
Selected Answer: B
Because Fluentd is created specifically for extracting logs.
https://docs.fluentd.org/input/tail
upvoted 1 times

roastc 1 month, 1 week ago
I think the correct answer is D
https://cloud.google.com/architecture/best-practices-for-operating-containers#log_aggregator_sidecar_pattern
Some applications can't be easily configured to write logs to stdout and stderr. Because such applications write to different log files on disk, the best way to handle them in Kubernetes is to use the sidecar pattern for logging.

In this solution, you add a logging agent in a sidecar container to your application (in the same pod) and share an emptyDir volume between the two containers, as shown in this YAML example on GitHub. You then configure the application to write its logs to the shared volume and configure the logging agent to read and forward them where needed.
upvoted 2 times

Manh 2 months ago
Answer is B.

D sounds good, the practice way. But the question is mention about sending log to Cloud Logging but D is just send log to shared disk
upvoted 1 times

raf2121 5 months ago
Point for discussion :

Is B the right answer ? When I was going through training content in Coursera, I read "Dont install Logging Agent in GKE nodes, as GKE are automatically enabled for Logging"

Considering this, Is D the right answer
upvoted 2 times

gcpengineer 5 months ago
Why not A?
upvoted 1 times

muhasinem 5 months, 2 weeks ago
B is correct.
https://cloud.google.com/architecture/customizing-stackdriver-logs-fluentd
upvoted 4 times

francisco_guerra 6 months, 3 weeks ago
Ans is B

Besides the list of default logs that the Logging agent streams by default, you can customize the Logging agent to send additional logs to Logging or to adjust agent settings by adding input configurations.
The configuration definitions in these sections apply to the fluent-plugin-google-cloud output plugin only and specify how logs are transformed and ingested into Cloud Logging.

https://cloud.google.com/logging/docs/agent/logging/configuration#configure

upvoted 4 times

WakandaF 6 months, 3 weeks ago

I believe that is B,
This tutorial describes how to customize Fluentd logging for a Google Kubernetes Engine cluster. You'll learn how to host your own configurable Fluentd daemonset to send logs to Cloud Logging, instead of selecting the cloud logging option when creating the Google Kubernetes Engine (GKE) cluster, which does not allow configuration of the Fluentd daemon

upvoted 3 times

ralf_cc 6 months, 4 weeks ago

B it is.

upvoted 1 times

pyc 7 months ago

It should be D.
Each sidecar container could tail a particular log file from a shared volume and then redirect the logs to its own stdout stream.
https://kubernetes.io/docs/concepts/cluster-administration/logging/
B sounds good, however, /var/log is not in the application pods IMHO. Please correct me if I am wrong here.

upvoted 1 times

syslog 6 months, 3 weeks ago

You can mount a volume wherever you want in a pod, so /var/log could exist.

upvoted 1 times

zzz 7 months, 1 week ago

I think B

upvoted 1 times

devopsbatch 7 months, 1 week ago

D i think..

upvoted 1 times

akg001 7 months, 1 week ago

Agree. answer should be D.

upvoted 2 times

rinkeshgala1 7 months, 1 week ago

why not B?

upvoted 1 times

saminlo 6 months, 3 weeks ago

just my thought process for choosing D over B (not sure if that's correct):
if there are multiple such app containers that write logs to a non-standard location then you'd have to create a custom fluentd input config for each app. Using a sidecar and running it in the same pod as the app container makes more sense since you're 'bundling' related piece of code together.

upvoted 1 times

Question #5 *Topic 1*

You are running an application in a virtual machine (VM) using a custom Debian image. The image has the Stackdriver Logging agent installed. The VM has the cloud-platform scope. The application is logging information via syslog. You want to use Stackdriver Logging in the Google Cloud Platform Console to visualize the logs. You notice that syslog is not showing up in the "All logs" dropdown list of the Logs Viewer. What is the first thing you should do?

A. Look for the agentג€™s test log entry in the Logs Viewer.

B. Install the most recent version of the Stackdriver agent.

C. Verify the VM service account access scope includes the monitoring.write scope.

D. SSH to the VM and execute the following commands on your VM: ps ax | grep fluentd.

raf2121 Highly Voted 5 months ago
Between C and D, I think D

Reason : When an instance is created, we can specify which service account the instance uses when calling Google Cloud APIs. The instance is automatically configured with access scope and one such access scope is monitoring.write (Link : https://cloud.google.com/compute/docs/access/service- read is to publish metric data and logging.write is to write compute engine logs.

Considering above, I believe D as the answer (check whether the agent is running)
upvoted 7 times

cetanx 3 months, 4 weeks ago
Agree. If you check here: https://cloud.google.com/logging/docs/agent/logging/troubleshooting#checklist
You will see that first recommended troubleshooting step is to check if the agent is running or not... So it should be D.

Also if you refer to Google Groups link provided as the answer, you will see that they first checked if the agent is running/installed.
upvoted 2 times

alaahakim Most Recent 1 month ago
Ans: D
upvoted 1 times

Wwhite44 1 month, 2 weeks ago
C is not good, “monitoring.write" is use for metric not log
upvoted 1 times

danchoif2 4 months, 2 weeks ago
https://cloud.google.com/compute/docs/access/service-accounts#associating_a_service_account_to_an_instance

When you create an instance using the gcloud command-line tool or the Google Cloud Console, you can specify which service account the instance uses when calling Google Cloud APIs. The instance is automatically configured with the following access scopes:

* https://www.googleapis.com/auth/monitoring.write
* ...

So D is better than C.
upvoted 1 times

Manumj 3 months, 1 week ago
i don't think so , reason is option-D is looking for fluent d which is specifically for customized logs , also by default the syslog will be captured with default monitoring agent and no need for fluent-d
upvoted 1 times

danchoif2 2 months, 1 week ago
https://cloud.google.com/logging/docs/agent/logging/installation

Logging agent is fluentd based (now fluentbit).

The Logging agent streams logs from your VM instances and from selected third-party software packages to Cloud Logging. It is a best practice to run the Logging agent on all your VM instances.

The VM images for Compute Engine and Amazon Elastic Compute Cloud (EC2) don't include the Logging agent, so you must complete these steps to install it on those instances. The agent runs under both Linux and Windows.

If your VMs are running in Google Kubernetes Engine or App Engine, the agent is already included in the VM image, so you can skip this page.
upvoted 1 times

luchotluchot 5 months, 1 week ago

4- Then you should check that the agent is sending data to the correct project. See the following section, Verifying Compute Engine credentials.
The link for Verifying Compute Engine credentials is https://cloud.google.com/logging/docs/agent/logging/troubleshooting#verify-creds
In this link :
a- Verifying access scopes
b- Verifying default service account permission
==> Similar to Answer C) but C) Answer talks about monitoring.write instead of logging.write. And in the question they say "The VM has the cloud-platform scope" ==> logging.write is already here.
5- Verifying the agent installation using agent's test log entry in the Logs Explorer ==> Answer A)
6- Testing the agent using ps ax | grep fluentd ==> Answer D)
So for me the good answer is A).

upvoted 1 times

luchotluchot 5 months, 1 week ago

If we follow this link : https://cloud.google.com/logging/docs/agent/logging/troubleshooting
The action (for Linux VM) are in order :
1- If Linux installation commands result in errors, then make sure that you prefix the installation commands with sudo.
2- Verify that the agent service is running on your VM instance : sudo service google-fluentd status
3- See if the agent has written error messages to the logs.

upvoted 1 times

guruguru 6 months, 3 weeks ago

C, first thing to check should be the access scope. There are 3 types of scopes, default, full access and access for each API. Even thought the default scope have the Stackdriver write access, it doesn't mean the instance has the default scope. It could be access for each API. Hence, first thing to check is the scope. After that, you can check the fluentd service in the system. C over D.

upvoted 2 times

Wwhite44 1 month, 2 weeks ago

Monitoring.write is for metric, so C is not correct. In that case logging.write was the right command. So D is the correct ANS ;)

upvoted 1 times

TNT87 6 months, 3 weeks ago

Ans C
https://cloud.google.com/logging/docs/agent/logging/troubleshooting

upvoted 2 times

TNT87 3 months, 2 weeks ago

Sorry Ans is D

upvoted 2 times

francisco_guerra 6 months, 3 weeks ago

Ans is C
Why?:
A: Does not make sense at all
B: the version it's not possible?
C: Its OK because both (scope and service account) need access to write to logging
D: Really? the question clearly says: "The image has the Stackdriver Logging agent installed."

Explanation:
Generally, you can just set the cloud-platform access scope to allow access to most of the Cloud APIs, then grant the service account only relevant IAM roles. The combination of access scopes granted to the virtual machine instance and the IAM roles granted to the service account determines the amount of access the service account has for that instance. The service account can execute API methods only if they are allowed by both the access scope and its IAM roles.

https://cloud.google.com/compute/docs/access/create-enable-service-accounts-for-instances

Please do not try to confuse people if you put your explanation add the link

upvoted 3 times

burndayl 4 weeks ago

I think the answer is D. C couldn't be right because it suggest to verify the monitoring.write scope. But this kind of scope is for monitoring agent not for logging agent. If you see here:
https://cloud.google.com/logging/docs/agent/logging/troubleshooting?hl=en
they say: If you do not have suitable access scopes in your Compute Engine instance, add the needed access scopes to your instance. The following table shows the scopes relevant to the Logging and Monitoring agents:
Access scope Agent permissions
https://www.googleapis.com/auth/logging.write Adequate for the Logging agent
https://www.googleapis.com/auth/monitoring.write Adequate for the Monitoring agent
what do you think about it?

upvoted 1 times

syslog 6 months, 1 week ago

I think it's D: https://cloud.google.com/logging/docs/agent/logging/troubleshooting#test-agent. Maybe the agent is installed but not running.

upvoted 5 times

devopsbatch 7 months, 1 week ago

C because vm need writer access and i feel D as well because fluent need to be available to export ,aggregate and process logs into stack driver monitoring tool... suggestions needed here

upvoted 3 times

Zuy01 5 months, 3 weeks ago

i think it's D, cause ans C is less precise. on question mention "logging agent" not "monitoring agent" and from here :https://cloud.google.com/logging/docs/agent/logging/troubleshooting#verifying_access_scopes
it should be "logging.write" not "monitoring.write"

upvoted 2 times

akg001 7 months ago

Default: read-only access to Storage and Service Management, write access to Stackdriver Logging and Monitoring, read/write access to Service Control.

So answer should be D

upvoted 1 times

rinkeshgala1 7 months, 1 week ago

Cloud-platform scope covers all the GCP service scope so no need to add any other scope. hence answer should be D

upvoted 1 times

Question #6 Topic 1

You use a multiple step Cloud Build pipeline to build and deploy your application to Google Kubernetes Engine (GKE). You want to integrate with a third-party monitoring platform by performing a HTTP POST of the build information to a webhook. You want to minimize the development effort. What should you do?

A. Add logic to each Cloud Build step to HTTP POST the build information to a webhook.

B. Add a new step at the end of the pipeline in Cloud Build to HTTP POST the build information to a webhook.

C. Use Stackdriver Logging to create a logs-based metric from the Cloud Build logs. Create an Alert with a Webhook notification type.

D. Create a Cloud Pub/Sub push subscription to the Cloud Build cloud-builds PubSub topic to HTTP POST the build information to a webhook.

Charun Highly Voted 6 months, 2 weeks ago
I have submitted D answer
upvoted 10 times

francisco_guerra Highly Voted 6 months, 3 weeks ago
Ans: D
Pub/Sub

A: No becauseThere is not Structure attribute to create a http request in the steps and remember you want minimize the development effort.
B: The same A
C: minimize the development effort
D: Its OK

To receive messages from push subscriptions, use a webhook and process the POST requests that Pub/Sub sends to the push endpoint. For more information about processing these POST requests in App Engine, see Writing and responding to Pub/Sub messages.

https://cloud.google.com/pubsub/docs/push
https://cloud.google.com/build/docs/subscribe-build-notifications
upvoted 7 times

alaahakim Most Recent 1 month ago
Ans : D
upvoted 1 times

muk5658 1 month, 2 weeks ago
Its D. Cloud Build -> Pubsub -> HTTP Builder
upvoted 1 times

rinkeshgala1 7 months, 1 week ago
D is correct answer
https://cloud.google.com/build/docs/subscribe-build-notifications
upvoted 2 times

akg001 7 months ago
Agree D looks correct to me.
upvoted 1 times

devopsbatch 7 months, 1 week ago
no idea on this
upvoted 1 times

Question #7 Topic 1

You use Spinnaker to deploy your application and have created a canary deployment stage in the pipeline. Your application has an in-memory cache that loads objects at start time. You want to automate the comparison of the canary version against the production version. How should you configure the canary analysis?

A. Compare the canary with a new deployment of the current production version.

B. Compare the canary with a new deployment of the previous production version.

C. Compare the canary with the existing deployment of the current production version.

D. Compare the canary with the average performance of a sliding window of previous production versions.

rinkeshgala1 Highly Voted 7 months, 1 week ago
i guess A
https://spinnaker.io/guides/user/canary/
upvoted 13 times

giammydell 2 months, 2 weeks ago
Correct in the link: "You might be tempted to compare the canary deployment against your current production deployment. Instead always compare the canary against an equivalent baseline, deployed at the same time."
upvoted 2 times

DucLee3110 7 months ago
A is correct.
https://cloud.google.com/architecture/automated-canary-analysis-kubernetes-engine-spinnaker
https://spinnaker.io/guides/user/canary/best-practices/#compare-canary-against-baseline-not-against-production
upvoted 2 times

akg001 7 months ago
Agree with - A is the correct one.
https://cloud.google.com/architecture/automated-canary-analysis-kubernetes-engine-spinnaker
upvoted 1 times

francisco_guerra Highly Voted 6 months, 3 weeks ago
Ans A

https://spinnaker.io/guides/user/canary/best-practices/#compare-canary-against-baseline-not-against-production
You might be tempted to compare the canary deployment against your current production deployment. Instead always compare the canary against an equivalent baseline, deployed at the same time.

The baseline uses the same version and configuration that is currently running in production, but is otherwise identical to the canary:

Same time of deployment
Same size of deployment
Same type and amount of traffic
In this way, you control for version and configuration only, and you reduce factors that could affect the analysis, like the cache warmup time, the heap size, and so on.
upvoted 9 times

MF2C 2 months, 1 week ago
yes correct
upvoted 1 times

gcpz Most Recent 1 week ago
Selected Answer: A
A is the correct answer
upvoted 1 times

alaahakim 1 month ago
Ans : A
upvoted 1 times

lucabinc 1 month, 1 week ago
Selected Answer: A
100% A
upvoted 1 times

Charun 6 months, 2 weeks ago
I have submitted A
upvoted 4 times

devopsbatch 7 months, 1 week ago

i think B

upvoted 1 times

Question #8 Topic 1

You support a high-traffic web application and want to ensure that the home page loads in a timely manner. As a first step, you decide to implement a Service
Level Indicator (SLI) to represent home page request latency with an acceptable page load time set to 100 ms. What is the Google-recommended way of calculating this SLI?

A. Bucketize the request latencies into ranges, and then compute the percentile at 100 ms.

B. Bucketize the request latencies into ranges, and then compute the median and 90th percentiles.

C. Count the number of home page requests that load in under 100 ms, and then divide by the total number of home page requests.

D. Count the number of home page request that load in under 100 ms, and then divide by the total number of all web application requests.

Charun Highly Voted 6 months, 2 weeks ago
I have submitted C answer
upvoted 9 times

raf2121 5 months ago
https://sre.google/workbook/implementing-slos/
In the SRE principles book, it's recommended treating the SLI as the ratio of two numbers: the number of good events divided by the total number of events. For example:
Number of successful HTTP requests / total HTTP requests (success rate)
upvoted 2 times

danchoif2 Highly Voted 4 months, 2 weeks ago
A, B and D: aren't specific to home page, so they are incorrect.

C is correct.
upvoted 6 times

alaahakim Most Recent 1 month ago
Ans: C
upvoted 1 times

WakandaF 6 months, 3 weeks ago
B or C?
upvoted 1 times

TNT87 6 months, 3 weeks ago
Ans C
https://sre.google/workbook/implementing-slos/
upvoted 5 times

francisco_guerra 6 months, 3 weeks ago
Ans is B
After a lot of research i find out this:

The SLI for availability indicates whether the service is working. The SLI for availability is defined as follows:
The proportion of valid requests served successfully. (good request / total request)

The SLI for latency (sometimes called speed) indicates whether the service is fast enough.
The proportion of valid requests served faster than a threshold.
Latency is commonly measured as a distribution. Given a distribution, you can measure various percentiles. For example, you might measure the number of requests that are slower than the historical 99th percentile. In this case, we consider good events to be events that are faster than this threshold, which was set by examining the historical distribution. You can also set this threshold based on product requirements. You can even set multiple latency SLOs, for example typical latency versus tail latency.
upvoted 3 times

Dark_Lord 5 months, 3 weeks ago
The correct answer is "C", you can confirm it here, https://sre.google/workbook/slo-document/

Latency

The proportion of sufficiently fast requests, as measured from the load balancer metrics.

“Sufficiently fast” is defined as < 400 ms, or < 850 ms.

count of "api" http_requests with
a duration less than or equal to
"0.4" seconds
divided by
count of all "api" http_requests

upvoted 2 times

Dark_Lord 5 months, 3 weeks ago

Still not sure about B

upvoted 1 times

francisco_guerra 6 months, 3 weeks ago

and if this is not enough for you check how google calculate Availability and latency

Availability

sum(rate(http_requests_total{host="api", status!~"5.."}[7d]))
/
sum(rate(http_requests_total{host="api"}[7d])

Latency
histogram_quantile(0.9, rate(http_request_duration_seconds_bucket[7d]))
histogram_quantile(0.99, rate(http_request_duration_seconds_bucket[7d]))

https://sre.google/workbook/implementing-slos/
https://cloud.google.com/architecture/adopting-slos/

upvoted 1 times

akg001 7 months ago

Answer -C

SLI = good events/valid events X 100

upvoted 4 times

akg001 7 months ago

Answer -C

SLI = good events/good events X 100

upvoted 4 times

devopsbatch 7 months, 1 week ago

answer C

upvoted 5 times

Question #9 Topic 1

You deploy a new release of an internal application during a weekend maintenance window when there is minimal user tragic. After the window ends, you learn that one of the new features isn't working as expected in the production environment. After an extended outage, you roll back the new release and deploy a fix.

You want to modify your release process to reduce the mean time to recovery so you can avoid extended outages in the future. What should you do? (Choose two.)

A. Before merging new code, require 2 different peers to review the code changes.

B. Adopt the blue/green deployment strategy when releasing new code via a CD server.

C. Integrate a code linting tool to validate coding standards before any code is accepted into the repository.

D. Require developers to run automated integration tests on their local development environments before release.

E. Configure a CI server. Add a suite of unit tests to your code and have your CI server run them on commit and verify any changes.

Charun Highly Voted 6 months, 2 weeks ago
ans BE
upvoted 24 times

francisco_guerra Highly Voted 6 months, 3 weeks ago
Ans: B & E

A: No, More peers to review dont automate anything
B: Ok CD
C: No, Linting is for code format
D: No, Integration test are needed but its better automatically
E: Ok CI

CI/CD its OK
upvoted 12 times

simbu1299 Most Recent 6 days, 20 hours ago
Selected Answer: BE
Answer is B & E
upvoted 1 times

dturan 3 weeks, 4 days ago
Selected Answer: BE
ans BE
upvoted 1 times

PJ_2021 1 month, 3 weeks ago
Selected Answer: BE
Answer is B E
upvoted 3 times

Manh 2 months ago
BE is good for CI/CD practices
upvoted 1 times

TNT87 4 months, 1 week ago
A & B
upvoted 2 times

JuanitoNN 6 months, 3 weeks ago
I think B,D
upvoted 1 times

ralf_cc 6 months, 3 weeks ago
Reduce MTTR - B Blue/Green, E tests on CI
upvoted 4 times

akg001 7 months ago
A and B looks good option as in question they asked to modify the release process.
upvoted 1 times

DucLee3110 7 months, 1 week ago
AB are good, but C looks ok also

upvoted 1 times

devopsbatch 7 months, 1 week ago

A and B

upvoted 1 times

Question #10 Topic 1

You have a pool of application servers running on Compute Engine. You need to provide a secure solution that requires the least amount of configuration and allows developers to easily access application logs for troubleshooting. How would you implement the solution on GCP?

A. ג€¢ Deploy the Stackdriver logging agent to the application servers. ג€¢ Give the developers the IAM Logs Viewer role to access Stackdriver and view logs.

B. ג€¢ Deploy the Stackdriver logging agent to the application servers. ג€¢ Give the developers the IAM Logs Private Logs Viewer role to access Stackdriver and view logs.

C. ג€¢ Deploy the Stackdriver monitoring agent to the application servers. ג€¢ Give the developers the IAM Monitoring Viewer role to access Stackdriver and view metrics.

D. ג€¢ Install the gsutil command line tool on your application servers. ג€¢ Write a script using gsutil to upload your application log to a Cloud Storage bucket, and then schedule it to run via cron every 5 minutes. ג€¢ Give the developers the IAM Object Viewer access to view the logs in the specified bucket.

devopsbatch Highly Voted 7 months, 1 week ago
A
roles/logging.viewer (Logs Viewer) gives you read-only access to all features of Logging, except Access Transparency logs and Data Access audit logs.
upvoted 17 times

akg001 7 months ago
correct - A . least privilege principle
upvoted 5 times

Charun Highly Voted 6 months, 2 weeks ago
correct A
upvoted 6 times

roastc Most Recent 1 day, 3 hours ago
Looks like answer A is correct. A logging agent is required to enable the custom logs pushed to Stackdriver https://cloud.google.com/logging/docs/agent/logging . Developers need only Log Viewer permission, which is enough in this case and Private Log viewer is a superset of log viewer permission with elevated permission to view the private data in logs. Which is not needed in this case.
upvoted 1 times

simbu1299 6 days, 20 hours ago
Correct Answer is A
upvoted 1 times

scjs 1 week ago
B is correct as it talks about application logs
https://cloud.google.com/logging/docs/access-control

The Logs Viewer role doesn't let you read the Data Access audit logs that are in the _Default bucket

roles/logging.privateLogViewer (Private Logs Viewer) includes all the permissions contained by roles/logging.viewer, plus the ability to read Data Access audit logs in the _Default
upvoted 1 times

alaahakim 1 month ago
Ans : A
upvoted 1 times

Wwhite44 1 month, 1 week ago
Selected Answer: A
A is good
upvoted 2 times

Manh 2 months ago
A for sure
upvoted 1 times

danchoif2 4 months, 2 weeks ago
https://cloud.google.com/logging/docs/audit#access-control

A is correct.
B is incorrect because developers only need to access application logs, not private logs.

upvoted 4 times

Question #11 Topic 1

You support the backend of a mobile phone game that runs on a Google Kubernetes Engine (GKE) cluster. The application is serving HTTP requests from users.
You need to implement a solution that will reduce the network cost. What should you do?

