A. Supply the encryption key in a .boto configuration file. Use gsutil to upload the files.

B. Supply the encryption key using gcloud config. Use gsutil to upload the files to that bucket.

C. Use gsutil to upload the files, and use the flag --encryption-key to supply the encryption key.

D. Use gsutil to create a bucket, and use the flag --encryption-key to supply the encryption key. Use gsutil to upload the files to that bucket.

KouShikyou Highly Voted 5 years, 2 months ago

In GCP document, key could be configured in .boto.
I didn't find information show gsutil suppots flag "--encryption-key".

https://cloud.google.com/storage/docs/encryption/customer-supplied-keys

upvoted 46 times

JaimeMS 6 months, 1 week ago

The documentation is here:
https://cloud.google.com/storage/docs/encryption/using-customer-supplied-keys#upload-encrypt

Option C is correct. You can upload a file using customer-supplied encryption with the command:
gcloud storage cp SOURCE_DATA gs://BUCKET_NAME/OBJECT_NAME --encryption-key=YOUR_ENCRYPTION_KEY

upvoted 13 times

tartar 4 years, 4 months ago

A is ok

upvoted 16 times

nitinz 3 years, 9 months ago

A is correct

upvoted 4 times

kumarp6 4 years, 1 month ago

.boto file with encryption key, but it will works for individual users, every user should update their own .boto with same key. Also while retrieving you should use the same key to decryption.

upvoted 3 times

Eroc Highly Voted 5 years, 1 month ago

I agree, A.(https://cloud.google.com/storage/docs/gsutil/addlhelp/UsingEncryptionKeys#generating-customer-supplied-encryption-keys)

upvoted 18 times

mahi_h Most Recent 1 day, 11 hours ago

Selected Answer: D

I see option D is not even discussed. The question said "upload files", meaning multiple object. Isn't the encrypted bucked creation a securec way to store them in cloud storage?

upvoted 1 times

kip21 2 days, 19 hours ago

Selected Answer: A

[GSUtil]
check_hashes
content_language
decryption_key1 ... 100
default_api_version
disable_analytics_prompt
encryption_key

upvoted 1 times

deep316 1 week ago

Selected Answer: C

Option C: Use gsutil to upload the files and use the flag --encryption-key to supply the encryption key. This is the correct approach, as it allov you to specify the CSEK directly at the time of upload, ensuring that your files are encrypted using your provided key.

upvoted 1 times

klayytech 1 week, 3 days ago

Selected Answer: D

D. Use gsutil to create a bucket, and use the flag --encryption-key to supply the encryption key. Use gsutil to upload the files to that bucket.

This option provides the most comprehensive and secure approach:

Create an encrypted bucket:

Use gsutil mb -b location gs://your-bucket-name --encryption-key=your_encryption_key
This ensures that all objects uploaded to this bucket will be encrypted with your provided key.
Upload files to the encrypted bucket:

Use gsutil cp your_local_file gs://your-bucket-name
By following this approach, you guarantee that your files are encrypted both at rest and in transit on Cloud Storage, providing a robust securit posture.

The other options either lack the encryption key specification or do not create an encrypted bucket, leaving your data vulnerable.

upvoted 2 times

desertlotus1211 3 weeks, 2 days ago

Selected Answer: A

The boto configuration file in Google Cloud Platform (GCP) controls how the gsutil command behaves:

Setting up gsutil
You can use the boto configuration file to set up gsutil to work through a proxy.

Using encryption keys
You can use the boto configuration file to use customer-managed or customer-supplied encryption keys.

upvoted 1 times

desertlotus1211 3 weeks, 2 days ago

.boto is smoother to use consistently...

upvoted 1 times

icarogsm 3 weeks, 5 days ago

Selected Answer: A

A! I agree that the boto file sounds better

upvoted 1 times

46affda 4 weeks ago

Option C is correct - please refer https://cloud.google.com/storage/docs/encryption/using-customer-supplied-keys#command-line

upvoted 1 times

sim7243 1 month, 1 week ago

Selected Answer: A

option A,
Option A allows you to configure the .boto configuration file with the encryption key. This configuration file is used by gsutil to apply settings, including encryption key management. By placing the encryption key in the .boto file, you ensure that every time gsutil is used, it automaticall supplies the correct key for encrypting files as they are uploaded to Cloud Storage.