A. Configure the VPC as a Shared VPC Host project.

B. Configure your network services on the Standard Tier.

C. Configure your Kubernetes cluster as a Private Cluster.

D. Configure a Google Cloud HTTP Load Balancer as Ingress.

francisco_guerra Highly Voted 6 months, 3 weeks ago
Ans is D

A: No, Doest make sense
B: Who says that we are using a premium tier?
C: This does not help with the network cost?
D: Ok :)
Costs associated with a load balancer are charged to the project containing the load balancer components.
Because of these benefits, container-native load balancing is the recommended solution for load balancing through Ingress. When NEGs are used with GKE Ingress, the Ingress controller facilitates the creation of all aspects of the L7 load balancer. This includes creating the virtual IP address, forwarding rules, health checks, firewall rules, and more.

https://cloud.google.com/architecture/best-practices-for-running-cost-effective-kubernetes-applications-on-gke
upvoted 13 times

syslog 6 months, 3 weeks ago
Who says that we aren't use the load balancer?
I think it's B anyway, because you have to choose standard tier when "Cost is your main consideration, and you're willing to trade-off some network performance"
https://cloud.google.com/network-tiers
upvoted 6 times

exploregcp Highly Voted 5 months, 3 weeks ago
Ans is C.
Private cluster has only private IP assigned to nodes. As this is backend service public IPs are not required. Public IPs are are chargable.
https://cloud.google.com/architecture/prep-kubernetes-engine-for-prod#private_clusters
D is not correct. Ingress traffic is not charged. Hence will not help in network cost saving.
upvoted 5 times

Wwhite44 Most Recent 3 weeks, 3 days ago
Selected Answer: B
Standard Tier for sure, B
upvoted 1 times

not_thanos 3 weeks, 4 days ago
Selected Answer: D
https://cloud.google.com/architecture/prep-kubernetes-engine-for-prod#configuring_your_services_in_kubernetes_to_receive_internet_traffic

Ans is D
upvoted 1 times

ESP_SAP 1 month, 1 week ago
Correct Answer is D:
https://cloud.google.com/vpc/network-pricing

Ingress pricing
Traffic type Price
Ingress
No charge for ingress traffic. However there may be a charge for resource that processes ingress traffic. Services that process ingress traffic are as follows:

Load balancers
Cloud NAT
Protocol forwarding
Responses to requests count as egress are charged.
upvoted 3 times

Omni_Omnom 1 month, 1 week ago
Selected Answer: D

https://cloud.google.com/vpc/network-pricing
upvoted 3 times

Tire 1 month, 2 weeks ago
GKE setting Private cluster is immutable. This setting can only be set during the GKE cluster provisioning. So based on the fact that we already are using it, C is not an option.
upvoted 1 times

TNT87 1 month, 2 weeks ago
https://cloud.google.com/vpc/network-pricing
Ans D
upvoted 1 times

Manh 2 months ago
I think should be B
Standard tier reduce cost than premium tier

A no way
C private cluster need additional resource for ingress and egress like NAT
D configure HTTP LB, it's make more cost

https://cloud.netapp.com/blog/gcp-cvo-blg-gcp-network-pricing-how-to-beat-the-hidden-fees
upvoted 2 times

Debarati1 2 months, 4 weeks ago
Can someone confirm B or d?
upvoted 1 times

danchoif2 2 months, 1 week ago
See the explaination of syslog.
upvoted 1 times

MF2C 4 months ago
Standard Tier offers a lower-cost alternative for the following use cases:

You have applications that are not latency or performance sensitive.

Mobile gaming cannot choose B
upvoted 4 times

Charun 6 months, 2 weeks ago
D 100%
upvoted 3 times

zzz 7 months, 1 week ago
I think B
upvoted 4 times

devopsbatch 7 months, 1 week ago
D ingress is an internal LB and it can handle http request based on path rules
upvoted 4 times

DucLee3110 7 months, 1 week ago
but how is it related to reduce network cost?
upvoted 3 times

rinkeshgala1 7 months, 1 week ago
Correct answer should be option B
upvoted 5 times

akg001 7 months ago
B - looks good.
upvoted 3 times

Question #12 *Topic 1*

You encountered a major service outage that affected all users of the service for multiple hours. After several hours of incident management, the service returned to normal, and user access was restored. You need to provide an incident summary to relevant stakeholders following the Site Reliability Engineering recommended practices. What should you do first?

A. Call individual stakeholders to explain what happened.

B. Develop a post-mortem to be distributed to stakeholders.

C. Send the Incident State Document to all the stakeholders.

D. Require the engineer responsible to write an apology email to all stakeholders.

devopsbatch Highly Voted 7 months, 1 week ago
B postmortem analysis report to stakeholders
upvoted 16 times

akg001 7 months ago
correct.
upvoted 1 times

chidambaram Most Recent 3 weeks, 6 days ago
Selected Answer: B
As per SRE culture, postmortem is the correct one.
upvoted 1 times

alaahakim 1 month ago
Selected Answer: B
Ans : B
upvoted 2 times

Wwhite44 1 month, 1 week ago
Selected Answer: B
B for sure
upvoted 2 times

edner 1 month, 3 weeks ago
Selected Answer: B
B, blameless postmortem
https://sre.google/sre-book/postmortem-culture/
upvoted 2 times

Charun 6 months, 2 weeks ago
B correct
upvoted 3 times

francisco_guerra 6 months, 3 weeks ago
A: No
B: Correct
C: No, Incident State document is used for consultation with incident participants.
D: No, Blameless
upvoted 4 times

You are performing a semi-annual capacity planning exercise for your flagship service. You expect a service user growth rate of 10% month-over-month over the next six months. Your service is fully containerized and runs on Google Cloud Platform (GCP), using a Google Kubernetes Engine (GKE) Standard regional cluster on three zones with cluster autoscaler enabled. You currently consume about 30% of your total deployed CPU capacity, and you require resilience against the failure of a zone. You want to ensure that your users experience minimal negative impact as a result of this growth or as a result of zone failure, while avoiding unnecessary costs. How should you prepare to handle the predicted growth?

A. Verify the maximum node pool size, enable a horizontal pod autoscaler, and then perform a load test to verify your expected resource needs.

B. Because you are deployed on GKE and are using a cluster autoscaler, your GKE cluster will scale automatically, regardless of growth rate.

C. Because you are at only 30% utilization, you have significant headroom and you wonג€™t need to add any additional capacity for this rate of growth.

D. Proactively add 60% more node capacity to account for six months of 10% growth rate, and then perform a load test to make sure you have enough capacity.

Charun Highly Voted 6 months, 2 weeks ago
answer A
upvoted 15 times

francisco_guerra Highly Voted 6 months, 3 weeks ago
A: Correct. The Horizontal Pod Autoscaler changes the shape of your Kubernetes workload by automatically increasing or decreasing the number of Pods in response to the workload's CPU or memory consumption
B: Incorrect. It is not based on the CPU its based on the workload
C: No, Hope is not an strategy
D: No, have more resource than needed
upvoted 12 times

burndayl Most Recent 1 month ago
C for me: 30% of total deployed CPU consumption mean 10% of CUP on each zone; 10% of increment month-over-month mean at the beginning of the second mont you will have 11% of CPU, at the tird 12,1% and so on; you can easly accomodate a fault of a zone; you don't have additional cost
upvoted 1 times

alaahakim 1 month ago
Selected Answer: A
Ans: A
upvoted 1 times

Bala999 1 month, 2 weeks ago
Selected Answer: A
Correct answer A.
upvoted 1 times

Manh 2 months ago
answer A
upvoted 1 times

akg001 7 months ago
The correct answer - A
https://cloud.google.com/kubernetes-engine/docs/concepts/horizontalpodautoscaler
upvoted 3 times

> **Trony** 2 months, 2 weeks ago
> Agreed: Cluster autoscaler will add additional nodes if some pods can't be scheduled, but you need something to add new pods when load increases, and that is HPA.
> upvoted 1 times

zzz 7 months, 1 week ago
I think A
upvoted 1 times

devopsbatch 7 months, 1 week ago
B autoscaler will take care of user growth
upvoted 1 times

> **DucLee3110** 7 months, 1 week ago

I think A, as it mentioned "while avoiding unnecessary costs", if you set cluster autoscaler but have max node, it can also impact user. A can verify what is max size based on your load.

upvoted 1 times

rinkeshgala1 7 months, 1 week ago

what if there is a shortage of nodes then how cluster will auto scale. also, cluster auto scaler will take of under utilized nodes as well. so eventually you will save cost.
so option B should be the choice right ?

upvoted 3 times

DucLee3110 7 months, 1 week ago

A is still the option, as you already enable Node Autoscaler in the question, but you need to verify the max node in the node pool based on your load, if not, if the load increase and you reach the max node in the node pool, it still has down time

upvoted 1 times

Question #14 Topic 1

Your application images are built and pushed to Google Container Registry (GCR). You want to build an automated pipeline that deploys the application when the image is updated while minimizing the development effort. What should you do?

A. Use Cloud Build to trigger a Spinnaker pipeline.

B. Use Cloud Pub/Sub to trigger a Spinnaker pipeline.

C. Use a custom builder in Cloud Build to trigger Jenkins pipeline.

D. Use Cloud Pub/Sub to trigger a custom deployment service running in Google Kubernetes Engine (GKE).

MF2C Highly Voted 4 months ago
B is correct : https://cloud.google.com/architecture/continuous-delivery-toolchain-spinnaker-cloud#triggering_a_spinnaker_pipeline_when_a_docker_image_is_pushed_to_container_registry
upvoted 12 times

Charun Highly Voted 6 months, 2 weeks ago
B is correct
upvoted 6 times

alaahakim Most Recent 1 month ago
Ans : B
upvoted 1 times

Luvero 2 months, 2 weeks ago
Its B

Google Cloud Build vs Spinnaker: What are the differences?

What is Google Cloud Build? Continuously build, test, and deploy. Cloud Build lets you build software quickly across all languages. Get complete control over defining custom workflows for building, testing, and deploying across multiple environments such as VMs, serverless, Kubernetes, or Firebase.

What is Spinnaker? Multi-cloud continuous delivery platform for releasing software changes with high velocity and confidence. Created at Netflix, it has been battle-tested in production by hundreds of teams over millions of deployments. It combines a powerful and flexible pipeline management system with integrations to the major cloud providers.

Google Cloud Build and Spinnaker belong to "Continuous Deployment" category of the tech stack.
upvoted 1 times

gcpengineer 5 months ago
A is the answer
upvoted 1 times

Dark_Lord 5 months, 3 weeks ago
B, the pub/sub can trigger any deployment tool(spinnaker, cloud Run etc), but in platform native approach is to use spinnnaker.

You can also validate this, because they have only used platform native tools in the question like google container registry(instead of docker hub)
upvoted 4 times

TNT87 4 months, 1 week ago
no no no
upvoted 1 times

TNT87 4 months, 1 week ago
eyyy,sorry meant B
upvoted 2 times

MikeFR 6 months ago
OK for B but there is mistake by saying to bigger instead of to trigger
upvoted 2 times

holahola 6 months, 3 weeks ago
B is correct, because it says that image is built already, then there must be a trigger of some sort for spinnaker. Cloud Build does not trigger Spinnaker itself. Cloud Pub/Sub trigger can be configured in Spinnaker as documented: https://spinnaker.io/guides/user/pipeline/triggers/pubsub/
upvoted 2 times

MFay 7 months ago
Sorry the correct is D. Cloud Pub/Sub can trigger custom deployment service like Spinnaker pipeline etc.
upvoted 1 times

akg001 7 months ago

instead of using custom deployment service. We should focus on native tools for deployment. so should be -B the right option.

upvoted 2 times

MFay 7 months ago

B is correct.

upvoted 1 times

akg001 7 months ago

agree B looks correct.
https://cloud.google.com/architecture/continuous-delivery-toolchain-spinnaker-cloud

upvoted 1 times

devopsbatch 7 months, 1 week ago

A cloud build spinakker pipeline

upvoted 3 times

rinkeshgala1 7 months, 1 week ago

Cloud build directly can't trigger spinnaker pipeline. you have to use cloud pub/sub to trigger spinnaker pipeline. (In the backend it will use cloud build notifiers

upvoted 3 times

Question #15 Topic 1

Your product is currently deployed in three Google Cloud Platform (GCP) zones with your users divided between the zones. You can fail over from one zone to another, but it causes a 10-minute service disruption for the affected users. You typically experience a database failure once per quarter and can detect it within five minutes. You are cataloging the reliability risks of a new real-time chat feature for your product. You catalog the following information for each risk:
* Mean Time to Detect (MTTD) in minutes
* Mean Time to Repair (MTTR) in minutes
* Mean Time Between Failure (MTBF) in days
* User Impact Percentage
The chat feature requires a new database system that takes twice as long to successfully fail over between zones. You want to account for the risk of the new database failing in one zone. What would be the values for the risk of database failover with the new system?

A. MTTD: 5 MTTR: 10 MTBF: 90 Impact: 33%

B. MTTD: 5 MTTR: 20 MTBF: 90 Impact: 33%

C. MTTD: 5 MTTR: 10 MTBF: 90 Impact: 50%

D. MTTD: 5 MTTR: 20 MTBF: 90 Impact: 50%

Charun Highly Voted 6 months, 2 weeks ago
B 100%
upvoted 12 times

rinkeshgala1 Highly Voted 7 months, 1 week ago
B
MTR will increase to 20
upvoted 7 times

alaahakim Most Recent 1 month ago
Ans : B
upvoted 1 times

MF2C 4 months ago
How to cal User Impact Percentage?
upvoted 1 times

MF2C 2 months, 1 week ago
Because of 3 zones, one zone fail is 33%
upvoted 2 times

TNT87 4 months, 1 week ago
B
https://www.atlassian.com/incident-management/kpis/common-metrics
https://linkedin.github.io/school-of-sre/
upvoted 3 times

francisco_guerra 6 months, 3 weeks ago
I think its B
because the impacted users should be the same 33%
upvoted 3 times

devopsbatch 7 months, 1 week ago
i think A
upvoted 2 times

syslog 7 months, 1 week ago
Why A?
"the new database system that takes twice as long to successfully fail over between zones" so it takes 20 minutes to recover. MTTR=20, three zones means 33% of involved users. For me it's B.
upvoted 4 times

DucLee3110 7 months, 1 week ago
as it is 3 zones?
upvoted 1 times

Question #16 Topic 1

You are managing the production deployment to a set of Google Kubernetes Engine (GKE) clusters. You want to make sure only images which are successfully built by your trusted CI/CD pipeline are deployed to production. What should you do?

A. Enable Cloud Security Scanner on the clusters.

B. Enable Vulnerability Analysis on the Container Registry.

C. Set up the Kubernetes Engine clusters as private clusters.

D. Set up the Kubernetes Engine clusters with Binary Authorization.

devopsbatch Highly Voted 7 months, 1 week ago

D because binary authorization is deploy time security tool and it will allow only trusted and attested containers into GKE

upvoted 18 times

pondai Most Recent 1 day, 5 hours ago

D https://cloud.google.com/binary-authorization/?hl=zh-tw&utm_source=google&utm_medium=cpc&utm_campaign=japac-TW-all-en-dr-bkws-all-all-trial-e-dr-1009882&utm_content=text-ad-none-none-DEV_c-CRE_284325707741-ADGP_Hybrid%20%7C%20BKWS%20-%20EXA%20%7C%20Txt%20~%20Security%20and%20Identity%20~%20Binary%20Authorization_binary%20authorization-KWID_43700035200283171-kwd-473575914620&userloc_9040379-network_g&utm_term=KW_gcp%20binary%20authorization&gclid=CjwKCAiArOqOBhBmEiwAsgeLmXG4Cu1unuvnKxmO7tAykQtTp-q-jDNRi-mBpNES-S5xNMPb6qSLJBoCTxQQAvD_BwE&gclsrc=aw.ds

upvoted 1 times

simbu1299 1 day, 12 hours ago

Selected Answer: D

Correct Answer is D

upvoted 1 times

Wwhite44 3 weeks, 2 days ago

Selected Answer: D

D clear

upvoted 1 times

not_thanos 3 weeks, 4 days ago

Selected Answer: D

https://cloud.google.com/binary-authorization/docs/overview

upvoted 1 times

alaahakim 1 month ago

Ans: D

upvoted 2 times

exploregcp 5 months, 3 weeks ago

D

https://cloud.google.com/binary-authorization/docs/overview

upvoted 4 times

WakandaF 6 months, 2 weeks ago

erminology. Binary Authorization is a deploy time security service provided by Google that ensures that only trusted containers are deployed in our GKE cluster. It uses a policy driven model that allows us to configure security policies. Behind the scenes, this service talks to the Container Analysis service

upvoted 3 times

Charun 6 months, 2 weeks ago

D 100%

upvoted 4 times

Question #17 Topic 1

You support an e-commerce application that runs on a large Google Kubernetes Engine (GKE) cluster deployed on-premises and on Google Cloud Platform. The application consists of microservices that run in containers. You want to identify containers that are using the most CPU and memory. What should you do?

A. Use Stackdriver Kubernetes Engine Monitoring.

B. Use Prometheus to collect and aggregate logs per container, and then analyze the results in Grafana.

C. Use the Stackdriver Monitoring API to create custom metrics, and then organize your containers using groups.

D. Use Stackdriver Logging to export application logs to BigQuery, aggregate logs per container, and then analyze CPU and memory consumption.

Charun Highly Voted 6 months, 2 weeks ago
B correct
upvoted 10 times

raf2121 5 months ago
Point for discussion :
Google highly recommends Google Logging and monitoring when running workloads only on GKE on-prem and GKE. For applications with component running on GKE on-prem and traditional on-premises infrastructure, other monitoring and logging solutions for an end-to-end view of application can be considered

considering what is stated in the question "GKE cluster deployed on-premises and Google Cloud Platform", should "A" be the answer
upvoted 11 times

danchoif2 Highly Voted 4 months, 1 week ago
* https://cloud.google.com/anthos/clusters/docs/on-prem
GKE on-prem is also called Anthos clusters on VMware

* https://cloud.google.com/anthos/clusters/docs/on-prem/concepts/logging-and-monitoring
You have several logging and monitoring options for your Anthos clusters on VMware:
+ Cloud Logging and Cloud Monitoring, enabled by in-cluster agents deployed with Anthos clusters on VMware.
+ Prometheus and Grafana, disabled by default.
+ Validated configurations with third-party solutions.

=> it means, if not a special situation, the correct should be using the first option: Logging and Monitoring. In this case, we want metrics, so Monitoring (aka. Cloud Monitoring, Stackdriver Monitoring) should be used. We are talking about GKE, so we will use Kubernetest Engine Monitoring (https://cloud.google.com/kubernetes-engine-monitoring).

Obviously, A is correct.
upvoted 9 times

simbu1299 Most Recent 6 days, 15 hours ago
Selected Answer: A
Correct Answer is A
upvoted 1 times

TNT87 2 weeks ago
Selected Answer: A
A is the answer...check GKE monitoring onthe doc
upvoted 1 times

guid1984 2 weeks, 6 days ago
The question is application is running on Google Kubernetes Engine (GKE) cluster deployed on-premises and also on the Google Cloud Platform, this means we need to add grouping for containers that are running on-prem GKE and also in GKE GCP. Option C is more relevant in this case as compared to A
upvoted 1 times

alaahakim 1 month ago
Ans : B
upvoted 1 times

TNT87 1 month ago
C is he answer, B is not in GCP
https://cloud.google.com/anthos/clusters/docs/on-prem/1.0/concepts/logging-and-monitoring
upvoted 1 times

muk5658 1 month, 2 weeks ago
Selected Answer: A

Cloud Logging and Cloud Monitoring, enabled by in-cluster agents deployed with GKE on-prem.

Reference:https://cloud.google.com/anthos/clusters/docs/on-prem/1.5/concepts/logging-and-monitoring

upvoted 1 times

awrgdasfg 1 month, 3 weeks ago

Selected Answer: A

https://cloud.google.com/anthos/clusters/docs/on-prem/1.9/concepts/logging-and-monitoring#logging_and_monitoring

upvoted 1 times

Biden 1 month, 4 weeks ago

Answer is A. Reason - this statement "We highly recommend Logging and Monitoring when running workloads only on GKE on-prem, or workloads on GKE and GKE on-prem. For applications with components running on GKE on-prem and traditional on-premises infrastructure, you might consider other solutions for an end-to-end view of those applications."
THis question is about app running on GKE on-prem & GKE on Cloud - hence answer is A
Reference: https://cloud.google.com/anthos/clusters/docs/on-prem/1.5/concepts/logging-and-monitoring

upvoted 1 times

Manh 2 months ago

it's should be A

Options for GKE on-prem
You have several logging and monitoring options for your GKE on-prem clusters:

Cloud Logging and Cloud Monitoring, enabled by in-cluster agents deployed with GKE on-prem.
Prometheus and Grafana, disabled by default.
Validated configurations with third-party solutions.
https://cloud.google.com/anthos/clusters/docs/on-prem/1.5/concepts/logging-and-monitoring#stackdriver_gkeop

upvoted 1 times

MF2C 4 months ago

B- You have several logging and monitoring options for your GKE On-Prem clusters:

Cloud Logging and Cloud Monitoring, enabled by in-cluster agents deployed with GKE On-Prem.
Prometheus and Grafana, enabled by default in new clusters.

upvoted 2 times

TNT87 4 months, 1 week ago

B
https://cloud.google.com/anthos/clusters/docs/on-prem/1.7/concepts/logging-and-monitoring

upvoted 2 times

grace_lau 5 months, 2 weeks ago

1. both prometheus & stackdriver need to be configured
2. Prometheus doesn't collect & aggregate logs, it only plays metrics.
3. stackdriver is a default component for GKE on-prem
I would choose C.

upvoted 3 times

WakandaF 6 months, 2 weeks ago

Monitoring(Stackdriver) allows you to view and address that type of behavior, but yes you need to have Anthos!
Not sure if is A or B?

upvoted 2 times

luchotluchot 5 months, 1 week ago

The application runs on a large Google Kubernetes Engine (GKE) cluster deployed on-premises and on Google Cloud Platform ==> so they use Anthos (GKE on PREM = Anthos).
The answer is A.

upvoted 3 times

guruguru 6 months, 2 weeks ago

A - because CPU and memory are standard metrics, you shouldn't need to create any custom metric for them. And as holahola mentioned, "Cloud Monitoring monitors GKE on-prem clusters in a similar way as cloud-based GKE clusters."
https://cloud.google.com/anthos/clusters/docs/on-prem/1.7/concepts/logging-and-monitoring

upvoted 3 times

francisco_guerra 6 months, 2 weeks ago

Like you say Cloud monitoring is not the same that Kubernetes engine monitoring

upvoted 2 times

francisco_guerra 6 months, 3 weeks ago

Ans: C

A: No, Cloud Operations for GKE (Stackdriver Kubernetes Engine Monitoring)only displays information for GKE clusters running on Google Cloud. It doesn't display information for GKE clusters running anywhere else, for example using on-premise or bare-metal servers.

B: Google only recommed prometeus and Grafana if you have previous knowledge about it

C: Correct its the Google's recommendation
D: You want to monitoring

https://cloud.google.com/stackdriver/docs/solutions/gke

https://cloud.google.com/anthos/clusters/docs/on-prem/1.7/concepts/logging-and-monitoring

upvoted 3 times

gcpengineer 5 months ago

stackdiver monitoring displays GKE on prem.

upvoted 1 times

Question #18 *Topic 1*

Your company experiences bugs, outages, and slowness in its production systems. Developers use the production environment for new feature development and bug fixes. Configuration and experiments are done in the production environment, causing outages for users. Testers use the production environment for load testing, which often slows the production systems. You need to redesign the environment to reduce the number of bugs and outages in production and to enable testers to toad test new features. What should you do?

A. Create an automated testing script in production to detect failures as soon as they occur.

B. Create a development environment with smaller server capacity and give access only to developers and testers.

C. Secure the production environment to ensure that developers can't change it and set up one controlled update per year.

D. Create a development environment for writing code and a test environment for configurations, experiments, and load testing.

devopsbatch Highly Voted 7 months, 1 week ago

D i think creating seperate env for dev and testers

upvoted 16 times

Charun Highly Voted 6 months, 2 weeks ago

answer is D

upvoted 6 times

not_thanos Most Recent 3 weeks, 4 days ago

Selected Answer: D

Best practice to separate the dev and test environments

upvoted 1 times

Yog14 3 weeks, 4 days ago

Selected Answer: D

D because Developrs can test in Dev with out touching PR environment

upvoted 1 times

alaahakim 1 month ago

Selected Answer: D

Ans : D

upvoted 1 times

Wwhite44 1 month, 1 week ago

Selected Answer: D

D for sure

upvoted 1 times

pacman_user 3 months ago

D for sure 100% recommended

upvoted 2 times

akg001 7 months ago

Having a separate environment is a best practice. Answer is D.

upvoted 5 times

Question #19 Topic 1

You support an application running on App Engine. The application is used globally and accessed from various device types. You want to know the number of connections. You are using Stackdriver Monitoring for App Engine. What metric should you use?

A. flex/connections/current

B. tcp_ssl_proxy/new_connections

C. tcp_ssl_proxy/open_connections

D. flex/instance/connections/current

francisco_guerra Highly Voted 6 months, 3 weeks ago
Ans A
A: Metric for App engine & for version
B: NO, Metrics for Cloud Load Balancing.
C: NO, Metrics for Cloud Load Balancing.
D Metric for App engine & for instance

An App Engine app is made up of a single application resource that consists of one or more services. Each service can be configured to use different runtimes and to operate with different performance settings. Within each service, you deploy versions of that service. Each version then runs within one or more instances, depending on how much traffic you configured it to handle.

if the version runs within one or more instances we need for the version.
upvoted 14 times

danchoif2 2 months, 1 week ago
agree, the question is about number of connections of the app (could be multiple instances), not an instance.
upvoted 1 times

ralf_cc Highly Voted 6 months, 3 weeks ago
A it is
upvoted 5 times

alaahakim Most Recent 1 month ago
Ans : A
upvoted 1 times

TNT87 4 months, 1 week ago
A
https://cloud.google.com/monitoring/api/metrics_gcp#gcp-appengine
upvoted 4 times

Charun 6 months, 2 weeks ago
A correct
upvoted 4 times

devopsbatch 7 months, 1 week ago
flex/instance/connections/current GA
Connections
GAUGE, DOUBLE, 1
gae_instance Number of current active connections per App Engine flexible environment instance. Sampled every 60 seconds. After sampling, data is not visible for up to 240 seconds.
upvoted 1 times

rinkeshgala1 7 months, 1 week ago
what about option A
we need to count application connection count and the count at instance level. no. of instance will keep on changing in app engine in the backend.
upvoted 2 times

akg001 7 months ago
Agree for the answer -A
upvoted 2 times

Question #20 *Topic 1*

You support an application deployed on Compute Engine. The application connects to a Cloud SQL instance to store and retrieve data. After an update to the application, users report errors showing database timeout messages. The number of concurrent active users remained stable. You need to find the most probable cause of the database timeout. What should you do?

A. Check the serial port logs of the Compute Engine instance.

B. Use Stackdriver Profiler to visualize the resources utilization throughout the application.

C. Determine whether there is an increased number of connections to the Cloud SQL instance.

D. Use Cloud Security Scanner to see whether your Cloud SQL is under a Distributed Denial of Service (DDoS) attack.

francisco_guerra Highly Voted 6 months, 3 weeks ago
Ans: B
I don't find anything about ddos attacks and Cloud security Scanner & databases; its most used with App engine and compute so.

I go with Stackdriver profiler
upvoted 13 times

Manh 2 months ago
Agree. Ans B
upvoted 1 times

ralf_cc Highly Voted 6 months, 3 weeks ago
B - getting to know the app perf
upvoted 7 times

TNT87 Most Recent 4 months, 1 week ago
A
https://cloud.google.com/compute/docs/troubleshooting/troubleshooting-using-serial-console
upvoted 2 times

Manh 2 months ago
serial-port for SSH mate. A wrong
upvoted 1 times

TNT87 1 month, 3 weeks ago
I do not copy answers from here https://quizlet.com/605380672/cloud-devops-flash-cards/ like you, i research, thats why i include links,im not fighting you but write your answer, dnt go arouund marking other people's answers and commenting negatively
upvoted 1 times

TNT87 1 month, 3 weeks ago
No write your answer dnt argue with me cause i have proof for what i wrote ....
upvoted 1 times

luchotluchot 5 months, 1 week ago
For me it is first C) then if number of connections is normal than B).
With the new version there is a bug performance that can for example not close connections to the base. So even if there is the same number of user of the application , in the base there can be lot of connections.
If you have app reports time out database the first things to do is to check the database if there are slow queries but there is not answer for that.
upvoted 3 times

danchoif2 4 months, 1 week ago
Totally agree!
upvoted 1 times

MikeFR 6 months ago
Ans:B - not C as The number of concurrent active users remained stable
upvoted 3 times

Charun 6 months, 2 weeks ago
C 100%
upvoted 4 times

TNT87 2 weeks, 3 days ago
It cant be C, you just copied a wrong answer, logicically what does that C answer do to solve the problem?
upvoted 1 times

guruguru 6 months, 2 weeks ago
B. Because timeout happened after app update, this is likely related to the app itself. Timeout could be due to no available resources in GCE.

upvoted 4 times

akg001 7 months ago

Why not B?

upvoted 3 times

devopsbatch 7 months, 1 week ago

A or D not sure

upvoted 2 times

DucLee3110 7 months, 1 week ago

Can not be D as "The number of concurrent active users remained stable" so should not be DDOS attack

upvoted 1 times

Question #21 | *Topic 1*

Your application images are built using Cloud Build and pushed to Google Container Registry (GCR). You want to be able to specify a particular version of your application for deployment based on the release version tagged in source control. What should you do when you push the image?

A. Reference the image digest in the source control tag.

B. Supply the source control tag as a parameter within the image name.

C. Use Cloud Build to include the release version tag in the application image.

D. Use GCR digest versioning to match the image to the tag in source control.

francisco_guerra Highly Voted 6 months, 2 weeks ago
Ans C
Cloud Build provides the following default substitutions:
$TAG_NAME: build.Source.RepoSource.Revision.TagName
upvoted 13 times

> **cetanx** 3 months, 4 weeks ago
> OK but doesn't it make more sense to use this $TAG to include the release version tag in the application image?
>
> I would go with B.
> upvoted 3 times
>
>> **danchoif2** 2 months, 1 week ago
>> Agree. Cloud Build provides a variable for the tag, when we push the image, we must supply the variable to tag the image.
>> upvoted 2 times
>
>> **cetanx** 3 months, 4 weeks ago
>> Sorry, I meant "to use this $TAG as a parameter within the image name?"
>> upvoted 2 times

meetplanet Most Recent 3 weeks, 4 days ago
I go for B
https://cloud.google.com/container-registry/docs/pushing-and-pulling
upvoted 2 times

alaahakim 1 month ago
Ans: C
upvoted 2 times

guruguru 6 months, 2 weeks ago
C. tag your images with the sourced code release version.
upvoted 3 times

JuanitoNN 6 months, 3 weeks ago
I think is B, is the normal process in this cases
upvoted 1 times

> **JuanitoNN** 6 months, 3 weeks ago
> https://cloud.google.com/container-registry/docs/pushing-and-pulling
> upvoted 1 times

devopsbatch 7 months, 1 week ago
C inside cloudbuil.yml file can include release version
upvoted 4 times

Question #22 Topic 1

You are on-call for an infrastructure service that has a large number of dependent systems. You receive an alert indicating that the service is failing to serve most of its requests and all of its dependent systems with hundreds of thousands of users are affected. As part of your Site Reliability Engineering (SRE) incident management protocol, you declare yourself Incident Commander (IC) and pull in two experienced people from your team as Operations Lead (OL) and
Communications Lead (CL). What should you do next?

A. Look for ways to mitigate user impact and deploy the mitigations to production.

B. Contact the affected service owners and update them on the status of the incident.

C. Establish a communication channel where incident responders and leads can communicate with each other.

D. Start a postmortem, add incident information, circulate the draft internally, and ask internal stakeholders for input.

Charun Highly Voted 6 months, 2 weeks ago
C is the answer
upvoted 11 times

francisco_guerra Highly Voted 6 months, 3 weeks ago
Ans: C
Prepare Beforehand
In addition to incident response training, it helps to prepare for an incident beforehand. Use the following tips and strategies to be better prepared.

Decide on a communication channel
Decide and agree on a communication channel (Slack, a phone bridge, IRC, HipChat, etc.) beforehand.

Keep your audience informed
Unless you acknowledge that an incident is happening and actively being addressed, people will automatically assume nothing is being done to resolve the issue. Similarly, if you forget to call off the response once the issue has been mitigated or resolved, people will assume the incident is ongoing. You can preempt this dynamic by keeping your audience informed throughout the incident with regular status updates. Having a prepared list of contacts (see the next tip) saves valuable time and ensures you don't miss anyone.

https://sre.google/workbook/incident-response/
upvoted 8 times

Wwhite44 Most Recent 3 weeks, 2 days ago
Selected Answer: C
Ans A is not, cause it means:"man solve the problem", it is not your task solve it, you are IC not technician, C for sure
upvoted 1 times

alaahakim 1 month ago
Ans: C
upvoted 1 times

ESP_SAP 1 month, 1 week ago
Correct Answer is A:

Best Practices for Incident Management
Prioritize.Stop the bleeding, restore service, and preserve the evidence for root-causing.

Prepare.Develop and document your incident management procedures in advance, in consultation with incident participants.

Trust.Give full autonomy within the assigned role to all incident participants.

Introspect.Pay attention to your emotional state while responding to an incident. If you start to feel panicky or overwhelmed, solicit more support.

Consider alternatives.Periodically consider your options and re-evaluate whether it still makes sense to continue what you're doing or whether you should be taking another tack in incident response.

Practice.Use the process routinely so it becomes second nature.

Change it around.Were you incident commander last time? Take on a different role this time. Encourage every team member to acquire familiarity with each role.
upvoted 3 times

Manh 2 months ago
C is answer

Appoint one person to be in charge of the response
- They delegate necessary tasks to others and coordinate
- Handoff carefully if necessary until incident over

- Maintain a log of the incident state and response

Communicate

- Let those affected know you're responding
- Make it clear who to contact if you want to help

Clean up any loose ends left during incident response

Prepare a postmortem report

- Determine root causes
- Update playbooks, consider adding DR drills

upvoted 1 times

tee_dee26 1 month, 4 weeks ago

Took the exam a couple of days ago (passed).
Answer I chose was A.

The answer can't be C because communication channel and templates are create prior to incident occurrences

upvoted 2 times

danchoif2 4 months, 1 week ago

Check the example at https://sre.google/sre-book/managing-incidents/
you will find the sentence: mitigated the problem, closed the incident, and started work on the postmortem.

So A is correct.

upvoted 2 times

raf2121 5 months ago

Point for discussion -
Core SRE principles states -
When you declare an incident
1. Assemble Team
2. Triage the Incident
3. Start Communicating

And SRE principle says "Communication channel" should be decided before an incident occurs and when incident is declared

Considering this , my guess is "A" as the answer rather than C
Will

upvoted 2 times

gcpengineer 4 months, 3 weeks ago

The deploy in production part of ans A is not something we want to straightaway

upvoted 1 times

danchoif2 4 months, 1 week ago

A doesn't mean that IC will deploy but he will ask the right person to deploy the mitigation.
So, for me A is the correct answer.

upvoted 2 times

ralf_cc 6 months, 3 weeks ago

C - First step

upvoted 2 times

JuanitoNN 6 months, 3 weeks ago

I think is ""A"" Because "" The IC may either hand off their role to someone else and assume the OL role, or assign the OL role to someone else. The OL works to respond to the incident by applying operational tools to mitigate or resolve the incident."". The most important thing is mitigate the impact.

upvoted 2 times

akg001 7 months, 1 week ago

option C is the correct answer as per the SRE principle.

upvoted 1 times

devopsbatch 7 months, 1 week ago

A first we need to mitigate issue before creating postmortem

upvoted 2 times

rinkeshgala1 7 months, 1 week ago

mitigating the issue is not the job of Incident commander but of Operation Lead.
Incident commander should setup common communication channel , so option C is correct i guess

upvoted 5 times

Question #23 Topic 1

You are developing a strategy for monitoring your Google Cloud Platform (GCP) projects in production using Stackdriver Workspaces. One of the requirements is to be able to quickly identify and react to production environment issues without false alerts from development and staging projects. You want to ensure that you adhere to the principle of least privilege when providing relevant team members with access to Stackdriver Workspaces. What should you do?

A. Grant relevant team members read access to all GCP production projects. Create Stackdriver workspaces inside each project.

B. Grant relevant team members the Project Viewer IAM role on all GCP production projects. Create Stackdriver workspaces inside each project.

C. Choose an existing GCP production project to host the monitoring workspace. Attach the production projects to this workspace. Grant relevant team members read access to the Stackdriver Workspace.

D. Create a new GCP monitoring project and create a Stackdriver Workspace inside it. Attach the production projects to this workspace. Grant relevant team members read access to the Stackdriver Workspace.

Charun Highly Voted 6 months, 2 weeks ago
D 100%
upvoted 16 times

ralf_cc Most Recent 6 months, 3 weeks ago
D it is
upvoted 4 times

devopsbatch 7 months, 1 week ago
C answer
upvoted 2 times

syslog 7 months ago
I think D because when I choose to add other project to mine, without create a new project, Google tells me: "A Project can host many Projects and appear in many Projects, but it can only be used as the scoping project once. We recommend that you create a new Project for the purpose of having multiple Projects in the same scope."
upvoted 7 times

Question #24 Topic 1

You currently store the virtual machine (VM) utilization logs in Stackdriver. You need to provide an easy-to-share interactive VM utilization dashboard that is updated in real time and contains information aggregated on a quarterly basis. You want to use Google Cloud Platform solutions. What should you do?

A. 1. Export VM utilization logs from Stackdriver to BigQuery. 2. Create a dashboard in Data Studio. 3. Share the dashboard with your stakeholders.

B. 1. Export VM utilization logs from Stackdriver to Cloud Pub/Sub. 2. From Cloud Pub/Sub, send the logs to a Security Information and Event Management (SIEM) system. 3. Build the dashboards in the SIEM system and share with your stakeholders.

C. 1. Export VM utilization logs from Stackdriver to BigQuery. 2. From BigQuery, export the logs to a CSV file. 3. Import the CSV file into Google Sheets. 4. Build a dashboard in Google Sheets and share it with your stakeholders.

D. 1. Export VM utilization logs from Stackdriver to a Cloud Storage bucket. 2. Enable the Cloud Storage API to pull the logs programmatically. 3. Build a custom data visualization application. 4. Display the pulled logs in a custom dashboard.

Charun Highly Voted 6 months, 2 weeks ago
A is correct
upvoted 11 times

kai324 Highly Voted 5 months ago
A for sure
upvoted 5 times

alaahakim Most Recent 1 month ago
Ans: A
upvoted 1 times

ralf_cc 6 months, 3 weeks ago
A - no doubt
upvoted 4 times

devopsbatch 7 months, 1 week ago
answer B. because SEIM helps realtime analysis of security and also export logs into pubsub is realtime transactions.
upvoted 2 times

akg001 7 months ago
In the question it is asking for VM utilisation not the security events. so answer is A
upvoted 1 times

DucLee3110 7 months, 1 week ago
A is correct. It mentioned clearly in the questions: "You want to use Google Cloud Platform solutions"
upvoted 6 times

Question #25 Topic 1

You need to run a business-critical workload on a fixed set of Compute Engine instances for several months. The workload is stable with the exact amount of resources allocated to it. You want to lower the costs for this workload without any performance implications. What should you do?

A. Purchase Committed Use Discounts.

B. Migrate the instances to a Managed Instance Group.

C. Convert the instances to preemptible virtual machines.

D. Create an Unmanaged Instance Group for the instances used to run the workload.

Charun Highly Voted 6 months, 2 weeks ago
A is correct
upvoted 18 times

Wwhite44 Most Recent 3 weeks, 2 days ago
Selected Answer: A
In study guide you can find “user discount” and “preemptable”. In this case performance are qequired, so C is not possible. A for sure
upvoted 1 times

not_thanos 3 weeks, 3 days ago
Selected Answer: A
Answer is A => several months can be up to or more than a year
C is wrong because
1. Business critical workload, you don't want that stopped randomly
2. Preemptible requires the workload to be resumable -> not stated in the question
upvoted 2 times

meetplanet 3 weeks, 4 days ago
please look at the question: "You need to run a business-critical workload". this is not a good idea to go for preemtible vms as it can effect performance and bussiness. I go for A.
upvoted 1 times

danchoif2 2 months, 1 week ago
B and D is not related to cost because of stable workload.
Now, really unsure between A and C.
A: several months vs. at least one year
C: a fixed set of Compute Engine instances vs. preemptable

I think I will choose C because using preemptable, we can still try to find a way to create a new preemptable VM (same or different zones) if existing one is terminated.
upvoted 1 times

tycho 2 months, 3 weeks ago
A) not correct committed discounts 1-3 years, we have several months
B) MIG - not correct - stable workloads
C) Preemptible vm's - not correct they last only 24 hours
D) not sure--Unmanaged instance groups-- do they offer cost savings?
upvoted 1 times

daas01 2 months, 4 weeks ago
C is correct, committed use discounts must be purchased for a minimum of one year.
upvoted 1 times

gcpengineer 5 months ago
C is the answer
upvoted 1 times

Dark_Lord 5 months, 3 weeks ago
B is correct

When you purchase a committed use contract, you purchase compute resource (vCPUs, memory, GPUs, and local SSDs) at a discounted price in return for committing to paying for those resources for 1 year or 3 years minimum, not months.

https://cloud.google.com/compute/docs/instances/signing-up-committed-use-discounts
upvoted 1 times

exploregcp 5 months, 2 weeks ago
Price reference https://cloud.google.com/compute/vm-instance-pricing#general-purpose_machine_type_family
Let's consider
1 CPU and 1 GB memory required to run the workload for 8 months (~240 days)

On Demand vCPU $0.021811 / vCPU hour
One year commitment vCPU $0.013741 / vCPU hour
On Demand cost for 240 days = 0.021811*24*240 = $125.63136
1 year commitment cost (365 days) = $120.37116

Same is applicable for memory
On demand memory $0.002923 / GB hour
1 year commitment $0.001842 / GB hour
On demand cost for 8 months = 0.002923*24*240 = $16.83648
1 year commitment cost = 0.001842*24*365 = $16.13592

Now if we consider several months (could be 2 months or more than year). Commited usage provides cost savings for Stable workloads running on fix number of instances.
In this case MIG cannot be helpful, as scale up / scale down possibility is very less.

upvoted 3 times

akg001 7 months ago

A is the correct answer.

upvoted 3 times

zzz 7 months, 1 week ago

A is correct.

upvoted 4 times

devopsbatch 7 months, 1 week ago

purchase commited discounts or unmanaged instance groups because stable load

upvoted 4 times

devopsbatch 7 months, 1 week ago

B managed instance groups and A also seems to be right

upvoted 3 times

DucLee3110 7 months, 1 week ago

A is correct, how you lower cost with MIG? MIG is only for HA and autoscale

upvoted 7 times

Question #26 Topic 1

You are part of an organization that follows SRE practices and principles. You are taking over the management of a new service from the Development Team, and you conduct a Production Readiness Review (PRR). After the PRR analysis phase, you determine that the service cannot currently meet its Service Level
Objectives (SLOs). You want to ensure that the service can meet its SLOs in production. What should you do next?

A. Adjust the SLO targets to be achievable by the service so you can bring it into production.

B. Notify the development team that they will have to provide production support for the service.

C. Identify recommended reliability improvements to the service to be completed before handover.

D. Bring the service into production with no SLOs and build them when you have collected operational data.

Charun Highly Voted 6 months, 2 weeks ago
C is correct
upvoted 11 times

devopsbatch Highly Voted 7 months, 1 week ago
C identify improvements before handover with no meet SLO
upvoted 6 times

akg001 7 months ago
I also agree for the answer - C
upvoted 2 times

alaahakim Most Recent 1 month ago
Ans : C
upvoted 1 times

giammydell 2 months, 1 week ago
Why B is Not correct? SLO is used to understand if give priority to Develop or to Operation
upvoted 1 times

danchoif2 2 months, 1 week ago
According to SRE book, next phase of conducting PRR in Simple PRR model is to select items in PRR to improve before hand over the service to SRE team.
https://sre.google/sre-book/evolving-sre-engagement-model/#improvements-and-refactoring-xqsrUdcyO

So C is correct.
upvoted 3 times

francisco_guerra 6 months, 3 weeks ago
I don't find anything about this but C its the only one that ensure that the service can meet its SLOs in production so I go with C
upvoted 5 times

Question #27 Topic 1

You are running an experiment to see whether your users like a new feature of a web application. Shortly after deploying the feature as a canary release, you receive a spike in the number of 500 errors sent to users, and your monitoring reports show increased latency. You want to quickly minimize the negative impact on users. What should you do first?