Option C: The --encryption-key flag does not exist for gsutil. Instead, gsutil uses the .boto configuration file or the -o flag for customer-supplie encryption keys.

upvoted 2 times

nareshthumma 1 month, 3 weeks ago

Answer: C

Use gsutil to upload the files, and use the flag -encryption-key to supply the encryption key.
Here’s why this is the best option:
1. Using gsutil: gsutil is the command-line tool for interacting with Google Cloud Storage, and it supports options for specifying customer-supplied encryption keys directly during the upload process.
2. Flag -encryption-key: The -encryption-key flag allows you to specify the encryption key at the time of uploading the files. This ensures that files are encrypted with the provided key as they are being uploaded to Cloud Storage.

upvoted 3 times

AlainBas 2 months, 2 weeks ago

A is correct

upvoted 1 times

dfizban 2 months, 2 weeks ago

Selected Answer: C

Option C is correct.

upvoted 2 times

3fd692e 2 months, 2 weeks ago

Selected Answer: C

Straight for the docs: https://cloud.google.com/storage/docs/encryption/using-customer-supplied-keys#upload-encrypt

upvoted 4 times

Upender_PDE 2 months, 3 weeks ago

Option C is correct
C. Use gsutil to upload the files, and use the flag --encryption-key to supply the encryption key.

```
gsutil -o "GSUtil:encryption_key=YOUR_BASE64_ENCRYPTION_KEY" cp your_file.txt gs://your-bucket/
```

upvoted 4 times

maxdanny 3 months, 1 week ago

Selected Answer: C

When using customer-supplied encryption keys (CSEK) in Google Cloud Storage, you can provide the encryption key directly in your gsutil command during the upload operation. The --encryption-key flag allows you to specify the encryption key for encrypting the files as they are uploaded.

upvoted 4 times

JohnJamesB1212 3 months, 1 week ago

Selected Answer: C

The correct answer is C. Use gsutil to upload the files, and use the flag --encryption-key to supply the encryption key.

Here's why:

To encrypt files with a customer-supplied encryption key (CSEK), you can use the gsutil command along with the --encryption-key flag to spe the encryption key when uploading files to Cloud Storage.
This allows each file to be encrypted using your specified encryption key, providing an additional layer of security beyond Google-managed encryption.
The other options are incorrect:

A and B reference .boto configuration files and gcloud config, but those methods are not used to specify customer-supplied encryption keys f file uploads.
D incorrectly suggests using --encryption-key when creating a bucket, but encryption keys are supplied during file uploads, not during bucket creation.
Thus, C is the correct option to upload files with customer-supplied encryption keys using gsutil.

upvoted 5 times

Question #66 *Topic 1*

Your customer wants to capture multiple GBs of aggregate real-time key performance indicators (KPIs) from their game servers running on Google Cloud Platform and monitor the KPIs with low latency. How should they capture the KPIs?

A. Store time-series data from the game servers in Google Bigtable, and view it using Google Data Studio.

B. Output custom metrics to Stackdriver from the game servers, and create a Dashboard in Stackdriver Monitoring Console to view them.

C. Schedule BigQuery load jobs to ingest analytics files uploaded to Cloud Storage every ten minutes, and visualize the results in Google Data Studio.

D. Insert the KPIs into Cloud Datastore entities, and run ad hoc analysis and visualizations of them in Cloud Datalab.

suryalsp Highly Voted 👍 4 years, 12 months ago

Ans is B. Data studio cannot be used with BigTable
https://datastudio.google.com/datahttps://datastudio.google.com/data

upvoted 33 times

Raja101 3 years, 3 months ago

A is correct

upvoted 4 times

ErenYeager 2 years, 1 month ago

As of today you can

upvoted 7 times

anshumankmr80 2 years ago

Source?

https://lookerstudio.google.com/data?search=big

upvoted 2 times

HD2023 1 year, 8 months ago

That’s BigQuery, not BigTable, no?

upvoted 2 times

jrisl1991 1 year, 1 month ago

Looker is not the same as Data Studio. I know it came to replace it, but these questions are kind of old, so unless it clearly says "looker", I wouldn't take both as the same.

upvoted 2 times

kolcsarzs Highly Voted 👍 5 years ago

correct is B

upvoted 12 times

nareshthumma Most Recent 🕘 1 month, 3 weeks ago

Answer is B

upvoted 1 times

belouh 1 month, 3 weeks ago

Selected Answer: B

Bigtable is not real time solution

upvoted 1 times

kip21 11 months, 1 week ago

B - Correct
A - It is not a real-time solution

upvoted 1 times

Saxena_Vibhor 10 months ago

Why is A not a real time solution? https://cloud.google.com/bigtable/docs/integrations#opentsdb

it says: OpenTSDB is a time-series database that can use Bigtable for storage. Monitoring time-series data with OpenTSDB on Bigtable ar GKE shows how to use OpenTSDB to collect, record, and monitor time-series data on Google Cloud. The OpenTSDB documentation provides additional information to help you get started.

upvoted 1 times

AdityaGupta 1 year, 2 months ago

Selected Answer: B

BigTable doesn't integrate with Data Studio

https://cloud.google.com/bigtable/docs/integrations

upvoted 1 times

LaxmanTiwari 1 year, 7 months ago

B is correct, you should create custom KPI in Stack Driver

upvoted 1 times

omermahgoub 1 year, 12 months ago

B. Output custom metrics to Stackdriver from the game servers, and create a Dashboard in Stackdriver Monitoring Console to view them.