A. Roll back the experimental canary release.

B. Start monitoring latency, traffic, errors, and saturation.

C. Record data for the postmortem document of the incident.

D. Trace the origin of 500 errors and the root cause of increased latency.

devopsbatch Highly Voted 7 months, 1 week ago
A rollback experiment
upvoted 19 times

akg001 7 months ago
Agree with A
upvoted 3 times

holahola 6 months, 3 weeks ago
Agree with A, that is even why Spinnaker has "Manual judgment" stage that if Canary deployment seems dangerous, it can be immediately cancelled.
upvoted 3 times

cloudbee Most Recent 1 week, 1 day ago
Selected Answer: A
A should be the answer. error happens after canary release so we are not sure for actual cause. so first we should rollback canary release.
upvoted 1 times

alaahakim 1 month ago
Ans : A
upvoted 1 times

driftwood 5 months ago
Has to be A
upvoted 3 times

Question #28 *Topic 1*

You are responsible for creating and modifying the Terraform templates that define your Infrastructure. Because two new engineers will also be working on the same code, you need to define a process and adopt a tool that will prevent you from overwriting each other's code. You also want to ensure that you capture all updates in the latest version. What should you do?

A. ג€¢ Store your code in a Git-based version control system. ג€¢ Establish a process that allows developers to merge their own changes at the end of each day. ג€¢ Package and upload code to a versioned Cloud Storage basket as the latest master version.

B. ג€¢ Store your code in a Git-based version control system. ג€¢ Establish a process that includes code reviews by peers and unit testing to ensure integrity and functionality before integration of code. ג€¢ Establish a process where the fully integrated code in the repository becomes the latest master version.

C. ג€¢ Store your code as text files in Google Drive in a defined folder structure that organizes the files. ג€¢ At the end of each day, confirm that all changes have been captured in the files within the folder structure. ג€¢ Rename the folder structure with a predefined naming convention that increments the version.

D. ג€¢ Store your code as text files in Google Drive in a defined folder structure that organizes the files. ג€¢ At the end of each day, confirm that all changes have been captured in the files within the folder structure and create a new .zip archive with a predefined naming convention. ג€¢ Upload the .zip archive to a versioned Cloud Storage bucket and accept it as the latest version.

devopsbatch Highly Voted 7 months, 1 week ago
B peer review and source code management tool required
upvoted 18 times

akg001 7 months ago
Agree with you. Answer is B
upvoted 3 times

alaahakim Most Recent 1 month ago
Agree with B
upvoted 1 times

Luvero 2 months, 2 weeks ago
agree its B
upvoted 2 times

Charun 6 months, 2 weeks ago
B for sure
upvoted 4 times

ralf_cc 6 months, 3 weeks ago
B - for sure
upvoted 3 times

Question #29 Topic 1

You support a high-traffic web application with a microservice architecture. The home page of the application displays multiple widgets containing content such as the current weather, stock prices, and news headlines. The main serving thread makes a call to a dedicated microservice for each widget and then lays out the homepage for the user. The microservices occasionally fail; when that happens, the serving thread serves the homepage with some missing content. Users of the application are unhappy if this degraded mode occurs too frequently, but they would rather have some content served instead of no content at all. You want to set a Service Level Objective (SLO) to ensure that the user experience does not degrade too much. What Service Level Indicator (SLI) should you use to measure this?

A. A quality SLI: the ratio of non-degraded responses to total responses.

B. An availability SLI: the ratio of healthy microservices to the total number of microservices.

C. A freshness SLI: the proportion of widgets that have been updated within the last 10 minutes.

D. A latency SLI: the ratio of microservice calls that complete in under 100 ms to the total number of microservice calls.

francisco_guerra Highly Voted 6 months, 3 weeks ago
Ans: A
Quality as an SLI
Quality is a helpful SLI for complex services that are designed to fail gracefully by degrading when dependencies are slow or unavailable. The SLI for quality is defined as follows:

The proportion of valid requests served without degradation of service.

https://cloud.google.com/architecture/adopting-slos
upvoted 23 times

Charun Highly Voted 6 months, 2 weeks ago
Ans: B
upvoted 7 times

TNT87 2 weeks ago
Nope A
upvoted 1 times

guid1984 Most Recent 2 weeks, 5 days ago
Answer A - Quality as an SLI suits well for degrading dependencies
upvoted 1 times

not_thanos 3 weeks, 3 days ago
Selected Answer: A
https://cloud.google.com/architecture/adopting-slos?hl=en#sli-quality

Quality is a helpful SLI for complex services that are designed to fail gracefully by degrading when dependencies are slow or unavailable. The SLI for quality is defined as follows:

The proportion of valid requests served without degradation of service.
For example, a web page might load its main content from one datastore and load ancillary, optional assets from 100 other services and datastores. If one optional service is out of service or too slow, the page can still be rendered without the ancillary elements. By measuring the number of requests that are served a degraded response (that is, a response missing at least one backend service's response), you can report the ratio of requests that were bad. You might even track how many responses to the user were missing a response from a single backend, or were missing responses from multiple backends.
upvoted 2 times

alaahakim 1 month ago
Ans : B
upvoted 2 times

Manh 2 months ago
Ans is A
https://sre.google/workbook/implementing-slos/
Request-driven: Quality

If the service degrades gracefully when overloaded or when backends are unavailable, you need to measure the proportion of responses that were served in an undegraded state. For example, if the User Data store is unavailable, the game is still playable but uses generic imagery.
upvoted 1 times

TNT87 1 month, 3 weeks ago
Ans B
https://cloud.google.com/blog/products/gcp/available-or-not-that-is-the-question-cre-life-lessons, your answer is wrong
upvoted 3 times

giammydell 2 months, 1 week ago

I think D is the correct, B is not time-bound. B have to be writen as an availability probability in a time window

upvoted 1 times

MF2C 4 months ago

A Users may
not be consciously aware of the degradation in quality until it becomes
severe, but their subconscious perceptions may still have an impact on
your business if e.g. degrading quality means serving less relevant ads
to users, reducing click-through rates.

upvoted 2 times

TNT87 4 months, 1 week ago

B
https://cloud.google.com/blog/products/gcp/available-or-not-that-is-the-question-cre-life-lessons

upvoted 1 times

akg001 7 months ago

answer - B

upvoted 1 times

devopsbatch 7 months, 1 week ago

B webapplication availability is SLI

upvoted 2 times

Question #30 Topic 1

You support a multi-region web service running on Google Kubernetes Engine (GKE) behind a Global HTTP/S Cloud Load Balancer (CLB). For legacy reasons, user requests first go through a third-party Content Delivery Network (CDN), which then routes traffic to the CLB. You have already implemented an availability
Service Level Indicator (SLI) at the CLB level. However, you want to increase coverage in case of a potential load balancer misconfiguration, CDN failure, or other global networking catastrophe. Where should you measure this new SLI? (Choose two.)

A. Your application servers' logs.

B. Instrumentation coded directly in the client.

C. Metrics exported from the application servers.

D. GKE health checks for your application servers.

E. A synthetic client that periodically sends simulated user requests.

celia20200410 Highly Voted 5 months, 3 weeks ago
https://cloud.google.com/architecture/adopting-slos#choosing_a_measurement_method
B > Using client instrumentation.
E > Implementing synthetic testing.
upvoted 11 times

cloudbee 1 week, 1 day ago
How you code instrumentation at each client side?
upvoted 1 times

Charun Highly Voted 6 months, 2 weeks ago
BE is correct
upvoted 8 times

guid1984 Most Recent 2 weeks, 5 days ago
IMHO -> (E and C)A synthetic client that periodically sends simulated user requests could be used for checking CDN connection is up and running at frequent intervals and other one C for metrics exposed from Application servers. Since as per the question CLB SLI is already defined.
upvoted 1 times

alaahakim 1 month ago
Ans : BE
upvoted 1 times

muk5658 1 month, 2 weeks ago
Its B and E, when there is a networking catastrophe we cannot rely on Application as traffic may not even come there.
upvoted 1 times

francisco_guerra 6 months, 3 weeks ago
I have so many doubts with this one
The SLI for coverage is defined as follows:
The proportion of valid data processed successfully.

I think:
A logs are a good option and C Metrics exported
I don't get it why code directly in the client but if anyone have some information or a link please let me know.

the documentation says this
Finally, to generate your SLI for coverage, you count the number of records that processed successfully and compare that number against the total valid record count.
(we can do it with logs)
https://cloud.google.com/architecture/adopting-slos
upvoted 1 times

DucLee3110 7 months, 1 week ago
B,E should be the answers as you better check it at user level
upvoted 4 times

rinkeshgala1 7 months, 1 week ago
as there is an SLI already configured at LB level and they want to increase the coverage then I we need SLI which will detect CDN/LB failures as well.
running health checks at application/server level wont cover this.
so according to me option B & E are correct which are outside of the GCP infra, which give more coverage and resembles the use behavior
upvoted 4 times

akg001 7 months ago

Agree. Correct answer should be B and E.

upvoted 2 times

devopsbatch 7 months, 1 week ago

D gke health check is one answer and i dont know the second

upvoted 1 times

holahola 6 months, 3 weeks ago

I would go for D & E. Haven't seen anyone explaining why B is a good option as probably nobody knows why it is a good idea. GKE health check is important for load balancer to properly distribute traffic. E would also make sense as then success rates could be calculated.

upvoted 2 times

luchotluchot 5 months, 1 week ago

GKE health checks is not a good answer because in case of potential load balancer misconfiguration, CDN failure the GKE health checks will be be OK and so your SLI OK too whereas nobody can use the application !

upvoted 1 times

Question #31 Topic 1

Your team is designing a new application for deployment into Google Kubernetes Engine (GKE). You need to set up monitoring to collect and aggregate various application-level metrics in a centralized location. You want to use Google Cloud Platform services while minimizing the amount of work required to set up monitoring. What should you do?

A. Publish various metrics from the application directly to the Stackdriver Monitoring API, and then observe these custom metrics in Stackdriver.

B. Install the Cloud Pub/Sub client libraries, push various metrics from the application to various topics, and then observe the aggregated metrics in Stackdriver.

C. Install the OpenTelemetry client libraries in the application, configure Stackdriver as the export destination for the metrics, and then observe the application's metrics in Stackdriver.

D. Emit all metrics in the form of application-specific log messages, pass these messages from the containers to the Stackdriver logging collector, and then observe metrics in Stackdriver.

giammydell Highly Voted 2 months, 1 week ago
C is correct, for A the installing of stackdriver library in the application is missing, without the lbrary custom metric cannot be created by the application
upvoted 5 times

Luvero Highly Voted 2 months, 2 weeks ago
You want to use Google Cloud Platform services while minimizing the amount of work required to set up monitoring.

Hence A
upvoted 5 times

TNT87 Most Recent 4 months, 1 week ago
A
https://cloud.google.com/stackdriver/docs/solutions/gke
upvoted 4 times

driftwood 5 months ago
I would go with C
C says OpenTelemetry which has merged with OpenSensus. Look at:
https://cloud.google.com/monitoring/custom-metrics/open-census
There are many ways to capture custom metrics, including using the Cloud Monitoring API directly. Cloud Monitoring recommends that you use OpenCensus to instrument your code for collecting custom metrics.
Although Cloud Monitoring provides an API that supports defining and collecting custom metrics, it is a low-level, proprietary API. OpenCensus provides a much more idiomatic API, along with an exporter that sends your metric data to Cloud Monitoring through the Monitoring API for you.
upvoted 2 times

manojb7 4 months, 1 week ago
In Question, "You want to use Google Cloud Platform services while minimizing the amount of work required to set up monitoring" . So I think Answer A is correct
upvoted 2 times

kubosuke 5 months, 2 weeks ago
please tell me why D is wrong, I think we just emit all application logs to Cloud Monitoring via monitoring agent which is installed into GKE containers.
upvoted 1 times

kubosuke 5 months, 2 weeks ago
ok I got it it's wrong 'cause D said that 'emit all metrics as application logs' . it should be wrong haha
upvoted 1 times

celia20200410 5 months, 3 weeks ago
ANS: A

https://cloud.google.com/kubernetes-engine/docs/concepts/custom-and-external-metrics#custom_metrics
https://github.com/GoogleCloudPlatform/k8s-stackdriver/blob/master/custom-metrics-stackdriver-adapter/README.md
Your application can report a custom metric to Cloud Monitoring.
You can configure Kubernetes to respond to these metrics and
scale your workload automatically.
Before you can use custom metrics, you must enable Monitoring
in your
Google Cloud project and
install the Stackdriver adapter on
your cluster. After custom metrics are exported to Monitoring,
they can

trigger autoscaling events by Horizontal Pod Autoscaler to change the shape of
the workload.

upvoted 4 times

Charun 6 months, 2 weeks ago

Based on my experience A

upvoted 3 times

francisco_guerra 6 months, 3 weeks ago

Ans: A

Your application can report a custom metric to Cloud Monitoring. You can configure Kubernetes to respond to these metrics and scale your workload automatically. For example, you can scale your application based on metrics such as queries per second, writes per second, network performance, latency when communicating with a different application, or other metrics that make sense for your workload.

https://cloud.google.com/kubernetes-engine/docs/concepts/custom-and-external-metrics

upvoted 4 times

ralf_cc 6 months, 3 weeks ago

C - you would need OpenTelemetry SDK in the app to export the app specific metrics out

upvoted 2 times

holahola 6 months, 3 weeks ago

I agree with C as it also says minimize the effort and Google article shows example of doing it with "OpenCensus". https://cloud.google.com/monitoring/custom-metrics. Answer A is not easy at all from effort perspective and not sure if possible if application passes logs to a random log file which by default is not sent to stackdriver.

upvoted 3 times

suresh18 6 months, 3 weeks ago

https://cloud.google.com/monitoring/custom-metrics/creating-metrics#monitoring_create_metric-java

upvoted 1 times

suresh18 6 months, 3 weeks ago

A i guess. We can create custom metric without opentelemetry

upvoted 1 times

devopsbatch 7 months, 1 week ago

A i think

upvoted 1 times

akg001 7 months ago

Looks like Answer A to me as well.

upvoted 1 times

Question #32 *Topic 1*

You support a production service that runs on a single Compute Engine instance. You regularly need to spend time on recreating the service by deleting the crashing instance and creating a new instance based on the relevant image. You want to reduce the time spent performing manual operations while following Site
Reliability Engineering principles. What should you do?

A. File a bug with the development team so they can find the root cause of the crashing instance.

B. Create a Managed instance Group with a single instance and use health checks to determine the system status.

C. Add a Load Balancer in front of the Compute Engine instance and use health checks to determine the system status.

D. Create a Stackdriver Monitoring dashboard with SMS alerts to be able to start recreating the crashed instance promptly after it was crashed.

devopsbatch Highly Voted 7 months, 1 week ago
B managed instance groups can be handled when a vm crashed and immediately created new one
upvoted 13 times

akg001 7 months ago
Agree. correct Answer : B
upvoted 5 times

Charun Highly Voted 6 months, 2 weeks ago
B is correct
upvoted 6 times

garmstrong Most Recent 3 weeks, 5 days ago
Selected Answer: B
I'd say B, as a managed instance group can recreate crashed VMs
upvoted 1 times

meetplanet 3 weeks, 6 days ago
Selected Answer: B
It may take more time to resolve your issue if you open a bug. And this is not a bug. we only need to find best solution for this. I go for B.
upvoted 1 times

Vallal 4 weeks, 1 day ago
a is correct
upvoted 1 times

alaahakim 1 month ago
B is Correct
upvoted 1 times

lucabinc 1 month, 1 week ago
It is true health checks in managed instance group can automatically recreate VMs, but B answer says: "use health checks to determine the system status". "determine", not "automatically recreate". For me it's not a matter of automating toil, but improving reliability. I vote A
upvoted 1 times

Question #33

Topic 1

Your application artifacts are being built and deployed via a CI/CD pipeline. You want the CI/CD pipeline to securely access application secrets. You also want to more easily rotate secrets in case of a security breach. What should you do?

A. Prompt developers for secrets at build time. Instruct developers to not store secrets at rest.

B. Store secrets in a separate configuration file on Git. Provide select developers with access to the configuration file.

C. Store secrets in Cloud Storage encrypted with a key from Cloud KMS. Provide the CI/CD pipeline with access to Cloud KMS via IAM.

D. Encrypt the secrets and store them in the source code repository. Store a decryption key in a separate repository and grant your pipeline access to it.

driftwood Highly Voted 5 months ago
C is the "best" from the choices given
upvoted 8 times

Charun Highly Voted 6 months, 2 weeks ago
Answer C
upvoted 5 times

alaahakim Most Recent 1 month ago
Ans : C
upvoted 1 times

akg001 7 months ago
C is the best option.
upvoted 4 times

devopsbatch 7 months, 1 week ago
answer C storing secrets in cloud is better option
upvoted 4 times

Question #34 Topic 1

Your company follows Site Reliability Engineering practices. You are the person in charge of Communications for a large, ongoing incident affecting your customer-facing applications. There is still no estimated time for a resolution of the outage. You are receiving emails from internal stakeholders who want updates on the outage, as well as emails from customers who want to know what is happening. You want to efficiently provide updates to everyone affected by the outage.
What should you do?

A. Focus on responding to internal stakeholders at least every 30 minutes. Commit to ג€next updateג€ times.

B. Provide periodic updates to all stakeholders in a timely manner. Commit to a ג€next updateג€ time in all communications.

C. Delegate the responding to internal stakeholder emails to another member of the Incident Response Team. Focus on providing responses directly to customers.

D. Provide all internal stakeholder emails to the Incident Commander, and allow them to manage internal communications. Focus on providing responses directly to customers.

francisco_guerra Highly Voted 6 months, 3 weeks ago
Ans: B (the communication lead CAN'T delegate)

When disaster strikes, the person who declares the incident typically steps into the IC role and directs the high-level state of the incident. The IC concentrates on the 3Cs and does the following:

Commands and coordinates the incident response, delegating roles as needed. By default, the IC assumes all roles that have not been delegated yet.
Communicates effectively.
Stays in control of the incident response.
Works with other responders to resolve the incident.

https://sre.google/workbook/incident-response/
upvoted 16 times

Charun Highly Voted 6 months, 2 weeks ago
B is correct
upvoted 8 times

dalecolor Most Recent 2 days, 7 hours ago
B was my first answer, but turns out that CL can delegate, according to SRE workbook (https://sre.google/workbook/incident-response/):
"Both the CL and OL may lead a team of people to help manage their specific areas of incident response. These teams can expand or contract as needed. If the incident becomes small enough, the CL role can be subsumed back into the IC role."
In that case, taking into account that this is a major incidente, C seems to be the most accurate answer.
upvoted 1 times

garmstrong 3 weeks, 5 days ago
Selected Answer: B
B - providing updates to all stakeholders is your job as being in charge of communications. Incident Commander delegates.
upvoted 2 times

meetplanet 3 weeks, 6 days ago
Selected Answer: B
B is correct. everyone is saying B is correct. not sure why final answer is C!!
upvoted 2 times

danchoif2 2 months, 1 week ago
B is correct
C is wrong. If CL want to delegate, s/he must talk with IC that we need another internal CL. IC will delegate if needed.
upvoted 2 times

ralf_cc 6 months, 3 weeks ago
B is most correct one, with quite a lot of details missing, but the direction is right
upvoted 2 times

rinkeshgala1 7 months, 1 week ago
we can have external communication lead. as there is a large outage we can choose to have one more role of external communication lead. hence option C
upvoted 1 times

akg001 7 months ago
for answer C. one doubt does Communication Leads (CL) can delegate the task or this is Incident commander (IC) can do...
B looks more closer.

upvoted 2 times

akg001 7 months ago

Looks correct to me as well.

upvoted 1 times

devopsbatch 7 months, 1 week ago

could be B

upvoted 1 times

Question #35 *Topic 1*

Your team uses Cloud Build for all CI/CD pipelines. You want to use the kubectl builder for Cloud Build to deploy new images to Google Kubernetes Engine
(GKE). You need to authenticate to GKE while minimizing development effort. What should you do?

A. Assign the Container Developer role to the Cloud Build service account.

B. Specify the Container Developer role for Cloud Build in the cloudbuild.yaml file.

C. Create a new service account with the Container Developer role and use it to run Cloud Build.

D. Create a separate step in Cloud Build to retrieve service account credentials and pass these to kubectl.

zzz Highly Voted 7 months, 1 week ago
I think A
upvoted 16 times

TNT87 Highly Voted 4 months, 1 week ago
A
https://cloud.google.com/build/docs/securing-builds/configure-user-specified-service-accounts
upvoted 5 times

cloudbee Most Recent 1 week, 1 day ago
Selected Answer: A
A should be the correct one. because assigning permission to cloud build service account will give permission to deploy while minimizing additional overhead.
upvoted 1 times

Biden 1 month ago
Agree with A.
Reference to container.developer role: https://cloud.google.com/kubernetes-engine/docs/how-to/iam
upvoted 1 times

Charun 6 months, 2 weeks ago
A is correct
upvoted 3 times

francisco_guerra 6 months, 3 weeks ago
Ans: A
minimizing development effort
So create another account with all the needed roles its not an option
upvoted 2 times

ralf_cc 6 months, 3 weeks ago
A - https://cloud.google.com/build/docs/deploying-builds/deploy-gke
upvoted 1 times

akg001 7 months ago
User managed service account in the option C can be used only for manual builds.

As CI/CD is being used so assigning the permission to default build service account could be good idea. so it seems best answer is A

https://cloud.google.com/build/docs/securing-builds/configure-user-specified-service-accounts
upvoted 2 times

devopsbatch 7 months, 1 week ago
i think D
upvoted 1 times

Question #36 *Topic 1*

You support an application that stores product information in cached memory. For every cache miss, an entry is logged in Stackdriver Logging. You want to visualize how often a cache miss happens over time. What should you do?

A. Link Stackdriver Logging as a source in Google Data Studio. Filter the logs on the cache misses.

B. Configure Stackdriver Profiler to identify and visualize when the cache misses occur based on the logs.

C. Create a logs-based metric in Stackdriver Logging and a dashboard for that metric in Stackdriver Monitoring.

D. Configure BigQuery as a sink for Stackdriver Logging. Create a scheduled query to filter the cache miss logs and write them to a separate table.

Charun Highly Voted 6 months, 2 weeks ago
C for sure
upvoted 10 times

syslog Highly Voted 7 months ago
I think C: https://cloud.google.com/logging/docs/logs-based-metrics#counter-metric
upvoted 6 times

TNT87 Most Recent 4 months, 1 week ago
C
https://cloud.google.com/logging/docs/logs-based-metrics#counter-metric
upvoted 3 times

devopsbatch 7 months, 1 week ago
D export to biguery as sink and analyse logs
upvoted 1 times

> **tycho** 2 months, 3 weeks ago
> and how would you visualize the data in bq?
> upvoted 2 times

Question #37 *Topic 1*

You need to deploy a new service to production. The service needs to automatically scale using a Managed Instance Group (MIG) and should be deployed over multiple regions. The service needs a large number of resources for each instance and you need to plan for capacity. What should you do?

A. Use the n1-highcpu-96 machine type in the configuration of the MIG.

B. Monitor results of Stackdriver Trace to determine the required amount of resources.

C. Validate that the resource requirements are within the available quota limits of each region.

D. Deploy the service in one region and use a global load balancer to route traffic to this region.

Charun Highly Voted 6 months, 2 weeks ago
C 100%
upvoted 7 times

meetplanet Most Recent 3 weeks, 6 days ago
Selected Answer: C
Correct answer is C. this service is deployed into MIG and we only have to take care of quota
upvoted 1 times

Shasha1 4 weeks ago
Answer is D
Networking and load balancing quotas are not regional quotes, those are global quotas. Any region can use a global quota. For example, in-use and static external IP addresses assigned to load balancers and HTTP(S) proxies consume global quotas.
reference https://cloud.google.com/compute/quotas
upvoted 1 times

TNT87 4 months, 1 week ago
C
https://cloud.google.com/compute/quotas
upvoted 4 times

kubosuke 5 months, 2 weeks ago
absolutely C 'cause this service is deployed into MIG and you only have to take care of quota.
upvoted 3 times

ralf_cc 6 months, 3 weeks ago
C - it is asking for quota
upvoted 4 times

DucLee3110 7 months, 1 week ago
I think C is the answer.
https://cloud.google.com/compute/quotas#understanding_quotas
https://cloud.google.com/compute/quotas
upvoted 4 times

> **akg001** 7 months, 1 week ago
> Agree for the answer : C
> upvoted 2 times

devopsbatch 7 months, 1 week ago
A can be the answer
upvoted 1 times

> **akg001** 7 months, 1 week ago
> you have to check the required resources available on those particular regions or not. As you know not all type of VM or a resource available in all regions. There is not surety that n1-highcpu-96 machine type available in all regions.
> upvoted 1 times
>
> > **syslog** 7 months ago
> > And nobody is saying you need 96 CPU.
> > upvoted 4 times

Question #38 *Topic 1*

You are running an application on Compute Engine and collecting logs through Stackdriver. You discover that some personally identifiable information (PII) is leaking into certain log entry fields. All PII entries begin with the text userinfo. You want to capture these log entries in a secure location for later review and prevent them from leaking to Stackdriver Logging. What should you do?

A. Create a basic log filter matching userinfo, and then configure a log export in the Stackdriver console with Cloud Storage as a sink.

B. Use a Fluentd filter plugin with the Stackdriver Agent to remove log entries containing userinfo, and then copy the entries to a Cloud Storage bucket.

C. Create an advanced log filter matching userinfo, configure a log export in the Stackdriver console with Cloud Storage as a sink, and then configure a log exclusion with userinfo as a filter.

D. Use a Fluentd filter plugin with the Stackdriver Agent to remove log entries containing userinfo, create an advanced log filter matching userinfo, and then configure a log export in the Stackdriver console with Cloud Storage as a sink.

DucLee3110 Highly Voted 7 months, 1 week ago
looks like it is B. https://medium.com/google-cloud/fluentd-filter-plugin-for-google-cloud-data-loss-prevention-api-42bbb1308e76
upvoted 13 times

Manh 2 months ago
Agree with B
upvoted 1 times

holahola 6 months, 3 weeks ago
B to me as well. Because fluentd can filter the logs quite nicely before passing information to Stackdriver. It can cober sensitive information such as credit card details, social security numbers, etc. Once the filtering is done, then the log can be passed to Cloud Storage, but the unfiltered information should not even reach stackdriver, so most of the answers are wrong.
upvoted 4 times

akg001 7 months, 1 week ago
to me , looks B is the correct answer .
upvoted 2 times

syslog 7 months ago
Why not D?
upvoted 1 times

francisco_guerra 6 months, 2 weeks ago
prevent them from leaking to Stackdriver Logging.
If you need to create a log export & log filter so the information is leaking to logging.
upvoted 3 times

francisco_guerra Highly Voted 6 months, 3 weeks ago
Im not pretty sure but
Ans B
Prevent them form leaking to Stackdriver logging
A: Incorrect, Leaking to Stackdriver
B: Correct, not leaking to Stackdriver & fluentD
C: Incorrect, Leaking
D: If we removed why we need to create a filter matching there will not be logs with userinfo?
upvoted 5 times

TNT87 Most Recent 2 weeks ago
Selected Answer: B
Ans B
https://medium.com/google-cloud/fluentd-filter-plugin-for-google-cloud-data-loss-prevention-api-42bbb1308e76
upvoted 1 times

garmstrong 3 weeks, 5 days ago
Selected Answer: B
Agree with B
upvoted 1 times

Shasha1 4 weeks ago
A
question is about capture logs entries in a secure location for later review, not removing the log sensitive data before store then in a secure location. so answer is A
upvoted 1 times

TNT87 4 months, 1 week ago

B
https://medium.com/google-cloud/fluentd-filter-plugin-for-google-cloud-data-loss-prevention-api-42bbb1308e76

upvoted 3 times

j3e 6 months ago

B. filter_record_transformer to be exact.

upvoted 3 times

Charun 6 months, 2 weeks ago

B answer

upvoted 4 times

ralf_cc 6 months, 3 weeks ago

C - https://cloud.google.com/logging/docs/exclusions
fluentd filter plugin is on the client-side, the question is asking the server (gcp) side

upvoted 1 times

kubosuke 5 months, 2 weeks ago

I think C is wrong 'cause we need to leak logs to Cloud Logging as below:
> prevent them from leaking to Stackdriver Logging.

and C is just filter Logs on the Cloud Logging, so the logs has leaked into Cloud Logging.
so we need to filter Logs not on the Cloud Logging, but fluentd.
for these backgrounds, the answer gonna be B.

upvoted 2 times

devopsbatch 7 months, 1 week ago

C could be

upvoted 1 times

Question #39 Topic 1

You have a CI/CD pipeline that uses Cloud Build to build new Docker images and push them to Docker Hub. You use Git for code versioning. After making a change in the Cloud Build YAML configuration, you notice that no new artifacts are being built by the pipeline. You need to resolve the issue following Site
Reliability Engineering practices. What should you do?

A. Disable the CI pipeline and revert to manually building and pushing the artifacts.

B. Change the CI pipeline to push the artifacts is Container Registry instead of Docker Hub.

C. Upload the configuration YAML file to Cloud Storage and use Error Reporting to identify and fix the issue.

D. Run a Git compare between the previous and current Cloud Build Configuration files to find and fix the bug.

Charun Highly Voted 6 months, 2 weeks ago
D is correct
upvoted 13 times

ralf_cc Highly Voted 6 months, 3 weeks ago
D - find out what's changed in the build spec
upvoted 6 times

Shasha1 Most Recent 4 weeks ago
B is correct
artifact can not push to Docker hub only docker images possible. therefore, need to push the artifacts to google cloud container registry not to the public docker hub.
https://cloud.google.com/build/docs/interacting-with-dockerhub-images
upvoted 1 times

zzz 7 months, 1 week ago
I think D
upvoted 5 times

devopsbatch 7 months, 1 week ago
B push images into container registry instead docker hub
upvoted 1 times

akg001 7 months ago
"After making a change in the Cloud Build YAML configuration, you notice that no new artifacts are being built by the pipeline"- means something wrong on the recent change not with the image registry.

correct answer should be - D
upvoted 6 times

Question #40 | Topic 1

Your company follows Site Reliability Engineering principles. You are writing a postmortem for an incident, triggered by a software change, that severely affected users. You want to prevent severe incidents from happening in the future. What should you do?

A. Identify engineers responsible for the incident and escalate to their senior management.

B. Ensure that test cases that catch errors of this type are run successfully before new software releases.

C. Follow up with the employees who reviewed the changes and prescribe practices they should follow in the future.

D. Design a policy that will require on-call teams to immediately call engineers and management to discuss a plan of action if an incident occurs.

Charun Highly Voted 6 months, 2 weeks ago
B is correct
upvoted 14 times

looseboy 5 months ago
Agree with B. I find this answer in "Site Reliability Engineering: How Google Runs Production Systems".
upvoted 2 times

devopsbatch Highly Voted 7 months, 1 week ago
B make automation better
upvoted 5 times

akg001 7 months, 1 week ago
Agree with you. IMO - B is the correct answer.
upvoted 4 times

meetplanet Most Recent 3 weeks, 4 days ago
I go for D based on the on-call doc
upvoted 1 times

Vallal 3 weeks, 6 days ago
c is the correct answer
upvoted 3 times

muk5658 1 month, 2 weeks ago
I would go with B as they are saying incident is triggered by a software change, if this has been tested thoroughly it would have been avoided.
upvoted 1 times

MF2C 4 months ago
B is better over D because D is incident management, B is RCA.
upvoted 2 times

kubosuke 5 months, 2 weeks ago
I think D is correct.

> you want to prevent severe incidents from happening in the future.
we need to chose the answer that 'prevent severe incidents'.

B: create test cases can reduce the possibility of incidents, but it doesn't ease the 'severe incidents'.
to minimize the effect of incidents, we need to make a consensus to manage incidents.
for these backgrounds, the answer is D.
upvoted 4 times

francisco_guerra 6 months, 2 weeks ago
D sounds very good but
to prevent severe incidents form happening in the future
test cases are a very good option
upvoted 1 times

francisco_guerra 6 months, 2 weeks ago
I correct myself
I find out this
https://sre.google/sre-book/being-on-call/

Being on-call is a critical duty that many operations and engineering teams must undertake in order to keep their services reliable and available.

when an incident occurs, it’s important to evaluate what went wrong, recognize what went well, and take action to prevent the same errors from recurring in the future. SRE teams must write postmortems after significant incidents and detail a full timeline of the events that occurred.

I don't find anything about test cases so I go with D

upvoted 5 times

mkumar118 4 months, 2 weeks ago

D is incorrect because the plan of action needs to be ready BEFORE the incident occurs. If you create a PoA AFTER the incident happens then you are losing critical time and reducing your error budget.

upvoted 2 times

Question #41 Topic 1

You support a high-traffic web application that runs on Google Cloud Platform (GCP). You need to measure application reliability from a user perspective without making any engineering changes to it. What should you do? (Choose two.)

A. Review current application metrics and add new ones as needed.

B. Modify the code to capture additional information for user interaction.

C. Analyze the web proxy logs only and capture response time of each request.

D. Create new synthetic clients to simulate a user journey using the application.

E. Use current and historic Request Logs to trace customer interaction with the application.

ralf_cc Highly Voted 6 months, 3 weeks ago
DE - synthetic transactions
upvoted 14 times

Biden 3 weeks, 6 days ago
A&D. Why E isnt correct - Synthetic transaction already provides the capability mentioned in E - "Use current and historic Request Logs to trace customer interaction with the application". Instead, option A - to review and add additional metrics makes sense !!
upvoted 1 times

Charun Highly Voted 6 months, 2 weeks ago
CE ans
upvoted 11 times

cetanx 3 months, 3 weeks ago
Web proxy is not a reverse proxy, it is a forward proxy - a type of server that runs at the client side. If you have clients from all over the world, how will you collect their proxy logs?

So it cannot be C - D&E should be the answer which don't require any engineering changes "in the" application.
upvoted 7 times

cloudbee Most Recent 1 week, 1 day ago
Selected Answer: DE
This two option doesn't require engineering changes into the application. Web Proxy logs is a forward proxy thing so it present in client side. others need changes
upvoted 1 times

guid1984 2 weeks, 5 days ago
C& E.
C-> a web proxy relays URL requests from clients to a server. Analyzing web proxy logs can give unobtrusive insights into the browsing behavior of users
upvoted 1 times

rspstudent 3 weeks, 2 days ago
Selected Answer: DE
upvoted 1 times

Freemiums 1 month ago
Selected Answer: CE
C and E should be the correct answer, since the question state that "without making ANY engineering changes"
upvoted 3 times

not_thanos 3 weeks, 3 days ago
with making any engineering changes to IT (i.e the application itself)
upvoted 1 times

Biden 1 month, 3 weeks ago
A&D should be the correct answer:
D - Easy/default choice since this doesnt need any changes on the app
A - Since the ask is to "measure reliability" - review and add the appropriate SLIs. Option E -tracing is needed only for collecting/troubleshooting latency issues - hence not the correct choice
upvoted 2 times

raf2121 5 months ago
To me , it looks C & E
B & D, need engineering changes and investment, hence I ruled these two out
This leaves us with A, C and E - The question is asking for "Need to measure Application Reliability from User perspective without Engineering Changes" - This rules out A, as talks about adding new metric but not stating which one

Considering high-traffic web application as "Request Driven Services" - Two of the suggested SLI's are Availability and Latency - C & E to me covers Latency

https://cloud.google.com/architecture/adopting-slos?hl=en

upvoted 3 times

gcpengineer 5 months ago

A & D is the answer

upvoted 2 times

kubosuke 5 months, 2 weeks ago

maybe C,D,E, and it looks like create synthetic client looks like "engineering change", so I choose C and E .

upvoted 1 times

luchotluchot 4 months ago

Create synthetic client is not an engineering change for the application : the application is not modified. So the answer is still valid.

upvoted 2 times

kubosuke 5 months, 2 weeks ago

umm but
> C. Analyze the web proxy logs 'only' and
the phrase 'only' bothers me...
we can know the reliability by getting the status of web applications by web proxy logs(I mean HTTP status is good/bad), but we don't need to view these logs 'only'...

upvoted 2 times

gcpengineer 5 months ago

C cant be the ans , as it talks about response time. we need answer for reliability

upvoted 2 times

akg001 7 months, 1 week ago

for me it looks like C,E the correct answer. E for sure.

upvoted 5 times

holahola 6 months, 3 weeks ago

Same here, because no engineering effort should be required. All others definitely need engineering effort.

upvoted 2 times

rinkeshgala1 7 months, 1 week ago

may be A&E as these options may not need any additional engineering efforts

upvoted 2 times

Question #42 Topic 1

You manage an application that is writing logs to Stackdriver Logging. You need to give some team members the ability to export logs. What should you do?

A. Grant the team members the IAM role of logging.configWriter on Cloud IAM.

B. Configure Access Context Manager to allow only these members to export logs.

C. Create and grant a custom IAM role with the permissions logging.sinks.list and logging.sink.get.

D. Create an Organizational Policy in Cloud IAM to allow only these members to create log exports.

rinkeshgala1 Highly Voted 7 months, 1 week ago
option A
upvoted 12 times

akg001 7 months, 1 week ago
agree for the A.
upvoted 2 times

irocketsoldier 1 month, 3 weeks ago
I understand that option A gives the ability to export logs, but isn't C the best option following the least privilege principle since the question only says that the team members needs to export logs and not to write them?
upvoted 1 times

cloudbee Most Recent 1 week, 1 day ago
https://cloud.google.com/logging/docs/export/configure_export_v2#before-you-begin A is the answer
upvoted 1 times

not_thanos 3 weeks, 3 days ago
Write answer is A as stated in the documentation here

https://cloud.google.com/logging/docs/export/configure_export_v2#before-you-begin

"Note that this guide describes creating and managing sinks at the Cloud project level, but you can create sinks (non-aggregated) for billing accounts, folders, and organizations. As you get started, ensure the following:

You have a Google Cloud project with logs that you can see in the Logs Explorer.

You have one of the following IAM roles for the source Cloud project from which you're routing logs.

Owner (roles/owner)
Logging Admin (roles/logging.admin)
Logs Configuration Writer (roles/logging.configWriter)
The permissions contained in these roles allow you to create, delete, or modify sinks. For information on setting IAM roles, see the Logging Access control guide."
upvoted 1 times

Manh 2 months ago
It's should be C. least privilege

The question is ask about export log and does not mention about read and write log
Option A give too many permission
Logs Configuration Writer
(roles/logging.configWriter)
Provides permissions to read and write the configurations of logs-based metrics and sinks for exporting logs.

logging.buckets.create
logging.buckets.delete
logging.buckets.get
logging.buckets.list
logging.buckets.undelete
logging.buckets.update
logging.cmekSettings.*
logging.exclusions.*
logging.locations.*
logging.logMetrics.*
logging.logServiceIndexes.*
logging.logServices.*
logging.logs.list
logging.notificationRules.*
logging.operations.*
logging.sinks.*
logging.views.create

logging.views.delete
logging.views.get
logging.views.list
logging.views.update
resourcemanager.projects.get
resourcemanager.projects.list
upvoted 2 times

Manh 2 months ago
After review again, Ans A had enough permission to export log https://cloud.google.com/logging/docs/routing/overview
upvoted 2 times

Goram113 1 month ago
logging.sinks.create is needed to export logs - this is why C is wrong
upvoted 2 times

giammydell 2 months, 1 week ago
but C could follow the least privilege priciple
upvoted 3 times

Trony 2 months, 1 week ago
I agree. logging.configWriter (answer A) gives too much power to the team members. We only need to give them the rights to export, not change the whole logging configuration.
C is ok.
upvoted 1 times

sticky 3 months, 1 week ago
A is correct

Logs Configuration Writer
(roles/logging.configWriter)
- Provides permissions to read and write the configurations of logs-based metrics and sinks for exporting logs.
https://cloud.google.com/logging/docs/access-control
upvoted 3 times

Question #43 Topic 1

Your application services run in Google Kubernetes Engine (GKE). You want to make sure that only images from your centrally-managed Google Container
Registry (GCR) image registry in the altostrat-images project can be deployed to the cluster while minimizing development time. What should you do?

A. Create a custom builder for Cloud Build that will only push images to gcr.io/altostrat-images.

B. Use a Binary Authorization policy that includes the whitelist name pattern gcr.io/altostrat-images/.

C. Add logic to the deployment pipeline to check that all manifests contain only images from gcr.io/altostrat-images.

D. Add a tag to each image in gcr.io/altostrat-images and check that this tag is present when the image is deployed.

rinkeshgala1 Highly Voted 7 months, 1 week ago
option B
upvoted 14 times

akg001 7 months ago
agree for answer-B
upvoted 3 times

Charun Highly Voted 6 months, 2 weeks ago
B is correct
upvoted 8 times

Shasha1 Most Recent 1 month ago
D
https://cloud.google.com/container-registry/docs/using-with-google-cloud-platform
upvoted 1 times

tycho 2 months, 3 weeks ago
B)
https://cloud.google.com/binary-authorization/docs/cloud-build
upvoted 3 times

Question #44 Topic 1

Your team has recently deployed an NGINX-based application into Google Kubernetes Engine (GKE) and has exposed it to the public via an HTTP Google Cloud
Load Balancer (GCLB) ingress. You want to scale the deployment of the application's frontend using an appropriate Service Level Indicator (SLI).
What should you do?

A. Configure the horizontal pod autoscaler to use the average response time from the Liveness and Readiness probes.

B. Configure the vertical pod autoscaler in GKE and enable the cluster autoscaler to scale the cluster as pods expand.

C. Install the Stackdriver custom metrics adapter and configure a horizontal pod autoscaler to use the number of requests provided by the GCLB.

D. Expose the NGINX stats endpoint and configure the horizontal pod autoscaler to use the request metrics exposed by the NGINX deployment.

Charun Highly Voted 6 months, 2 weeks ago
Option C
upvoted 9 times

kubosuke Highly Voted 5 months, 2 weeks ago
C is correct

A. Configure the horizontal pod autoscaler to use the average response time from the Liveness and Readiness Probes.
--> using health check as a trigger of scaling is weird. if the response time of the health check is delayed, it may be caused by resources issues such as CPU, memories, and so on. so you should use such values as SLIs.

B. Configure the vertical pod autoscaler in GKE and enable the cluster autoscaler to scale the cluster as pods expand.
--> it doesn't referred to pod autoscaling.

D. Expose the NGINX stats endpoint and configure the horizontal pod autoscaler to use the request metrics exposed by the NGINX deployment.
--> if you use request metrics as SLIs, you should use custom metrics as SLIs. it is a little bit redundant.
upvoted 8 times

cloudbee Most Recent 1 week ago
c looks more feasible to me. but also B is in small favour. Horizontal pod autoscaler will scale based on the custom metrics such as requests per second(i.e. no. of requests). but vertical autoscaling is also useful feature for the frontend application. as it requires more resource needs if the traffic is high. Since vertical autoscaling will first delete the pod and adjust the cpu and memory to recreate the pod, It can cause downtime for that duration and not recommended. Hence, More inclined towards answer C. Still, reply my answer with your explanation please

https://cloud.google.com/kubernetes-engine/docs/concepts/horizontalpodautoscaler#overview
upvoted 1 times

Shasha1 4 weeks ago
B is correct
front-end web applications Scale based on the number of incoming request. so need vertical scaling
Back-end Batch Processing (Scale Horizontally)
reference https://docs.rightscale.com/faq/What_is_auto-scaling.html
upvoted 2 times

TNT87 4 months, 1 week ago
C
https://cloud.google.com/kubernetes-engine/docs/tutorials/autoscaling-metrics
upvoted 2 times

IamSuren 5 months, 2 weeks ago
According to Google
https://cloud.google.com/kubernetes-engine/docs/tutorials/autoscaling-metrics#cpu_1
Horizontal Pod Autoscalers can scale based on CPU utilization natively, so the Custom Metrics Adapter is not needed, therefor C doesn't fit .
upvoted 2 times

luchotluchot 4 months ago
It is why the C answer say number of requests not CPU utilization.
upvoted 3 times

ralf_cc 6 months, 3 weeks ago
C - https://cloud.google.com/kubernetes-engine/docs/tutorials/autoscaling-metrics
You want to scale horizontally
upvoted 4 times

rinkeshgala1 7 months, 1 week ago
Option B

upvoted 1 times

Question #45 *Topic 1*

Your company follows Site Reliability Engineering practices. You are the Incident Commander for a new, customer-impacting incident. You need to immediately assign two incident management roles to assist you in an effective incident response. What roles should you assign? (Choose two.)

A. Operations Lead

B. Engineering Lead

C. Communications Lead

D. Customer Impact Assessor

E. External Customer Communications Lead

syslog Highly Voted 7 months ago
AC

https://sre.google/workbook/incident-response/
"The main roles in incident response are the Incident Commander (IC), Communications Lead (CL), and Operations or Ops Lead (OL)."
upvoted 20 times

akg001 7 months ago
could be. A and C.

why not E? this is customer impacting incident so should be an external customer comm lead as well.
upvoted 2 times

Charun Highly Voted 6 months, 2 weeks ago
AC for sure
upvoted 9 times

cloudbee Most Recent 1 week ago
Selected Answer: AC
It's mentioned in sre book by Google.
upvoted 1 times

Biden 1 month, 3 weeks ago
Who gave AE as the correct answer ? why not this tool display/reveal the correct answer from the "Highly Voted" from the discussion thread for each Q?
upvoted 2 times

Luvero 2 months, 2 weeks ago
A, C - other roles are appropriate ..
upvoted 3 times

Question #46 *Topic 1*

You support an application running on GCP and want to configure SMS notifications to your team for the most critical alerts in Stackdriver Monitoring. You have already identified the alerting policies you want to configure this for. What should you do?

A. Download and configure a third-party integration between Stackdriver Monitoring and an SMS gateway. Ensure that your team members add their SMS/phone numbers to the external tool.

B. Select the Webhook notifications option for each alerting policy, and configure it to use a third-party integration tool. Ensure that your team members add their SMS/phone numbers to the external tool.

C. Ensure that your team members set their SMS/phone numbers in their Stackdriver Profile. Select the SMS notification option for each alerting policy and then select the appropriate SMS/phone numbers from the list.