To capture multiple GBs of aggregate real-time KPIs from game servers running on Google Cloud Platform and monitor them with low latency the customer should output custom metrics to Stackdriver from the game servers. Stackdriver allows you to collect and store custom metrics well as view and analyze them in real-time using the Stackdriver Monitoring Console. The customer can create a Dashboard in the Monitoring Console to view the KPIs and monitor them with low latency.

upvoted 9 times

omermahgoub 1 year, 12 months ago

Option A, storing time-series data in Bigtable and viewing it using Data Studio, would not be suitable for capturing and monitoring real-tim KPIs with low latency. Bigtable is a scalable NoSQL database that is optimized for large-scale batch processing, and Data Studio is a visualization tool that is not designed for real-time data analysis.

Option C, scheduling BigQuery load jobs to ingest analytics files uploaded to Cloud Storage every ten minutes and visualizing the results i Data Studio, would not be suitable for capturing and monitoring real-time KPIs with low latency. BigQuery is a data warehouse that is optimized for batch processing, and it is not designed for real-time data analysis.

Option D, inserting the KPIs into Cloud Datastore entities and running ad hoc analysis and visualizations of them in Cloud Datalab, would r be suitable for capturing and monitoring real-time KPIs with low latency. Cloud Datastore is a NoSQL document database, and Cloud Data is a data analysis and visualization tool that is not designed for real-time data analysis.

upvoted 9 times

jlambdan 1 year, 9 months ago

big table is not for batch. It is used in IOT...
https://cloud.google.com/bigtable

upvoted 4 times

Raja101 2 years, 1 month ago

Selected Answer: A

A is correct

upvoted 1 times

megumin 2 years, 1 month ago

Selected Answer: B

B is ok

upvoted 1 times

Mahmoud_E 2 years, 1 month ago

Selected Answer: B

B is correct as Data studio does not support bigtable as a source

upvoted 4 times

zr79 2 years, 2 months ago

KPI, SLO,SLI all those work with observability which stackdriver

upvoted 2 times

jay9114 2 years, 2 months ago

The reference provided seems irrelevant to this question.

upvoted 1 times

bolington 2 years, 6 months ago

A is the correct answer, the key word here, real time and low latency.

upvoted 1 times

Nirca 2 years, 7 months ago

Selected Answer: B

BigTable has no connection to data studio.
https://datastudio.google.com/data?search=Big

upvoted 6 times

BeetleJuice 2 years, 11 months ago

Selected Answer: B

B, it is

upvoted 2 times

OrangeTiger 2 years, 11 months ago

I don't think there is a correct answer, but B looks correct in this.
If use Bigquery, then A is correct .
C is not for realtime.
D Datastore is for small usecase.
Keywords 'real time' ,'analytics'
https://events.withgoogle.com/solution-design-pattern-gaming/analytics-pattern/

upvoted 2 times

Question #67 *Topic 1*

You have a Python web application with many dependencies that requires 0.1 CPU cores and 128 MB of memory to operate in production. You want to monitor and maximize machine utilization. You also want to reliably deploy new versions of the application. Which set of steps should you take?

A. Perform the following: 1. Create a managed instance group with f1-micro type machines. 2. Use a startup script to clone the repository, check out the production branch, install the dependencies, and start the Python app. 3. Restart the instances to automatically deploy new production releases.

B. Perform the following: 1. Create a managed instance group with n1-standard-1 type machines. 2. Build a Compute Engine image from the production branch that contains all of the dependencies and automatically starts the Python app. 3. Rebuild the Compute Engine image, and update the instance template to deploy new production releases.

C. Perform the following: 1. Create a Google Kubernetes Engine (GKE) cluster with n1-standard-1 type machines. 2. Build a Docker image from the production branch with all of the dependencies, and tag it with the version number. 3. Create a Kubernetes Deployment with the imagePullPolicy set to 'IfNotPresent' in the staging namespace, and then promote it to the production namespace after testing.

D. Perform the following: 1. Create a GKE cluster with n1-standard-4 type machines. 2. Build a Docker image from the master branch with all of the dependencies, and tag it with 'latest'. 3. Create a Kubernetes Deployment in the default namespace with the imagePullPolicy set to 'Always'. Restart the pods to automatically deploy new production releases.

jcmoranp Highly Voted 👍 5 years, 1 month ago

C is correct, need "ifnotpresent"when uploads to container registry

upvoted 41 times

medi01 1 year, 8 months ago

ifnotpresent won't pull new version.

upvoted 4 times

heretolearnazure 1 year, 3 months ago

yes i agree

upvoted 1 times

TosO Highly Voted 👍 5 years ago

C is the best choice. You can create a k8s cluster with just one node and use a different namespaces for staging and production. In staging, y will test the changes

upvoted 23 times

AzureDP900 2 years, 2 months ago

Agreed

upvoted 1 times

Gayathri1608 Most Recent 🕓 3 weeks, 1 day ago

Selected Answer: C

i think suitable for the given scenario

upvoted 1 times

nareshthumma 1 month, 3 weeks ago

Answer is C

upvoted 1 times

44fa527 3 months, 3 weeks ago

Selected Answer: C

should be option C because if you are working in real world, GKE is the best solution for such a case. Furthermore, its reliable, scalable, flexib at least the best option among the other three.

upvoted 1 times

cai_engineer 3 months, 4 weeks ago

Selected Answer: A

Ngl it's A. Don't use GKE, it won't schedule the deployment as most of the resources already occupied by kube-system

upvoted 1 times

cai_engineer 3 months, 4 weeks ago

Also you can deploy COS Containerd in a VM

upvoted 1 times

awsgcparch 4 months, 3 weeks ago

Selected Answer: D

imagePullPolicy: Always ensures that the latest version of the image is always pulled, which guarantees that the most recent code is deployec
Restarting pods ensures that the new version is deployed without requiring manual intervention.

upvoted 1 times

krokskan 9 months, 3 weeks ago

Selected Answer: B

B because Kubernetes will be overkill and A is not reliable

upvoted 1 times

Gall 10 months, 2 weeks ago

Selected Answer: C

A is wrong as after the restart the script will be rerun and fetch the code directly from the repo (even if production). The load of the massive number of dependencies will take a lot of timee, and the application version will be fuzzy.

upvoted 1 times

moumou 10 months, 4 weeks ago

C is correct, B (instance template cannote be updated once created.

upvoted 2 times

kip21 11 months, 1 week ago

C - Correct

upvoted 1 times

AWS_Sam 11 months, 2 weeks ago

The correct answer is C. Because it is the only option that RELIABLY tests the app in staging before it is applied to production. Remember tha one of the requirements in the question is to reliably deploy the app.

upvoted 2 times

Roro_Brother 1 year ago

Selected Answer: A

You don't need GKE for 0.1 CPU, only A meet hte needs

upvoted 3 times

MahAli 1 year ago

Selected Answer: A

For 0.1 CPU I will never use GKE, considering the associated cost with control plane and not even one option in the question mentioning mici instances for the node pool

upvoted 4 times

mastrrrr 1 year ago

Selected Answer: A

When we read the question - "0.1 CPU cores and 128 MB of memory" to operate in production. You want to monitor and "maximize machine utilization"... Answer A should be a fit based on the question details. Would GKE for tiny application be overkill?

upvoted 4 times

Arun_m_123 1 year, 2 months ago

Selected Answer: C

python app on compute engine is a disastrous architecture. C is the correct architecture which tests the app before putting to prod

upvoted 1 times

AdityaGupta 1 year, 2 months ago

Selected Answer: C

You should use GKE, because your can scale up and down based on your demand. Also you can specifiy the resource size like 0.1 CPU and MB of memory per Pod.

Secondly, Kubernetes Deployment with the imagePullPolicy set to “IfNotPresent” in the staging namespace, and then promote it to productio namespace after testing, is best practice.

Question #68 *Topic 1*

Your company wants to start using Google Cloud resources but wants to retain their on-premises Active Directory domain controller for identity management.
What should you do?

A. Use the Admin Directory API to authenticate against the Active Directory domain controller.

B. Use Google Cloud Directory Sync to synchronize Active Directory usernames with cloud identities and configure SAML SSO.

C. Use Cloud Identity-Aware Proxy configured to use the on-premises Active Directory domain controller as an identity provider.

D. Use Compute Engine to create an Active Directory (AD) domain controller that is a replica of the on-premises AD domain controller using Google Cloud Directory Sync.