D. Configure a Slack notification for each alerting policy. Set up a Slack-to-SMS integration to send SMS messages when Slack messages are received. Ensure that your team members add their SMS/phone numbers to the external integration.

zzz Highly Voted 7 months, 1 week ago
I think C
upvoted 8 times

akg001 7 months ago
Agree. C looks more close from other given answer.
upvoted 4 times

kubosuke Highly Voted 5 months, 2 weeks ago
C

https://cloud.google.com/monitoring/support/notification-options#creating_channels
To configure SMS notifications, do the following:

In the SMS section, click Add new and follow the instructions.
Click Save.
When you set up your alerting policy, select the SMS notification type and choose a verified phone number from the list.
upvoted 7 times

cloudbee Most Recent 1 week ago
Selected Answer: C
Although stackdriver profile is not an named option in gcp. It looks like that to add phone no in stackdriver. so pretty straigtforward right answer is C
upvoted 1 times

Shasha1 4 weeks ago
i think answer is D
There is no Stackdriver Profile exists to add their phone number. only possible to add the phone number in the notification channel under sms category
upvoted 2 times

utwo 1 month, 1 week ago
Selected Answer: C
is option C
upvoted 1 times

TNT87 4 months, 1 week ago
C
https://cloud.google.com/monitoring/support/notification-options
upvoted 5 times

Charun 6 months, 2 weeks ago
C option
upvoted 5 times

Question #47 | Topic 1

You are managing an application that exposes an HTTP endpoint without using a load balancer. The latency of the HTTP responses is important for the user experience. You want to understand what HTTP latencies all of your users are experiencing. You use Stackdriver Monitoring. What should you do?

A. ג€¢ In your application, create a metric with a metricKind set to DELTA and a valueType set to DOUBLE. ג€¢ In Stackdriverג€™s Metrics Explorer, use a Stacked Bar graph to visualize the metric.

B. ג€¢ In your application, create a metric with a metricKind set to CUMULATIVE and a valueType set to DOUBLE. ג€¢ In Stackdriverג€™s Metrics Explorer, use a Line graph to visualize the metric.

C. ג€¢ In your application, create a metric with a metricKind set to GAUGE and a valueType set to DISTRIBUTION. ג€¢ In Stackdriverג€™s Metrics Explorer, use a Heatmap graph to visualize the metric.

D. ג€¢ In your application, create a metric with a metricKind set to METRIC_KIND_UNSPECIFIED and a valueType set to INT64. ג€¢ In Stackdriverג€™s Metrics Explorer, use a Stacked Area graph to visualize the metric.

raf2121 Highly Voted 5 months ago

Answer C
Reference : https://cloud.google.com/monitoring/api/v3/kinds-and-types?hl=en
GAUGE Metric : In which value measures a specific instant in time
DELTA Metric : In which the value measures the change since it was last recorded
CUMULATIVE metric : In which the value constantly increases over time

Question asks, "Latency of HTTP responses" - This needs to be specific instant in time , which is GAUGE, hence C

upvoted 13 times

francisco_guerra Highly Voted 6 months, 2 weeks ago

Ans C:

A: Incorrect: Stacked bar could be but latency its used with distributions
B: Incorrect: If we used a cumulative the latency would be increasing in the graph.
C: Correct: Latency is commonly measured as a distribution.
D: Incorrect: METRIC_KIND_UNSPECIFIED is not the answer that gcp wanted.

Latency is commonly measured as a distribution. Given a distribution, you can measure various percentiles. For example, you might measure the number of requests that are slower than the historical 99th percentile.

Latency
histogram_quantile(0.9, rate(http_request_duration_seconds_bucket[7d])
histogram_quantile(0.99, rate(http_request_duration_seconds_bucket[7d]))

https://sre.google/workbook/implementing-slos/
https://cloud.google.com/architecture/adopting-slos/

upvoted 8 times

cloudbee Most Recent 1 week ago

Selected Answer: C

It's guage metric as it is asking latency of http responses.

upvoted 1 times

Charun 6 months, 2 weeks ago

C is correct

upvoted 8 times

ralf_cc 6 months, 3 weeks ago

Option B

upvoted 1 times

> **syslog** 6 months, 3 weeks ago
>
> Absolutely not. Cumulative means a growing graph, whose latency values add up to the previous ones, and it doesn't make sense. It's C for sure.
>
> upvoted 3 times

rinkeshgala1 7 months, 1 week ago

Option C

upvoted 4 times

zzz 7 months, 1 week ago

I think C

upvoted 2 times

Question #48 *Topic 1*

Your team is designing a new application for deployment both inside and outside Google Cloud Platform (GCP). You need to collect detailed metrics such as system resource utilization. You want to use centralized GCP services while minimizing the amount of work required to set up this collection system. What should you do?

A. Import the Stackdriver Profiler package, and configure it to relay function timing data to Stackdriver for further analysis.

B. Import the Stackdriver Debugger package, and configure the application to emit debug messages with timing information.

C. Instrument the code using a timing library, and publish the metrics via a health check endpoint that is scraped by Stackdriver.

D. Install an Application Performance Monitoring (APM) tool in both locations, and configure an export to a central data storage location for analysis.

Charun Highly Voted 6 months, 2 weeks ago
Answer A
upvoted 16 times

rinkeshgala1 Highly Voted 7 months, 1 week ago
may be A, as profiler works both inside and outside of GCP.
upvoted 5 times

> **akg001** 7 months, 1 week ago
> I agree. A is the right answer.
> upvoted 3 times

cloudbee Most Recent 1 week ago
Selected Answer: A
Profiler can be used outside GCP also it is used to measure cpu utilization by the application.
upvoted 1 times

ralf_cc 6 months, 3 weeks ago
It is A
upvoted 3 times

Question #49 Topic 1

You need to reduce the cost of virtual machines (VM) for your organization. After reviewing different options, you decide to leverage preemptible VM instances.
Which application is suitable for preemptible VMs?

A. A scalable in-memory caching system.

B. The organizationλ€™s public-facing website.

C. A distributed, eventually consistent NoSQL database cluster with sufficient quorum.

D. A GPU-accelerated video rendering platform that retrieves and stores videos in a storage bucket.

Charun Highly Voted 6 months, 2 weeks ago
D is correct
upvoted 10 times

devopsbatch Highly Voted 7 months ago
ans: D
upvoted 5 times

akg001 7 months ago
Agree with you on Answer D
upvoted 4 times

TNT87 Most Recent 4 months, 1 week ago
D
https://cloud.google.com/compute/docs/instances/preemptible
upvoted 3 times

ralf_cc 6 months, 3 weeks ago
D - external persistent storage
upvoted 4 times

Question #50 Topic 1

Your organization recently adopted a container-based workflow for application development. Your team develops numerous applications that are deployed continuously through an automated build pipeline to a Kubernetes cluster in the production environment. The security auditor is concerned that developers or operators could circumvent automated testing and push code changes to production without approval. What should you do to enforce approvals?

A. Configure the build system with protected branches that require pull request approval.

B. Use an Admission Controller to verify that incoming requests originate from approved sources.

C. Leverage Kubernetes Role-Based Access Control (RBAC) to restrict access to only approved users.

D. Enable binary authorization inside the Kubernetes cluster and configure the build pipeline as an attestor.

francisco_guerra Highly Voted 6 months, 2 weeks ago
this question is a little bit strange, but first we need to remove the invalid answers

B: Incorrect An admission controller is a piece of code that intercepts requests to the Kubernetes API server prior to persistence of the object, but after the request is authenticated and authorized. (its for security but not "enforce approvals")
C: Incorrect, we need to "enforce approvals" roles apply in the cluster and Ops always could push to production without approval.
A: Incorrect, for me this answer sound well but this does not sound that an answer for a gcp exam and this do not enforce the use of the pipeline.
D: Correct, they cannot push code to production without approval because their images are not signed.
upvoted 17 times

francisco_guerra Highly Voted 6 months, 1 week ago
I win the exam today so this questions help me a lot
upvoted 9 times

DarkMatterOne Most Recent 5 days, 7 hours ago
D
https://cloud.google.com/binary-authorization
Binary Authorization is a deploy-time security control that ensures only trusted container images are deployed on Google Kubernetes Engine (GKE) or Cloud Run. With Binary Authorization, you can require images to be signed by trusted authorities during the development process and then enforce signature validation when deploying. By enforcing validation, you can gain tighter control over your container environment by ensuring only verified images are integrated into the build-and-release process.
upvoted 1 times

maddy94 3 months, 2 weeks ago
Questions 51-55 is not available.. can someone please help me to get 51-55 questions?
upvoted 3 times

zanhsieh 6 months, 2 weeks ago
Agreed with D. The keywords here is "developers or operators". Option A the operators could push images to production without approval (operators could touch the cluster directly and the cluster cannot do any action against them). Rest same as francisco_guerra.
upvoted 4 times

ralf_cc 6 months, 3 weeks ago
D - PR approval will ensure the automated testing etc., the question is asking how to ensure all code changes go through the pipeline, where automated tests are integrated
upvoted 1 times

akg001 7 months ago
Answer C is the most close answer. Leverage best practice .
answer A is for pulling the code but in the question , the security auditor is concern about pushing the code .
upvoted 1 times

devopsbatch 7 months ago
A could be the ans
upvoted 1 times

akg001 7 months ago
I think you are right : A
https://github.community/t/best-practices-for-protected-branches/10204
upvoted 1 times

Question #51 *Topic 1*

You support a stateless web-based API that is deployed on a single Compute Engine instance in the europe-west2-a zone. The Service Level Indicator (SLI) for service availability is below the specified Service Level Objective (SLO). A postmortem has revealed that requests to the API regularly time out. The time outs are due to the API having a high number of requests and running out memory. You want to improve service availability. What should you do?

A. Change the specified SLO to match the measured SLI

B. Move the service to higher-specification compute instances with more memory

C. Set up additional service instances in other zones and load balance the traffic between all instances

D. Set up additional service instances in other zones and use them as a failover in case the primary instance is unavailable

Alaaelanwr Highly Voted 2 months, 2 weeks ago

Ans: C

upvoted 7 times

muk5658 Most Recent 1 month, 2 weeks ago

C, this option will offer resilience and distribute the load, also provides ability to configure health checks at VM level and Load Balancer can send only to Healthy Instances.

upvoted 1 times

Manh 2 months ago

ANSWER: C

upvoted 1 times

Question #52 | Topic 1

You are running a real-time gaming application on Compute Engine that has a production and testing environment. Each environment has their own Virtual Private
Cloud (VPC) network. The application frontend and backend servers are located on different subnets in the environment's VPC. You suspect there is a malicious process communicating intermittently in your production frontend servers. You want to ensure that network traffic is captured for analysis. What should you do?

A. Enable VPC Flow Logs on the production VPC network frontend and backend subnets only with a sample volume scale of 0.5.

B. Enable VPC Flow Logs on the production VPC network frontend and backend subnets only with a sample volume scale of 1.0.

C. Enable VPC Flow Logs on the testing and production VPC network frontend and backend subnets with a volume scale of 0.5. Apply changes in testing before production.

D. Enable VPC Flow Logs on the testing and production VPC network frontend and backend subnets with a volume scale of 1.0. Apply changes in testing before production.

NXD Highly Voted 2 months, 1 week ago
B

https://cloud.google.com/vpc/docs/flow-logs#log-sampling
upvoted 5 times

Suraj2611 Most Recent 2 months, 2 weeks ago
The Answer for this is B
upvoted 3 times

Alaaelanwr 2 months, 2 weeks ago
i think Answer: D
upvoted 1 times

muk5658 1 month, 2 weeks ago
Question clearly says only in Production they suspect, so we can eliminate the C and D options.
upvoted 1 times

giammydell 2 months, 1 week ago
if there isnt problem in test environment why log it
upvoted 3 times

Question #53 Topic 1

Your team of Infrastructure DevOps Engineers is growing, and you are starting to use Terraform to manage infrastructure. You need a way to implement code versioning and to share code with other team members. What should you do?

A. Store the Terraform code in a version-control system. Establish procedures for pushing new versions and merging with the master.

B. Store the Terraform code in a network shared folder with child folders for each version release. Ensure that everyone works on different files.

C. Store the Terraform code in a Cloud Storage bucket using object versioning. Give access to the bucket to every team member so they can download the files.

D. Store the Terraform code in a shared Google Drive folder so it syncs automatically to every team memberג€™s computer. Organize files with a naming convention that identifies each new version.

giammydell Highly Voted 2 months, 1 week ago
A for sure
upvoted 7 times

Suraj2611 Most Recent 2 months, 2 weeks ago
A is the guaranteed ans
upvoted 2 times

TNT87 2 months, 2 weeks ago
Ans A
https://www.terraform.io/docs/cloud/guides/recommended-practices/part3.3.html
upvoted 3 times

job_search83 2 months, 2 weeks ago
A for sure
upvoted 3 times

Question #54 *Topic 1*

You are using Stackdriver to monitor applications hosted on Google Cloud Platform (GCP). You recently deployed a new application, but its logs are not appearing on the Stackdriver dashboard.
You need to troubleshoot the issue. What should you do?

A. Confirm that the Stackdriver agent has been installed in the hosting virtual machine.

B. Confirm that your account has the proper permissions to use the Stackdriver dashboard.

C. Confirm that port 25 has been opened in the firewall to allow messages through to Stackdriver.

D. Confirm that the application is using the required client library and the service account key has proper permissions.

TNT87 2 weeks, 2 days ago
The correct answer is A not D..D is mentioning one wrong thing thats why.
https://cloud.google.com/logging/docs/agent/logging/troubleshooting#try-installing
upvoted 1 times

not_thanos 3 weeks, 3 days ago
Selected Answer: A
A and D seems correct. I think D is less correct because since you are hosting on GCP, best practice is to not add a service account to the application itself but instead leverage the native logging capabilities of GCP's offerings like GKE, GCP, etc.
upvoted 3 times

TNT87 1 month ago
https://cloud.google.com/logging/docs/agent/logging/troubleshooting#verifying_default_service_account_permission
Ans D
upvoted 2 times

hfudjdn 1 month, 4 weeks ago
D - The question states that you are already using Stackdriver for the GCE instance (assuming the agent is already installed). However, the "new" application has issues shipping the logs
upvoted 4 times

> **JohnnieWalker** 1 month, 3 weeks ago
> The question mention application logs, not only monitoring metrics, so I think "D" is correct.
> The stackdriver agent would only provide metrics of resources. I think you need to setup logging "client libraries" on the application in order to have the logs, therefore "D". https://cloud.google.com/logging/docs/reference/libraries
> upvoted 3 times

tee_dee26 1 month, 4 weeks ago
A is the answer
upvoted 1 times

Dreamingjin 2 months, 1 week ago
D. There is no mention about fluentd. So A is incorrect
upvoted 1 times

NXD 2 months, 1 week ago
Both A and D are valid. But the first step should be A. So answer A is better.
upvoted 3 times

giammydell 2 months, 1 week ago
why not D, it is about application log. The question seems that stackdriver is already used
upvoted 1 times

job_search83 2 months, 2 weeks ago
A
B is wrong, "use the Stackdriver dashboard" no such thing.
upvoted 2 times

Question #55 *Topic 1*

Your organization recently adopted a container-based workflow for application development. Your team develops numerous applications that are deployed continuously through an automated build pipeline to the production environment. A recent security audit alerted your team that the code pushed to production could contain vulnerabilities and that the existing tooling around virtual machine (VM) vulnerabilities no longer applies to the containerized environment. You need to ensure the security and patch level of all code running through the pipeline. What should you do?

A. Set up Container Analysis to scan and report Common Vulnerabilities and Exposures.

B. Configure the containers in the build pipeline to always update themselves before release.

C. Reconfigure the existing operating system vulnerability software to exist inside the container.

D. Implement static code analysis tooling against the Docker files used to create the containers.

giammydell 2 months, 1 week ago
A is correct for me
upvoted 4 times

Alaaelanwr 2 months, 2 weeks ago
Ans: A
upvoted 3 times

job_search83 2 months, 2 weeks ago
should be A
upvoted 3 times

Question #56 Topic 1

You use Cloud Build to build your application. You want to reduce the build time while minimizing cost and development effort. What should you do?

A. Use Cloud Storage to cache intermediate artifacts.

B. Run multiple Jenkins agents to parallelize the build.

C. Use multiple smaller build steps to minimize execution time.

D. Use larger Cloud Build virtual machines (VMs) by using the machine-type option.

TNT87 Highly Voted 2 months, 2 weeks ago
Ans A
https://cloud.google.com/storage/docs/best-practices
upvoted 6 times

TNT87 Most Recent 2 weeks ago
Selected Answer: A
Ans A and thats cheap and fast
upvoted 1 times

TNT87 2 weeks, 1 day ago
minimising costs...high virtual machines are expensive
upvoted 1 times

bob_builder 3 weeks, 5 days ago
A - https://cloud.google.com/build/docs/speeding-up-builds#caching_directories_with_google_cloud_storage
upvoted 1 times

TNT87 1 month ago
lets correct something fellows ok. A is not ok, why, we can ok only use intermediate artifacts in Kaniko cache, not in Cloud storage, in cloud storage we use results not intermediate artifacts "You can copy the results of a previous build to a Google Cloud Storage bucket, use the results for faster calculation, and then copy the new results back to the bucket." go re-read the best practices and you will see what im talking about, then this leaves D as the correct answer.
https://cloud.google.com/build/docs/speeding-up-builds
upvoted 2 times

ESP_SAP 1 month ago
Correct Answer is (D):

Using custom virtual machine sizes
In addition to the standard machine type, Cloud Build provides four high-CPU virtual machine types to run your builds. To increase the speed of your build, select a virtual machine with a higher CPU. Requesting a high-CPU machine may increase the startup time of your build as Cloud Build only starts these machines on demand.

https://cloud.google.com/build/docs/speeding-up-builds
upvoted 4 times

> **TNT87** 1 month ago
> You are correct sir....
> upvoted 1 times
>
> **TNT87** 1 month ago
> in as much as D is correct A is also mentioned inthe Best practices
> upvoted 1 times

Tire 1 month, 2 weeks ago
Selected Answer: A
Caching directories with Google Cloud Storage
To increase the speed of a build, reuse the results from a previous build. You can copy the results of a previous build to a Google Cloud Storage bucket, use the results for faster calculation, and then copy the new results back to the bucket. Use this method when your build takes a long time and produces a small number of files that does not take time to copy to and from Google Cloud Storage.
upvoted 2 times

> **TNT87** 1 month ago
> results not intermediate artifacts, ok
> upvoted 1 times

muk5658 1 month, 2 weeks ago
Both A and D are valid options, but if we look in the question they are asking to Minimize Cost - Larger Compute Instances comes at price.
So I will go with A (Caching from GCS bucket)

upvoted 1 times

Manh 2 months ago
Ans is A
upvoted 1 times

Shasha1 2 months ago
A
https://cloud.google.com/build/docs/speeding-up-builds
upvoted 3 times

MBA_1 2 months, 1 week ago
A is not correct . From the Link shared -https://cloud.google.com/build/docs/speeding-up-builds - Cloud Build is to store previous builds and not intermediate. For Intermediate the ask is to use Kaniko.

If you scroll down. - you can find -- "To increase the speed of your build, select a virtual machine with a higher CPU. Requesting a high-CPU machine may increase the startup time of your build as Cloud Build only starts these machines on demand."

And hence C is the answer
upvoted 1 times

Manh 2 months ago
both A and D seems correct
upvoted 1 times

Manh 2 months ago
but the question is asking for "You want to reduce the build time while minimizing cost and development effort"
-> only A is best option
upvoted 2 times

MBA_1 2 months, 1 week ago
Sorry, I meant D is the answer
upvoted 1 times

TNT87 2 months, 1 week ago
Anyone writing the exam soon, lets collaborate and discuss , get th right answers for all these, anyone willing?
upvoted 1 times

WakandaF 2 months, 2 weeks ago
Why not C?
upvoted 1 times

NXD 2 months, 1 week ago
C is correct only if these steps in parallel.
Because we don't know if they could be run in parallel, A is better.
upvoted 1 times

job_search83 2 months, 2 weeks ago
A, caching, https://cloud.google.com/build/docs/speeding-up-builds
upvoted 4 times

MF2C 2 months ago
A caching
upvoted 1 times

Question #57 *Topic 1*

You support a web application that is hosted on Compute Engine. The application provides a booking service for thousands of users. Shortly after the release of a new feature, your monitoring dashboard shows that all users are experiencing latency at login. You want to mitigate the impact of the incident on the users of your service. What should you do first?

A. Roll back the recent release.

B. Review the Stackdriver monitoring.

C. Upsize the virtual machines running the login services.

D. Deploy a new release to see whether it fixes the problem.

PJ_2021 Highly Voted 1 month, 3 weeks ago

A Rollback is needed to mitigate the impact. Once the is done review can be done

upvoted 5 times

Manh Most Recent 2 months ago

A Rollback first

upvoted 1 times

MBA_1 2 months, 1 week ago

B - Find whats wrong with the system and mitigate. As the Q says only login is affected, So no point is rollback

upvoted 1 times

MF2C 2 months ago

you still use service you cannot login?

upvoted 1 times

MBA_1 2 months, 1 week ago

https://cloud.google.com/architecture/identifying-causes-of-app-latency-with-stackdriver-and-opencensus

upvoted 1 times

giammydell 2 months, 1 week ago

But the question is about mitigating the problema, with the rollback the system goes back to the old version.

upvoted 3 times

TNT87 2 months ago

roll back is the answer

upvoted 2 times

Nik22 2 months, 2 weeks ago

First roll back and then use monitoring to review what went wrong.

upvoted 4 times

job_search83 2 months, 2 weeks ago

A rollback

upvoted 4 times

Question #58 | *Topic 1*

You are deploying an application that needs to access sensitive information. You need to ensure that this information is encrypted and the risk of exposure is minimal if a breach occurs. What should you do?

A. Store the encryption keys in Cloud Key Management Service (KMS) and rotate the keys frequently

B. Inject the secret at the time of instance creation via an encrypted configuration management system.

C. Integrate the application with a Single sign-on (SSO) system and do not expose secrets to the application.

D. Leverage a continuous build pipeline that produces multiple versions of the secret for each instance of the application.

giammydell Highly Voted 2 months, 1 week ago
Ans: A
upvoted 5 times

TNT87 Most Recent 2 months, 2 weeks ago
https://cloud.google.com/security-key-management
upvoted 1 times

TNT87 2 months, 2 weeks ago
Ans is A.
upvoted 2 times

Alaaelanwr 2 months, 2 weeks ago
Ans: A
upvoted 3 times

Question #59 Topic 1

You encounter a large number of outages in the production systems you support. You receive alerts for all the outages that wake you up at night. The alerts are due to unhealthy systems that are automatically restarted within a minute. You want to set up a process that would prevent staff burnout while following Site
Reliability Engineering practices. What should you do?