KouShikyou Highly Voted 5 years, 2 months ago

According to the reference, my understanding is B is correct.
And in the document(https://cloud.google.com/iap/docs/concepts-overview), it says:
If you need to create Google Accounts for your existing users, you can use Google Cloud Directory Sync to synchronize with your Active Directory or LDAP server.

Is it possible to explain why correct answer is C?

upvoted 44 times

MikeB19 3 years, 3 months ago

It’s simple. Domain controllers are not meant authenticate saas or web applications. This includes iam. Domain controllers speak ntlm and Kerberos.
This why we use federation. Because web apps do not speak Kerberos or ntlm. They speak languages such oauth. Hence the need for ad federation proxy
B is correct

upvoted 5 times

Bill831231 3 years, 2 months ago

thanks for the explanation, may I ask if we go with SAML, why need sync the useraccount? seems we just need set up the federation between cloud and on-premise

upvoted 2 times

Ekramy_Elnaggar 1 month ago

if not, you will not be able to access resources on GCP with same accounts as onprem.

upvoted 1 times

BiddlyBdoyng 2 years, 2 months ago

"...As a prerequisite for access to GCP resources, employees must have a Google identity set up..."

upvoted 4 times

tartar 4 years, 4 months ago

B is ok

upvoted 9 times

kumarp6 4 years, 1 month ago

B should be correct

upvoted 5 times

nitinz 3 years, 9 months ago

B, use GCDS.

upvoted 5 times

MeasService Highly Voted 5 years, 1 month ago

B is the nearest answer I feel !

upvoted 25 times

eff12c1 Most Recent 6 months, 2 weeks ago

Selected Answer: B

To integrate Google Cloud with your on-premises Active Directory (AD) domain controller for identity management while retaining your on-premises AD, the best approach is:

B. Use Google Cloud Directory Sync to synchronize Active Directory usernames with cloud identities and configure SAML SSO.

upvoted 1 times

svkds 7 months, 2 weeks ago

Selected Answer: D

The most suitable option for integrating Google Cloud resources with an on-premises Active Directory domain controller for identity managem is option D. This involves creating a replica of the on-premises Active Directory domain controller using Compute Engine and Google Cloud Directory Sync for synchronization.

upvoted 1 times

LaxmanTiwari 1 year, 7 months ago

B is correct https://cloud.google.com/architecture/identity/federating-gcp-with-active-directory-introduction

upvoted 2 times

vamgcp 1 year, 10 months ago

Connect your on-premises Active Directory to Google Cloud: You can use Google Cloud Directory Sync (GCDS) to synchronize your on-prem Active Directory with Google Cloud. This allows you to use your existing Active Directory users and groups in Google Cloud.

Set up single sign-on (SSO): You can use Google Cloud Identity-Aware Proxy (IAP) to set up SSO for your Google Cloud resources. IAP integrates with your on-premises Active Directory and allows users to log in to Google Cloud using their existing Active Directory credentials.

upvoted 2 times

omermahgoub 1 year, 12 months ago

B. Use Google Cloud Directory Sync to synchronize Active Directory usernames with cloud identities and configure SAML SSO.

To retain their on-premises Active Directory domain controller for identity management while using Google Cloud resources, the company car use Google Cloud Directory Sync to synchronize Active Directory usernames with cloud identities and configure SAML single sign-on (SSO). will allow users to use their existing Active Directory credentials to access Google Cloud resources, while still maintaining their on-premises Active Directory domain controller as the primary source of identity management.

upvoted 7 times

omermahgoub 1 year, 12 months ago

Option A, using the Admin Directory API to authenticate against the Active Directory domain controller, would not be a suitable solution because it would require implementing custom authentication logic in the application, which would be time-consuming and error-prone.

Option C, using Cloud Identity-Aware Proxy configured to use the on-premises Active Directory domain controller as an identity provider, would be a suitable solution, but it would not allow you to synchronize Active Directory usernames with cloud identities.

Option D, using Compute Engine to create an Active Directory (AD) domain controller that is a replica of the on-premises AD domain contr using Google Cloud Directory Sync, would not be a suitable solution because it would require setting up and maintaining an additional AD domain controller in Google Cloud, which would be unnecessary if the company wants to retain their on-premises AD domain controller as primary source of identity management.

upvoted 3 times

SureshbabuK 2 years ago

Selected Answer: B

GCDS and Cloud Identity is provided exactly for this use case

upvoted 1 times

megumin 2 years, 1 month ago

Selected Answer: B

B is ok

upvoted 2 times

Mahmoud_E 2 years, 1 month ago

Selected Answer: B

B is correct https://cloud.google.com/architecture/identity/federating-gcp-with-active-directory-introduction

upvoted 2 times

cbarg 2 years, 5 months ago

Selected Answer: B

Answer is B

upvoted 1 times

SAMBIT 2 years, 9 months ago

https://support.google.com/a/answer/106368?hl=en

upvoted 1 times

haroldbenites 3 years ago

Go for B.
Cloud Directory Sync
https://cloud.google.com/blog/products/identity-security/using-your-existing-identity-management-system-with-google-cloud-platform

upvoted 4 times

vincy2202 3 years ago

B is the correct answer

upvoted 1 times

pulkit0627 3 years ago

B as AD groups are directly mapped to Cloud Directory Sync

upvoted 1 times

MaxNRG 3 years, 1 month ago

B – use Google Cloud Directory Sync to sync Active Directory user names with cloud identities and configure SAML SSO.
Check the flowchart here illustrating integration of your existing identity management system into GCP:
https://cloud.google.com/blog/products/identity-security/using-your-existing-identity-management-system-with-google-cloud-platform
C – does not work, since Cloud IAP serves different purpose. It s a building block toward BeyondCorp, an enterprise security model that enab
every employee to work from untrusted networks without the use of a VPN.

upvoted 2 times

MamthaSJ 3 years, 5 months ago

Answer is B

upvoted 4 times

Question #69 *Topic 1*

You are running a cluster on Kubernetes Engine (GKE) to serve a web application. Users are reporting that a specific part of the application is not responding anymore. You notice that all pods of your deployment keep restarting after 2 seconds. The application writes logs to standard output. You want to inspect the logs to find the cause of the issue. Which approach can you take?

A. Review the Stackdriver logs for each Compute Engine instance that is serving as a node in the cluster.

B. Review the Stackdriver logs for the specific GKE container that is serving the unresponsive part of the application.

C. Connect to the cluster using gcloud credentials and connect to a container in one of the pods to read the logs.

D. Review the Serial Port logs for each Compute Engine instance that is serving as a node in the cluster.

jcmoranp Highly Voted 4 years, 1 month ago

think answer is B. C cannot be, you don't need to connect to the container to view logs, you connect to stackdriver for this

upvoted 34 times

nitinz 2 years, 9 months ago

B, google wants you to use stackdriver.

upvoted 6 times

crypt0 4 years, 1 month ago

Stackdriver Logging seems to be enabled by default for GKE.

Looking here:
https://cloud.google.com/monitoring/kubernetes-engine/legacy-stackdriver/logging
For container and system logs, GKE deploys a per-node logging agent that reads container logs, adds helpful metadata, and then stores them. The logging agent checks for container logs in the following sources:

Standard output and standard error logs from containerized processes

I would also go with B

upvoted 10 times

AzureDP900 1 year, 2 months ago

agreed with B

upvoted 1 times

kumarp6 3 years, 1 month ago

Yes it is B

upvoted 3 times

crypt0 4 years, 1 month ago

Is Stackdriver enabled by default?
Stackdriver Logging is independent and first needs to enable with GKE I guess?

upvoted 1 times

crypt0 4 years, 1 month ago

Please forget this comment ^
Answer B should be correct.

upvoted 8 times

tartar 3 years, 4 months ago

B is ok

upvoted 7 times

Jack_in_Large 3 years, 7 months ago

Yes for GKE

upvoted 1 times

JoeShmoe Highly Voted 4 years, 1 month ago

B is correct. Serial console doesnt give you StdOut

upvoted 9 times

AdityaGupta Most Recent 2 months, 2 weeks ago

B. Review the Stackdriver logs for the specific GKE container that is serving the unresponsive part of the application.

GKE be default integrats with Google Operation Suit (Stackdriver) and you can filter the logs for more specific part of application i.e container view logs. Also it is most efficient way of investigation.

upvoted 1 times

jalberto 4 months ago

Selected Answer: B

B is the simples option and more effective

upvoted 1 times

MestreCholas 9 months, 2 weeks ago

Selected Answer: B

B. Review the Stackdriver logs for the specific GKE container that is serving the unresponsive part of the application.

Since the application writes logs to standard output, the logs should be available in the Stackdriver logs for the container running the unresponsive part of the application. Kubernetes Engine automatically exports these logs to Stackdriver, so you can use the Stackdriver Logg console to view the logs. Option A is not the best choice because reviewing the logs for each Compute Engine instance would be time-consuming and may not provide the necessary information. Option C may work, but it involves extra steps and may not be necessary if the lo are available in Stackdriver. Option D is not relevant in this case because Serial Port logs are not likely to provide useful information for troubleshooting an unresponsive web application.

upvoted 1 times

omermahgoub 12 months ago

C. Connect to the cluster using gcloud credentials and connect to a container in one of the pods to read the logs.

To inspect the logs of a Kubernetes Engine (GKE) cluster to find the cause of an issue, you can connect to the cluster using gcloud credential and connect to a container in one of the pods to read the logs. This will allow you to access the logs of the application as it is running in the cluster, which should help you identify the cause of the issue.

upvoted 2 times

omermahgoub 12 months ago

Option A, reviewing the Stackdriver logs for each Compute Engine instance that is serving as a node in the cluster, would not be suitable because the application writes logs to standard output, not to Stackdriver.