A. Eliminate unactionable alerts.

B. Create an incident report for each of the alerts.

C. Distribute the alerts to engineers in different time zones.

D. Redefine the related Service Level Objective so that the error budget is not exhausted.

AL12 Highly Voted 2 months, 1 week ago
I reckon its A, the reason is because it seems like the problem is automatically fixed with an restart of the service after a minute, therefore engineers don't really need to be woken up about these problems. If it failed multiple times or if the restart failed, then the engineer should be woken up
upvoted 7 times

MF2C 2 months ago
A or C
upvoted 1 times

gcpz Most Recent 1 week, 4 days ago
answer is c. it follows google SRE and prevents staff burnout. https://sre.google/workbook/team-lifecycles/
upvoted 1 times

ESP_SAP 1 month ago
The team may continue to work on non-reliability features if:

The outage was caused by a company-wide networking problem.
The outage was caused by a service maintained by another team, who have themselves frozen releases to address their reliability issues.
The error budget was consumed by users out of scope for the SLO (e.g., load tests or penetration testers).
Miscategorized errors consume budget even though no users were impacted.

https://sre.google/workbook/error-budget-policy/
upvoted 3 times

ESP_SAP 1 month ago
Correct Answer is (D):
upvoted 2 times

Manh 2 months ago
Answer D
upvoted 1 times

NXD 2 months, 1 week ago
C follows the SRE.
upvoted 3 times

TNT87 2 months, 2 weeks ago
Ans D
https://www.atlassian.com/incident-management/kpis/error-budget
upvoted 4 times

TNT87 2 weeks, 1 day ago
Ans A...point of correction
upvoted 1 times

TNT87 2 weeks, 1 day ago
NO!D is correct
upvoted 1 times

neutrino9 2 months, 2 weeks ago
Should be A
upvoted 3 times

job_search83 2 months, 2 weeks ago
D redefine SLI
upvoted 1 times

Question #60 Topic 1

You have migrated an e-commerce application to Google Cloud Platform (GCP). You want to prepare the application for the upcoming busy season. What should you do first to prepare for the busy season?

A. Load teat the application to profile its performance for scaling.

B. Enable AutoScaling on the production clusters, in case there is growth.

C. Pre-provision double the compute power used last season, expecting growth.

D. Create a runbook on inflating the disaster recovery (DR) environment if there is growth.

NXD Highly Voted 2 months, 1 week ago
https://cloud.google.com/architecture/black-friday-production-readiness#preparation_stage

The objective of the preparation stage is to test the system's ability to scale for peak user traffic and to document the results. Completing the preparation stage results in architecture refinement to handle peak traffic more efficiently and increase system reliability. This stage also yields procedures for operations and support that help streamline processes for handling the peak event and any issues that might occur. Consider this stage as practice for the peak event from a system and operations perspective.

A is exactly what mentioned above.
B is the step after the preparation stage.
upvoted 7 times

TNT87 1 month, 2 weeks ago
Changing the architecture for scale and reliability
Load testing and failure testing, along with architecture reviews, encourage limited-scope architectural changes that can enhance the scale and reliability of the system. However, introducing changes adds risk, so limit the changes to a conservative range of time.https://cloud.google.com/architecture/black-friday-production-readiness#changing_the_architecture_for_scale_and_reliability
upvoted 1 times

TNT87 Most Recent 1 week, 6 days ago
Selected Answer: A
Set up load and performance testing
Load testing is the process of deploying a test version of the system and creating requests to simulate high use of the system. Load testing normally focuses on testing for sustainable user-perceived behavior at some percentile below the absolute peak. Testing for peak requires hitting that top percentile with consistent good performance.
upvoted 1 times

TNT87 2 weeks ago
Selected Answer: B
B is the answer
upvoted 1 times

TNT87 1 week, 6 days ago
Sorry guys this is wrong
upvoted 1 times

TNT87 1 month ago
https://cloud.google.com/blog/topics/retail/preparing-for-peak-holiday-season-while-wfh
Ans A makes sense according to this doc
upvoted 1 times

tee_dee26 1 month, 4 weeks ago
Passed exam a couple of days ago. Chose A
upvoted 4 times

MBA_1 2 months, 1 week ago
Should be A , To check how application performs with load
upvoted 4 times

Manh 2 months ago
Agree with A
upvoted 1 times

Alaaelanwr 2 months, 1 week ago
Ans : B
upvoted 2 times

giammydell 2 months, 1 week ago
Ans: B

upvoted 2 times

TNT87 2 months, 2 weeks ago

Ans B
https://cloud.google.com/architecture/black-friday-production-readiness

upvoted 2 times

Question #61 Topic 1

You support a web application that runs on App Engine and uses CloudSQL and Cloud Storage for data storage. After a short spike in website traffic, you notice a big increase in latency for all user requests, increase in CPU use, and the number of processes running the application. Initial troubleshooting reveals:
- After the initial spike in traffic, load levels returned to normal but users still experience high latency.
- Requests for content from the CloudSQL database and images from Cloud Storage show the same high latency.
- No changes were made to the website around the time the latency increased.
- There is no increase in the number of errors to the users.

You expect another spike in website traffic in the coming days and want to make sure users don't experience latency. What should you do?

A. Upgrade the GCS buckets to Multi-Regional.

B. Enable high availability on the CloudSQL instances.

C. Move the application from App Engine to Compute Engine.

D. Modify the App Engine configuration to have additional idle instances.

TNT87 2 weeks ago
D is the answer
upvoted 1 times

TNT87 2 weeks ago
Selected Answer: D
D is the answer
upvoted 1 times

ESP_SAP 1 month, 1 week ago
Correct Answer is D:

Scaling App Engine scales the number of instances automatically in response to processing volume. This scaling factors in the automatic_scaling settings that are provided on a per-version basis in the configuration file. 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. You configure the number of instances of each version in that service's configuration file. The number of instances usually corresponds to the size of a dataset being held in memory or the desired throughput for offline work. You can adjust the number of instances of a manually-scaled version very quickly, without stopping instances that are currently running, using the Modules API set_num_instances function.

https://cloud.google.com/appengine/docs/standard/python/how-instances-are-managed
upvoted 2 times

Biden 1 month, 3 weeks ago
D looks like the nearest correct solution though this will not address with high latency with CloudSQL & storage instances
upvoted 1 times

MBA_1 2 months, 1 week ago
D is correct - https://cloud.google.com/appengine/docs/standard/python/config/appref
max_idle_instances
Optional. The maximum number of idle instances that App Engine should maintain for this version. Specify a value from 1 to 1000. If not specified, the default value is automatic, which means App Engine will manage the number of idle instances. Keep the following in mind:

A high maximum reduces the number of idle instances more gradually when load levels return to normal after a spike. This helps your application maintain steady performance through fluctuations in request load, but also raises the number of idle instances (and consequent running costs) during such periods of heavy load.
upvoted 2 times

Manh 2 months ago
Agree with D
upvoted 1 times

NXD 2 months, 1 week ago
D is correct to me.

A: wrong – because increase in latency for all user requests, not for specific region. So
B: wrong – problem affects both database and GCS
C: wrong

increase in CPU use, and the number of processes running the application => problem is that CPU is not enough to run application processes.
upvoted 2 times

giammydell 2 months, 2 weeks ago
B could be useful but does not solve latency problem on Cloud Storage side

upvoted 3 times

TNT87 2 months, 2 weeks ago
Ans B
https://cloud.google.com/sql/docs/mysql/high-availability
upvoted 2 times

TNT87 1 month, 2 weeks ago
Ans D,B has latency issues
upvoted 1 times

Nik22 2 months, 2 weeks ago
A. Upgrade the GCS buckets to Multi-Regional.
B. Enable high availability on the CloudSQL instances.
C. Move the application from App Engine to Compute Engine.
D. Modify the App Engine configuration to have additional idle instances.

There is nothing in the question that talks about region. If I assume that bucket is created in the region where the app is deployed
B - Gives redundancy. I don't see how this can improve the latency
C - Does not make any sense
D - Additional instance, would reduce the CPU Time & memory.

I would go with D. But not too sure.
upvoted 2 times

Question #62 *Topic 1*

Your application runs on Google Cloud Platform (GCP). You need to implement Jenkins for deploying application releases to GCP. You want to streamline the release process, lower operational toil, and keep user data secure. What should you do?

A. Implement Jenkins on local workstations.

B. Implement Jenkins on Kubernetes on-premises.

C. Implement Jenkins on Google Cloud Functions.

D. Implement Jenkins on Compute Engine virtual machines.

muk5658 1 month, 2 weeks ago
I am sorry ignore my previous comment, they are saying Kubernetes on Premise, not GKE (Google Managed), so I would go with GCE.
upvoted 1 times

muk5658 1 month, 2 weeks ago
I believe its B - GKE since they are saying reducing the toil and secure. We can use GKE secrets and also enabling autoscaling.

Correct me if my thinking is wrong
upvoted 1 times

TNT87 2 months, 2 weeks ago
he Google Compute Engine (GCE) Plugin allows you to use GCE virtual machines (VMs) with Jenkins to execute build tasks. GCE VMs provision quickly, are destroyed by Jenkins when idle, and offer Preemptible VMs that run at a much lower price than regular VMs.
upvoted 3 times

MF2C 2 months ago
yes, Jenkins only got 2 options for GCP as of now, GKE or compute engine
upvoted 1 times

TNT87 2 months, 2 weeks ago
Ans D
https://plugins.jenkins.io/google-compute-engine/
upvoted 3 times

job_search83 2 months, 2 weeks ago
D, GCE
upvoted 3 times

Question #63 Topic 1

You are working with a government agency that requires you to archive application logs for seven years. You need to configure Stackdriver to export and store the logs while minimizing costs of storage. What should you do?

A. Create a Cloud Storage bucket and develop your application to send logs directly to the bucket.

B. Develop an App Engine application that pulls the logs from Stackdriver and saves them in BigQuery.

C. Create an export in Stackdriver and configure Cloud Pub/Sub to store logs in permanent storage for seven years.

D. Create a sink in Stackdriver, name it, create a bucket on Cloud Storage for storing archived logs, and then select the bucket as the log export destination.

Manh 2 months ago
Answer D
https://cloud.google.com/logging/docs/routing/overview
upvoted 3 times

giammydell 2 months, 1 week ago
ans: D
upvoted 3 times

Alaaelanwr 2 months, 1 week ago
Ans : D
upvoted 2 times

job_search83 2 months, 2 weeks ago
D, sink
upvoted 4 times

Question #64 Topic 1

You support a trading application written in Python and hosted on App Engine flexible environment. You want to customize the error information being sent to
Stackdriver Error Reporting. What should you do?

A. Install the Stackdriver Error Reporting library for Python, and then run your code on a Compute Engine VM.

B. Install the Stackdriver Error Reporting library for Python, and then run your code on Google Kubernetes Engine.

C. Install the Stackdriver Error Reporting library for Python, and then run your code on App Engine flexible environment.

D. Use the Stackdriver Error Reporting API to write errors from your application to ReportedErrorEvent, and then generate log entries with properly formatted error messages in Stackdriver Logging.

muk5658 1 month, 2 weeks ago
@TNT87 - Answer is C, the link you shared has a pip install in the beginning which means Python requires installing library first.
pip install --upgrade google-cloud-error-reporting
upvoted 4 times

TNT87 1 month ago
Ans C https://cloud.google.com/error-reporting/docs/setup/python
i think you can see that 1 month ago answered it ok, the one with answer D was a mistake
upvoted 1 times

TNT87 1 month ago
App Engine flexible environment
App Engine grants the Error Reporting Writer role by default.

The Error Reporting library for Python can be used without needing to explicitly provide credentials.

Error Reporting is automatically enabled for App Engine flexible environment applications. No additional setup is required.
Yes anser is C
https://cloud.google.com/error-reporting/docs/setup/python#app-engine
upvoted 1 times

TNT87 1 month, 2 weeks ago
Ans D
https://cloud.google.com/error-reporting/docs/reference/libraries#client-libraries-install-python
upvoted 1 times

muk5658 1 month, 2 weeks ago
C for sure - https://cloud.google.com/error-reporting/docs/setup/python
upvoted 1 times

tee_dee26 1 month, 4 weeks ago
Exam passed. Answer chosen was D
upvoted 2 times

TNT87 1 month ago
you answered wrong, here is what google says, re read the question
App Engine flexible environment
App Engine grants the Error Reporting Writer role by default.

The Error Reporting library for Python can be used without needing to explicitly provide credentials.

Error Reporting is automatically enabled for App Engine flexible environment applications. No additional setup is required.
upvoted 1 times

Manh 2 months ago
Ans is C.
the question is asking about "You want to customize the error information being sent to
Stackdriver Error Reporting."
so you can use the instrumentation libraries available for a number of languages:
https://cloud.google.com/error-reporting/docs/setup/app-engine-flexible-environment
upvoted 3 times

awrgdasfg 1 month, 3 weeks ago
Yes. "Customization" is key: https://cloud.google.com/error-reporting/docs/setup/app-engine-flexible-environment#examples_using_the_instrumentation_libraries
upvoted 2 times

MBA_1 2 months, 1 week ago

Answer is D
From the Link - https://cloud.google.com/error-reporting/docs/setup/python
App Engine flexible environment
App Engine grants the Error Reporting Writer role by default.

The Error Reporting library for Python can be used without needing to explicitly provide credentials.

Error Reporting is automatically enabled for App Engine flexible environment applications. No additional setup is required.
Note: Error logs written to stderr are processed automatically by Error Reporting, without needing to use the Error Reporting library for Python directly.

upvoted 2 times

AL12 2 months, 1 week ago
You need to install the library in python yes, but when you add the code to your python code, you technically call the error report API where you can manually report errors/probably customise the error reporting as well. So i think it might be D

upvoted 1 times

Alaaelanwr 2 months, 1 week ago
Ans : C

upvoted 2 times

TNT87 2 months, 2 weeks ago
C,is correct

upvoted 1 times

job_search83 2 months, 2 weeks ago
C, https://cloud.google.com/error-reporting/docs/setup/python

upvoted 4 times

Question #65 *Topic 1*

You need to define Service Level Objectives (SLOs) for a high-traffic multi-region web application. Customers expect the application to always be available and have fast response times. Customers are currently happy with the application performance and availability. Based on current measurement, you observe that the
90
percentile of latency is 120ms and the 95
percentile of latency is 275ms over a 28-day window. What latency SLO would you recommend to the team to th th publish?

A. 90 percentile 100 "€ms th 95 percentile 250 "€ms th

B. 90 percentile 120 "€ms th 95 percentile 275 "€ms th

C. 90 percentile 150 "€ms th 95 percentile 300 "€ms th

D. 90 percentile 250 "€ms th 95 percentile 400 "€ms th

job_search83 Highly Voted 2 months, 2 weeks ago
C, https://sre.google/sre-book/service-level-objectives/
"Don't pick a target based on current performance"

upvoted 10 times

Nik22 Highly Voted 2 months, 2 weeks ago
Picking an SLO based upon current performance can commit you to unnecessarily strict SLOs. Select slightly lower SLO. Will go wtih C

upvoted 5 times

Manh Most Recent 2 months ago
Agree with answer C

upvoted 1 times

giammydell 2 months, 1 week ago
SLO is selected well if User are happy. B is correct

upvoted 2 times

Question #66 Topic 1

You support a large service with a well-defined Service Level Objective (SLO). The development team deploys new releases of the service multiple times a week.
If a major incident causes the service to miss its SLO, you want the development team to shift its focus from working on features to improving service reliability.
What should you do before a major incident occurs?

A. Develop an appropriate error budget policy in cooperation with all service stakeholders.

B. Negotiate with the product team to always prioritize service reliability over releasing new features.

C. Negotiate with the development team to reduce the release frequency to no more than once a week.

D. Add a plugin to your Jenkins pipeline that prevents new releases whenever your service is out of SLO.

smoaz 1 week, 6 days ago
Correct answer: A
upvoted 1 times

TNT87 2 weeks ago
Selected Answer: A
the reason why A is the answer we want something that is in relation to A....Service reliability, and who needs that service to be reliable its the customer, remember as Devops engneer you must put yourself inthe shoes of a customer.
upvoted 1 times

TNT87 2 weeks ago
Selected Answer: A
thats the enswer
upvoted 1 times

not_thanos 3 weeks, 3 days ago
I don't think the answer should be A.
Error Budget = 100% - SLO.
Since the SLO is "well defined", ideally the Error Budget is going to already be well defined as well.
upvoted 2 times

Biden 3 weeks, 6 days ago
Correct Answer - A
Error Budget Definition: A "Quantitative" measurement shared between SRE & product teams to balance innovation and stability. Hence first step is defining this "quantitative" error budget(Answer A). Only when there is risk of exceeding error budget then negotiate with product team (stakeholder) to prioritize reliability over features (option B)
upvoted 2 times

ESP_SAP 1 month ago
Correct Answer is (B):
When developing for your system, think of reliability as a feature, and in fact your most important feature, as customers simply expect that things 'just work'.
Once you have your objectives, reliability engineering provides practices to help you reach them, including:
• Redundancy systems: Such as contingencies for using backup servers
• Fault tolerance: Such as error correction algorithms for incoming network data
• Preventative maintenance: Such as cycling through hardware resources before failure through overuse
• Human error prevention: Such as cleaning and validating human input into the system
• Reliability optimization: Such as writing code optimized for quick and consistent loading
Keeping these reliability practices in mind as you develop will make your code acceptably reliable. At the same time, you're able to confidently accelerate development by evaluating it against SLOs.
upvoted 1 times

TNT87 1 month ago
Ans B
https://www.fullstory.com/blog/bootstrapping-an-availability-program-using-sre-principles/
Lets not forget the principles of availbility & reliabilty
upvoted 1 times

Manh 2 months ago
Should be A
upvoted 3 times

MF2C 2 months ago
the key is "shift its focus from working on features to improving service reliability" which means to reduce risky deployment and the answer should be B
upvoted 2 times

sindra 2 months, 1 week ago

I think it should be A

upvoted 3 times

giammydell 2 months, 1 week ago

Could be A but also D: the request is preventing deployment of new release when SLO is missing

upvoted 2 times

job_search83 2 months, 2 weeks ago

A, error budget https://sre.google/sre-book/embracing-risk/#xref_risk-management_unreliability-budgets

upvoted 3 times

giammydell 2 months, 1 week ago

why stakeholders are involved in the error budget definition

upvoted 2 times

Dreamingjin 2 months, 1 week ago

Just provider can be involved.

upvoted 1 times

Question #67 Topic 1

Your company is developing applications that are deployed on Google Kubernetes Engine (GKE). Each team manages a different application. You need to create the development and production environments for each team, while minimizing costs. Different teams should not be able to access other teams' environments.
What should you do?

A. Create one GCP Project per team. In each project, create a cluster for Development and one for Production. Grant the teams IAM access to their respective clusters.

B. Create one GCP Project per team. In each project, create a cluster with a Kubernetes namespace for Development and one for Production. Grant the teams IAM access to their respective clusters.

C. Create a Development and a Production GKE cluster in separate projects. In each cluster, create a Kubernetes namespace per team, and then configure Identity Aware Proxy so that each team can only access its own namespace.

D. Create a Development and a Production GKE cluster in separate projects. In each cluster, create a Kubernetes namespace per team, and then configure Kubernetes Role-based access control (RBAC) so that each team can only access its own namespace.

TNT87 Highly Voted 2 months, 2 weeks ago
https://cloud.google.com/architecture/prep-kubernetes-engine-for-prod#roles_and_groups
Ans D
upvoted 10 times

guid1984 Most Recent 2 weeks, 5 days ago
The answer is D (enterprise multi-tenancy using GKE, reduce costs and control access by RBAC)
upvoted 1 times

muk5658 1 month, 2 weeks ago
D -100%
upvoted 2 times

Manh 2 months ago
Sound like B is good ans

B. Create one GCP Project per team. In each project, create a cluster with a Kubernetes namespace for Development and one for Production. Grant the teams IAM access to their respective clusters.

1 project and 1 cluster per team with 2 namespace
upvoted 1 times

PJ_2021 1 month, 3 weeks ago
Mate you have one project per app per environment. You explaination clearly violates this basic principle
upvoted 2 times

TNT87 1 month, 2 weeks ago
Re-read the question again....and we cant mix development and production project NO!
upvoted 1 times

NXD 2 months, 1 week ago
I go with A.
upvoted 2 times

Biden 1 month, 3 weeks ago
I will go with A since PROD and DEV/TEST environments need to kept separate always. Having them in the same cluster, may impact the resources for PROD when there is a need to do a load testing spinning off multiple PODs and nodes
upvoted 1 times

TNT87 2 weeks, 1 day ago
https://www.google.com/search?q=For+almost+all+cases%2C+Kubernetes+RBAC+can+be+used+instead+of+IAM.+GKE+users+require+at+minimum%2C+the+container.clusters.get+IAM+permission+in+the+project+...&oq=For+almost+all+cases%2C+Kubernetes+RBAC+can+be+used+instead+of+IAM.+GKE+users+require+at+minimum%2C+the+container.clusters.get+IAM+permission+in+the+project+...&aqs=chrome..69i57.479j0j7&sourceid=chrome&ie=UTF-8
upvoted 1 times

giammydell 2 months, 1 week ago
but you have to minimize the cost
upvoted 1 times

Alaaelanwr 2 months, 1 week ago

Ans: D

upvoted 3 times

Nik22 2 months, 2 weeks ago

Will go with D

upvoted 3 times

Question #68 *Topic 1*

Some of your production services are running in Google Kubernetes Engine (GKE) in the eu-west-1 region. Your build system runs in the us-west-1 region. You want to push the container images from your build system to a scalable registry to maximize the bandwidth for transferring the images to the cluster. What should you do?

A. Push the images to Google Container Registry (GCR) using the gcr.io hostname.

B. Push the images to Google Container Registry (GCR) using the us.gcr.io hostname.

C. Push the images to Google Container Registry (GCR) using the eu.gcr.io hostname.

D. Push the images to a private image registry running on a Compute Engine instance in the eu-west-1 region.

Nik22 Highly Voted 2 months, 2 weeks ago

To maximize the bandwidth for transferring the images to the cluster, one needs the the registry to be closer to the production or system where it needs to be deployed. I would go with C, since the production system is in Europe.

upvoted 5 times

Manh Most Recent 2 months ago

C for sure

upvoted 1 times

MBA_1 2 months ago

It's C - because of GDPR compliance.

Hostname Storage location
gcr.io Stores images in data centers in the United States
asia.gcr.io Stores images in data centers in Asia
eu.gcr.io Stores images in data centers within member states of the European Union
us.gcr.io Stores images in data centers in the United States

upvoted 2 times

giammydell 2 months, 1 week ago

C could be correct, but also D is nearer because in the same zone. A and B are are both in US

upvoted 2 times

Question #69 *Topic 1*

You manage several production systems that run on Compute Engine in the same Google Cloud Platform (GCP) project. Each system has its own set of dedicated Compute Engine instances. You want to know how must it costs to run each of the systems. What should you do?