Option B, reviewing the Stackdriver logs for the specific GKE container that is serving the unresponsive part of the application, would not b suitable because the application writes logs to standard output, not to Stackdriver.

Option D, reviewing the Serial Port logs for each Compute Engine instance that is serving as a node in the cluster, would not be suitable because the application writes logs to standard output, not to the Serial Port.

upvoted 3 times

jaxclain 1 year ago

Selected Answer: B

This should be easy, the answer is B.
Just eliminate the wrong answers (A) is not correct because the question is about GKE and not CE.
C and D are totally lost

upvoted 1 times

habros 1 year ago

Selected Answer: B

A, C, D all sounds unfeasible (credentials, and compute engine)

upvoted 1 times

megumin 1 year, 1 month ago

Selected Answer: B

B is ok

upvoted 1 times

Mahmoud_E 1 year, 1 month ago

Selected Answer: B

is correct answer

upvoted 1 times

Superr 1 year, 6 months ago

Selected Answer: B

correct

upvoted 1 times

OrangeTiger 1 year, 11 months ago

B is correct ans.I agree.
https://cloud.google.com/blog/ja/products/management-tools/finding-your-gke-logs

upvoted 2 times

haroldbenites 2 years ago

Go for B

upvoted 1 times

vincy2202 2 years ago

B is the correct answer

upvoted 1 times

MaxNRG 2 years, 1 month ago

B – Review Stackdriver logs for specific GKE container that is serving the unresponsive part of the app.
This is a most directly matching answer for this Q, since it reviews GKE container logs, by that advertising this Stackdriver feature.
“For container and system logs, GKE deploys a per-node logging agent that reads container logs, adds helpful metadata, and then stores the
The logging agent checks for container logs in the following sources:
• Standard output and standard error logs from containerized processes
• kubelet and container runtime logs
• Logs for system components, such as VM startup scripts”
Originally we thought, that D is a right answer, since were confused with 2 seconds restart. But, that’s restart for Pod, not for Node (GCE)
D – Review Serial Port logs for each Compute Engince instance, that is serving as the in the cluster.
Serial Port output is standard feature of Compute Engine (which retains 1 MB most recent logs for analysis). But, it is irrelevant for Pod’s resta
caused by malfunction of some container.

upvoted 3 times

MamthaSJ 2 years, 5 months ago

Answer is B

upvoted 3 times

lovingsmart2000 2 years, 5 months ago

B is right answer. There is a catch here - Legacy logging of GKE with Stackdriver has deprecated. If this is used, you need to migrate to Clouc
Operations for GKE, a new enhanced offering by Google with same functionality.
Future questions will have the answer choices with new tool "Cloud Operations for GKE" instead of Stackdriver.
https://cloud.google.com/monitoring/kubernetes-engine/legacy-stackdriver/logging

upvoted 2 times

Question #70 *Topic 1*

You are using a single Cloud SQL instance to serve your application from a specific zone. You want to introduce high availability. What should you do?

A. Create a read replica instance in a different region

B. Create a failover replica instance in a different region

C. Create a read replica instance in the same region, but in a different zone

D. Create a failover replica instance in the same region, but in a different zone

AWS56 Highly Voted 4 years, 11 months ago

Agree D

upvoted 36 times

tartar 4 years, 4 months ago

D is ok

upvoted 7 times

kumarp6 4 years, 1 month ago

Yes D is right

upvoted 4 times

kimharsh 2 years, 6 months ago

this Question is very Old and should be deleted from the exam , there is no Failover replica now , to do an HA we just confer it for the SQL instance that we have .

upvoted 25 times

nwk 2 years, 6 months ago

https://cloud.google.com/sql/docs/mysql/replication#:~:text=Read%20replicas%20neither%20provide%20high%20availability%20nor%2
fer%20it.&text=A%20primary%20instance%20cannot%20failover,any%20way%20during%20an%20outage.&text=Maintenance%20winc
s%20cannot%20be%20set,windows%20with%20the%20primary%20instance.