A. In the Google Cloud Platform Console, use the Cost Breakdown section to visualize the costs per system.

B. Assign all instances a label specific to the system they run. Configure BigQuery billing export and query costs per label.

C. Enrich all instances with metadata specific to the system they run. Configure Stackdriver Logging to export to BigQuery, and query costs based on the metadata.

D. Name each virtual machine (VM) after the system it runs. Set up a usage report export to a Cloud Storage bucket. Configure the bucket as a source in BigQuery to query costs based on VM name.

TNT87 Highly Voted 2 months, 2 weeks ago
https://cloud.google.com/billing/docs/how-to/export-data-bigquery; B
upvoted 7 times

not_thanos Most Recent 3 weeks, 3 days ago
Selected Answer: B
https://cloud.google.com/billing/docs/how-to/export-data-bigquery
upvoted 1 times

Manh 2 months ago
B. U NEED TO ADD LABELS TO INSTANCE FOR COST visibility
upvoted 2 times

job_search83 2 months, 2 weeks ago
B, labels
upvoted 3 times

Question #70 *Topic 1*

You use Cloud Build to build and deploy your application. You want to securely incorporate database credentials and other application secrets into the build pipeline. You also want to minimize the development effort. What should you do?

A. Create a Cloud Storage bucket and use the built-in encryption at rest. Store the secrets in the bucket and grant Cloud Build access to the bucket.

B. Encrypt the secrets and store them in the application repository. Store a decryption key in a separate repository and grant Cloud Build access to the repository.

C. Use client-side encryption to encrypt the secrets and store them in a Cloud Storage bucket. Store a decryption key in the bucket and grant Cloud Build access to the bucket.

D. Use Cloud Key Management Service (Cloud KMS) to encrypt the secrets and include them in your Cloud Build deployment configuration. Grant Cloud Build access to the KeyRing.

TNT87 Highly Voted 2 months, 1 week ago
Ans is D
upvoted 10 times

Alaaelanwr Most Recent 2 months, 1 week ago
Ans: D
upvoted 4 times

Question #71 | *Topic 1*

You support a popular mobile game application deployed on Google Kubernetes Engine (GKE) across several Google Cloud regions. Each region has multiple
Kubernetes clusters. You receive a report that none of the users in a specific region can connect to the application. You want to resolve the incident while following Site Reliability Engineering practices. What should you do first?

A. Reroute the user traffic from the affected region to other regions that donλ€™t report issues.

B. Use Stackdriver Monitoring to check for a spike in CPU or memory usage for the affected region.

C. Add an extra node pool that consists of high memory and high CPU machine type instances to the cluster.

D. Use Stackdriver Logging to filter on the clusters in the affected region, and inspect error messages in the logs.

job_search83 Highly Voted 2 months, 2 weeks ago
A, reroute trafic to unblock access to site.
upvoted 7 times

Manh Most Recent 2 months ago
A. Reroute the traffic first
upvoted 2 times

MF2C 2 months ago
A - resume service first
upvoted 3 times

TNT87 2 months ago
Anyone available for didscussion please lets collaborate
upvoted 2 times

Question #72 Topic 1

You are writing a postmortem for an incident that severely affected users. You want to prevent similar incidents in the future. Which two of the following sections should you include in the postmortem? (Choose two.)

A. An explanation of the root cause of the incident.

B. A list of employees responsible for causing the incident

C. A list of action items to prevent a recurrence of the incident

D. Your opinion of the incidentג€™s severity compared to past incidents

E. Copies of the design documents for all the services impacted by the incident

TNT87 Highly Voted 2 months, 2 weeks ago
Ans is AC
upvoted 9 times

MF2C Highly Voted 2 months ago
A n C are correct
upvoted 5 times

Alaaelanwr Most Recent 2 months, 1 week ago
Ans: AC
upvoted 5 times

TNT87 2 months, 2 weeks ago
https://cloud.google.com/blog/products/gcp/fearless-shared-postmortems-cre-life-lessons
upvoted 1 times

job_search83 2 months, 2 weeks ago
A,C explanation + list of actions to prevent in the future
upvoted 4 times

Question #73 | *Topic 1*

You are ready to deploy a new feature of a web-based application to production. You want to use Google Kubernetes Engine (GKE) to perform a phased rollout to half of the web server pods.
What should you do?

A. Use a partitioned rolling update.

B. Use Node taints with NoExecute.

C. Use a replica set in the deployment specification.

D. Use a stateful set with parallel pod management policy.

TNT87 Highly Voted 2 months, 2 weeks ago
I do agree to A as the answer.
upvoted 6 times

bob_builder Most Recent 3 weeks, 2 days ago
A => https://kubernetes.io/docs/concepts/workloads/controllers/statefulset/#partitions
upvoted 1 times

not_thanos 3 weeks, 3 days ago
https://cloud.google.com/kubernetes-engine/docs/how-to/updating-apps#partitioning_a_rollingupdate

partition rollout only works if the workload is stateful. Nothing in the question tells us this.
upvoted 1 times

Shasha1 2 months ago
A
https://medium.com/velotio-perspectives/exploring-upgrade-strategies-for-stateful-sets-in-kubernetes-c02b8286f251
upvoted 2 times

Question #74 *Topic 1*

You are responsible for the reliability of a high-volume enterprise application. A large number of users report that an important subset of the application's functionality `" a data intensive reporting feature `" is consistently failing with an HTTP 500 error. When you investigate your application's dashboards, you notice a strong correlation between the failures and a metric that represents the size of an internal queue used for generating reports. You trace the failures to a reporting backend that is experiencing high I/O wait times. You quickly fix the issue by resizing the backend's persistent disk (PD). How you need to create an availability
Service Level Indicator (SLI) for the report generation feature. How would you define it?

A. As the I/O wait times aggregated across all report generation backends

B. As the proportion of report generation requests that result in a successful response

C. As the applicationλ€™s report generation queue size compared to a known-good threshold

D. As the reporting backend PD throughout capacity compared to a known-good threshold

NXD Highly Voted 2 months, 1 week ago
The question is: "create an availability SLI for the report generation feature." => availability.

B is correct.
Others aren't availability SLI.
upvoted 8 times

MF2C 2 months ago
B is more like SLO rather than SLI.
upvoted 1 times

Shasha1 Highly Voted 2 months ago
B is correct, availability = good time/ total time.
upvoted 6 times

Manh 2 months ago
AGREE WITH B
upvoted 2 times

TNT87 Most Recent 2 weeks ago
Selected Answer: B
B B B B is the answer!
upvoted 1 times

sindra 2 months, 1 week ago
should be D.. since the throughput and IOPS become the issue
upvoted 2 times

giammydell 2 months, 1 week ago
Why not C, you already have a metric that represents the size of an internal queue
upvoted 2 times

Nik22 2 months, 1 week ago
D for sure
upvoted 1 times

Question #75 Topic 1

You have an application running in Google Kubernetes Engine. The application invokes multiple services per request but responds too slowly. You need to identify which downstream service or services are causing the delay. What should you do?

A. Analyze VPC flow logs along the path of the request.

B. Investigate the Liveness and Readiness probes for each service.

C. Create a Dataflow pipeline to analyze service metrics in real time.

D. Use a distributed tracing framework such as OpenTelemetry or Stackdriver Trace.

job_search83 Highly Voted 2 months, 2 weeks ago
D, opentelemetry
upvoted 9 times

TNT87 Most Recent 1 month ago
https://cloud.google.com/dataflow/docs/guides/using-monitoring-intf
upvoted 1 times

TNT87 1 month ago
This solution also explains how you can change the pipeline to run in streaming mode, for low-latency, asynchronous log processing
upvoted 1 times

TNT87 1 month ago
https://cloud.google.com/architecture/processing-logs-at-scale-using-dataflow?hl=en
Kindly read this and say why is C wrong
upvoted 1 times

giammydell 2 months, 1 week ago
Ans: D
upvoted 4 times

Dreamingjin 2 months, 1 week ago
B is correct
upvoted 1 times

Question #76 Topic 1

You are creating and assigning action items in a postmodern for an outage. The outage is over, but you need to address the root causes. You want to ensure that your team handles the action items quickly and efficiently. How should you assign owners and collaborators to action items?

A. Assign one owner for each action item and any necessary collaborators.

B. Assign multiple owners for each item to guarantee that the team addresses items quickly.

C. Assign collaborators but no individual owners to the items to keep the postmortem blameless.

D. Assign the team lead as the owner for all action items because they are in charge of the SRE team.

Trony Highly Voted 2 months, 1 week ago
A is correct. Each action item should have one owner.
upvoted 7 times

Manh 2 months ago
Agree with A
upvoted 4 times

Manh 2 months ago
https://sre.google/sre-book/example-postmortem/
upvoted 2 times

TNT87 Most Recent 2 weeks ago
The fact that the the question STRESSES that the outage is OVER ust give you a clue.
Check what google SRE book says

Missing ownership
Declaring official ownership results in accountability, which leads to action. Our example postmortem contains several examples of missing ownership:

The postmortem lists four owners. Ideally, an owner is a single point of contact who is responsible for the postmortem, follow-up, and completion.
The Action Items section has little or no ownership for its entries. Actions items without clear owners are less likely to be resolved.
It's better to have a single owner and multiple collaborators.
upvoted 1 times

TNT87 2 weeks, 2 days ago
https://devops.com/when-it-disaster-strikes-part-3-conducting-a-blameless-post-mortem/
then its A
upvoted 1 times

TNT87 2 weeks, 2 days ago
Missing ownership
Declaring official ownership results in accountability, which leads to action. Our example postmortem contains several examples of missing ownership:

The postmortem lists four owners. Ideally, an owner is a single point of contact who is responsible for the postmortem, follow-up, and completion.
The Action Items section has little or no ownership for its entries. Actions items without clear owners are less likely to be resolved.
It's better to have a single owner and multiple collaborators.
upvoted 1 times

Freemiums 1 month ago
Either A or C,
For answer C, the principles of postmortem culture it's blameless
Blameless postmortems are a tenet of SRE culture. For a postmortem to be truly blameless, it must focus on identifying the contributing causes of the incident without indicting any individual or team for bad or inappropriate behavior.
https://sre.google/sre-book/postmortem-culture/

However looking at the postmortem example, each assignment has an owner
https://sre.google/sre-book/example-postmortem/
upvoted 1 times

job_search83 2 months, 2 weeks ago
C, https://sre.google/sre-book/postmortem-culture/
upvoted 4 times

Manh 2 months ago
ans is A, mate
upvoted 2 times

TNT87 1 month ago

the answer is C because this must be kept blameless...

upvoted 1 times

Question #77 Topic 1

Your development team has created a new version of their service's API. You need to deploy the new versions of the API with the least disruption to third-party developers and end users of third-party installed applications. What should you do?

A. Introduce the new version of the API. Announce deprecation of the old version of the API. Deprecate the old version of the API. Contact remaining users of the old API. Provide best effort support to users of the old API. Turn down the old version of the API.

B. Announce deprecation of the old version of the API. Introduce the new version of the API. Contact remaining users on the old API. Deprecate the old version of the API. Turn down the old version of the API. Provide best effort support to users of the old API.

C. Announce deprecation of the old version of the API. Contact remaining users on the old API. Introduce the new version of the API. Deprecate the old version of the API. Provide best effort support to users of the old API. Turn down the old version of the API.

D. Introduce the new version of the API. Contact remaining users of the old API. Announce deprecation of the old version of the API. Deprecate the old version of the API. Turn down the old version of the API. Provide best effort support to users of the old API.

Dreamingjin Highly Voted 2 months, 1 week ago
A. Introduce new API ahead
upvoted 10 times

Biden 3 weeks, 6 days ago
no use contacting the users after the API is deprecated - they will come to know anyway when the API fails. Hence A is INCORRECT !!
upvoted 1 times

not_thanos 3 weeks, 3 days ago
It's not been turned off yet, so they will still be able to use it
upvoted 1 times

TNT87 Most Recent 2 weeks ago
Selected Answer: B
https://httptoolkit.tech/blog/how-to-turn-off-your-old-apis/
C the second action doesnt make sense, you will be supporting remaining users of what?
upvoted 1 times

smoaz 2 weeks, 5 days ago
A. Is correct 100%
upvoted 1 times

smoaz 2 weeks, 5 days ago
after you depreciate the old version of the Api. you must provide the support to the remaining users
upvoted 1 times

TNT87 2 weeks, 2 days ago
B is correct
upvoted 1 times

smoaz 2 weeks, 5 days ago
You can't contact the remaining users before you depreciate the old version of the API
upvoted 1 times

Biden 3 weeks, 6 days ago
Sorry friends ignore my previous comments..upon re-reading "A" makes more sense. "Deprecated" = function still works but not supported or recommended.
Hence Introduction --> Announce Deprecation --> Deprecate --> Best effort support --> Turn OFF ...makes perfect sense
upvoted 2 times

Biden 4 weeks ago
A - Incorrect - No use contacting the users of the old API after depreciating
B - Correct - since users are contacted before depreciation
C & D: Sequence doesnt make sense
upvoted 3 times

TNT87 2 weeks, 2 days ago
B is correct
upvoted 1 times

TNT87 1 month ago
Ans B
https://httptoolkit.tech/blog/how-to-turn-off-your-old-apis/
upvoted 3 times

Wwhite44 1 month, 3 weeks ago
It is not possible announce deprecation without introduce a new version, so B and C are not good. After new version introduction you cannot contact remaining old version user, you must before announce deprecation, so D is not good. My opinion, A is good
upvoted 3 times

MF2C 2 months ago
https://cloud.google.com/migrate/compute-engine/support/lifecycle
B is correct, announce must be first, best effort support to the last because after API sunset, no more patch to be released to support only based on best effort
upvoted 4 times

MBA_1 2 months ago
Answer is C - The correct sequence is provided.
upvoted 1 times

MBA_1 2 months ago
Sorry, it should be A. First it should be introduced and then the old version should be depreciated
upvoted 4 times

NXD 2 months, 1 week ago
C

Turn down the old version of the API must be the last step
Contact users must be before deprecate the old version.
upvoted 3 times

Question #78 | Topic 1

You are running an application on Compute Engine and collecting logs through Stackdriver. You discover that some personally identifiable information (PII) is leaking into certain log entry fields. You want to prevent these fields from being written in new log entries as quickly as possible. What should you do?

A. Use the filter-record-transformer Fluentd filter plugin to remove the fields from the log entries in flight.

B. Use the fluent-plugin-record-reformer Fluentd output plugin to remove the fields from the log entries in flight.

C. Wait for the application developers to patch the application, and then verify that the log entries are no longer exposing PII.

D. Stage log entries to Cloud Storage, and then trigger a Cloud Function to remove the fields and write the entries to Stackdriver via the Stackdriver Logging API.

MF2C Highly Voted 2 months ago
reformer is Fluentd plugin to add or replace fields of a event record, so ans is A
upvoted 5 times

not_thanos Most Recent 3 weeks, 3 days ago
Selected Answer: A
Seems both A and B will work.
However i will go with A, since it is included in the fluentd core and does not require installing a new plugin

"The filter_record_transformer filter plugin mutates/transforms incoming event streams in a versatile manner. If there is a need to add/delete/modify events, this plugin is the first filter to try.
It is included in the Fluentd's core."

https://docs.fluentd.org/filter/record_transformer
upvoted 3 times

not_thanos 3 weeks, 3 days ago
https://cloud.google.com/logging/docs/agent/logging/configuration#modifying_log_records
upvoted 1 times

MBA_1 2 months ago
Yes, its A and not B as fluent-plugin-google-cloud from https://cloud.google.com/logging/docs/agent/logging/configuration#cloud-fluentd-config

Besides the list of default logs that the Logging agent streams by default, you can customize the Logging agent to send additional logs to Logging or to adjust agent settings by adding input configurations.

The configuration definitions in these sections apply to the fluent-plugin-google-cloud output plugin only and specify how logs are transformed and ingested into Cloud Logging.
upvoted 3 times

giammydell 2 months, 1 week ago
I think A because The fluent-plugin-record-reformer output plugin provides functionality similar to the filter_record_transformer filter plugin, except that it also allows you to modify log tags
upvoted 3 times

Question #79 *Topic 1*

You support a service that recently had an outage. The outage was caused by a new release that exhausted the service memory resources. You rolled back the release successfully to mitigate the impact on users. You are now in charge of the post-mortem for the outage. You want to follow Site Reliability Engineering practices when developing the post-mortem. What should you do?

A. Focus on developing new features rather than avoiding the outages from recurring.

B. Focus on identifying the contributing causes of the incident rather than the individual responsible for the cause.

C. Plan individual meetings with all the engineers involved. Determine who approved and pushed the new release to production.

D. Use the Git history to find the related code commit. Prevent the engineer who made that commit from working on production services.

arunraveendran 1 month, 2 weeks ago
Ans: B
upvoted 4 times

sindra 1 month, 4 weeks ago
Agreed B
upvoted 2 times

Alaaelanwr 2 months ago
Ans: B
upvoted 3 times

sindra 2 months, 1 week ago
Confirm B
upvoted 2 times

giammydell 2 months, 1 week ago
Ans B, yes
upvoted 2 times

TNT87 2 months, 2 weeks ago
Ans B,yes
upvoted 3 times

Question #80 Topic 1

You support a user-facing web application. When analyzing the application's error budget over the previous six months, you notice that the application has never consumed more than 5% of its error budget in any given time window. You hold a Service Level Objective (SLO) review with business stakeholders and confirm that the SLO is set appropriately. You want your application's SLO to more closely reflect its observed reliability. What steps can you take to further that goal while balancing velocity, reliability, and business needs? (Choose two.)

A. Add more serving capacity to all of your applicationג€™s zones.

B. Have more frequent or potentially risky application releases.

C. Tighten the SLO match the applicationג€™s observed reliability.

D. Implement and measure additional Service Level Indicators (SLIs) fro the application.

E. Announce planned downtime to consume more error budget, and ensure that users are not depending on a tighter SLO.

TNT87 1 week, 6 days ago
https://cloud.google.com/blog/products/management-tools/sre-error-budgets-and-maintenance-windows This is the link to the answers of this question
upvoted 1 times

TNT87 2 weeks ago
Selected Answer: DE
These are the correct choices
upvoted 1 times

Biden 3 weeks, 6 days ago
Ask is "You want your application's SLO to MORE CLOSELY REFLECT its observed reliability".
Based on that C is correct, and also agree going ahead for a risky release.
Hence B&C !?
upvoted 2 times

Biden 4 weeks ago
C&D would be the closest correct answer.. risky release should never be considered - hence B is out.
upvoted 1 times

Biden 4 weeks ago
A doesnt make sense ..why to add more when there is no issue and the error budget is hardly utilized ?
upvoted 1 times

TNT87 1 month ago
Ans A,D
Its not always the case that they post wrong answers here, some of them are correct and this is one of the few correct answers. go and read SRE book
upvoted 1 times

azuretestingpoc 1 month, 2 weeks ago
in example global chubby outage plan they mentioned planned outages.
Also to increase the additional parameters in SLI
https://sre.google/sre-book/service-level-objectives/
I think it D & E
upvoted 1 times

sindra 1 month, 4 weeks ago
I think its B and D

B because we can innovate since the error budget only hit 5%
D it will help to obserb realitbiity better
upvoted 2 times

> **Biden** 1 month, 3 weeks ago
> Though B says "risky releases..." , B&D seems to be the least controversial option.
> upvoted 1 times

Manh 2 months ago
"You want your application's SLO to more closely reflect its observed reliability."
CD should be answer
upvoted 3 times

> **muk5658** 1 month, 2 weeks ago
> The question says - You hold a Service Level Objective (SLO) review with business stakeholders and confirm that the SLO is set appropriately.
> Which means we should not make any changes to SLO. I would go with B and D - Adopt more risky releases and add more SLI's to better

measure system.
upvoted 1 times

Shasha1 2 months ago
AD
C is not correct, If you implement the tighter SLO, you'll be permanently out of SLO and subject to your error budget policy. In this situation, you can make the refined SLO.
A ; - can add more zone to increase velocity,
D : can push new releases if error budget allows
upvoted 2 times

MBA_1 2 months ago
B+D. No way E because noone expects a downtime.
upvoted 1 times

Trony 2 months, 1 week ago
I would go for B+D:
-A: no, there's no reason to add capacity if we are barely scratching error budget;
-B: everything seems fine, so it's ok to dare with more innovative/risky releases;
-C: no, stakeholders said SLO is ok;
-D: adding additional SLIs (and so SLOs) might be a way to reflect observer reliability more closely;
-E: put the servers down for no reason is a no-no.
upvoted 4 times

Biden 4 weeks ago
there is no mention of innovation, only "risky"..hence not a right choices
upvoted 1 times

giammydell 2 months, 1 week ago
D+E, if SLO is ok for the business you have to increase the error budget using less resource or adding SLI monitoring other resourses
upvoted 2 times

TNT87 1 week, 6 days ago
True....
upvoted 1 times

Question #81 Topic 1

You support a service with a well-defined Service Level Objective (SLO). Over the previous 6 months, your service has consistently met its SLO and customer satisfaction has been consistently high. Most of your service's operations tasks are automated and few repetitive tasks occur frequently. You want to optimize the balance between reliability and deployment velocity while following site reliability engineering best practices. What should you do? (Choose two.)

A. Make the serviceג€™s SLO more strict.

B. Increase the serviceג€™s deployment velocity and/or risk.

C. Shift engineering time to other services that need more reliability.

D. Get the product team to prioritize reliability work over new features.

E. Change the implementation of your Service Level Indicators (SLIs) to increase coverage.

NXD Highly Voted 2 months, 1 week ago
BC

https://sre.google/workbook/implementing-slos/#slo-decision-matrix

A: wrong – SLO is already well-defined, customer satisfaction is high.
E: wrong – change SLI means how SLO, which is already well-defined.

CD are valid, but the best option is C because current product is already quite reliable.
upvoted 12 times

Manh 2 months ago
Agree with BC
upvoted 1 times

MF2C 2 months ago
yes B and C
upvoted 2 times

TNT87 Most Recent 2 weeks ago
Selected Answer: BC
These are the correct answers. Thank me later.

All the best guys
upvoted 1 times

TNT87 2 weeks, 2 days ago
After perusing the SRE book...
D, E Is correct, there is a question that is almost this very question but the wording is different
upvoted 1 times

TNT87 2 weeks ago
B C, ,,,, D; E Are for the previous question, number 80
upvoted 1 times

TNT87 1 month ago
Ans C; D are correct.
upvoted 1 times

TNT87 2 weeks ago
its a mistake here
upvoted 1 times

Alaaelanwr 2 months ago
i think BC
upvoted 3 times

Shasha1 2 months ago
i think CD are correct
regarding E i am not sure we can modify SLI after we defined
upvoted 2 times

giammydell 2 months, 1 week ago
I think B and E:
A No: SLO is well defined
B YES: the service met the SLO so you have error budget available for DEPLOY

C I think NO, you will reduce your team number
D NO higher reliability is unnecessary (SLO well defined)
E YES you can modify SLI to extend coverage