- Read replicas neither provide high availability nor offer it.

Agree D

upvoted 7 times

jay9114 2 years, 3 months ago

That link is helpful! I navigated to the "quick reference for Cloud SQL read replicas" and read the "failover" and "high availability" topics
They state:
1. Failover - "A primary instance cannot failover to a read replica, and read replicas are unable to failover in any way during an outage."
2. High Availability - "Read replicas neither provide high availability nor offer it."

upvoted 2 times

spuyol 10 months, 3 weeks ago

Sorry for this, but in the same link you can read:
High availability Read replicas allow you to enable high availability on the replicas.

(What I understand is that Read Replicas give you high availability on reads, of course, not in writes).

upvoted 1 times

GunjGupta Highly Voted 4 years, 7 months ago

Cloud SQL is regional. For high availability, we need to think fo a failover strategy. So Option D meets the requirement.
create failover replica in the same region but in different Zone

upvoted 17 times

Lenifia Most Recent 1 month, 3 weeks ago

Selected Answer: C

C is the correct answer, failover is more like DR

upvoted 1 times

nareshthumma 1 month, 3 weeks ago

Answer is D:
Create a failover replica instance in the same region, but in a different zone.

Here’s why this option is the best:

1. High Availability: A failover replica provides automatic failover capabilities, meaning that if the primary instance becomes unavailable (due t zone failure, for example), Cloud SQL can automatically promote the failover replica to be the new primary instance, minimizing downtime.

2. Same Region, Different Zone: By creating the failover replica in the same region but a different zone, you ensure that the instances are geographically close to each other, which helps maintain low latency and faster failover times while still protecting against zone-specific outag

3. Cost Efficiency: Using a failover replica in the same region is typically more cost-effective than setting up a replica in a different region, as cross-region replication can introduce additional latency and costs.

upvoted 1 times

hehe_24 1 month, 4 weeks ago

C is incorrect. D is the right answer. Read-replica is just an instance for read operation, it cannot provide HA.

upvoted 1 times

0verK0alafied 7 months, 4 weeks ago

Selected Answer: D

The HA configuration provides data redundancy. A Cloud SQL instance configured for HA is also called a regional instance and has a primary secondary zone within the configured region. Within a regional instance, the configuration is made up of a primary instance and a standby instance. Through synchronous replication to each zone's persistent disk, all writes made to the primary instance are replicated to disks in bo zones before a transaction is reported as committed. In the event of an instance or zone failure, the standby instance becomes the new prima instance. Users are then rerouted to the new primary instance. This process is called a failover.
https://cloud.google.com/sql/docs/mysql/high-availability#HA-configuration

upvoted 3 times

Gall 10 months, 2 weeks ago

Selected Answer: D

"Note: Read replicas do not provide failover capability. To provide failover capability for an instance, see Configuring an instance for high availability."
https://cloud.google.com/sql/docs/mysql/replication/

upvoted 2 times

parthkulkarni998 1 year ago

Selected Answer: D

Correct answer would be D as a failover replica acts as a redundant copy incase of zone failure. However, option C causes confusion becaus read replica can provide availability for reads, in case of zone failure for primary, but they cant provide support for writes. They would only wo for reads.

upvoted 1 times

Roro_Brother 1 year ago

Selected Answer: D

D, its regional product and failover is required for HA

upvoted 1 times

thewalker 1 year, 1 month ago

C
1. Failover replica is a legacy way and is not available in GCP now - B and D are not the options: https://cloud.google.com/sql/docs/mysql/hi availability#legacy_mysql_high_availability_option
2. Cloud SQL is regional resource. However, cross-region read replicas are allowed now in Cloud SQL (https://cloud.google.com/blog/products/databases/introducing-cross-region-replica-for-cloud-sql) - A and C are options.
Chosen C, as there is no requirement or mention of cross-regional / global db.

upvoted 1 times

hogtrough 11 months, 2 weeks ago

Read replica is not a valid choice for HA configurations. It does not provide automatic failover that is required for HA. It may be called something different or this answer has changed, but D is still the best option.

upvoted 1 times

piiizu 1 year, 2 months ago

The key is High Availability, not Resilience or Disaster Recovery. Therefore my answer is C

upvoted 1 times

someone2011 1 year, 3 months ago

D.
In HA config, the second replica is caled stand by. The process of replacing the primary damaged node is called failover.
https://cloud.google.com/sql/docs/postgres/high-availability

upvoted 2 times

didek1986 1 year, 3 months ago

Selected Answer: C

C for sure

upvoted 1 times

red_panda 1 year, 6 months ago

Selected Answer: C

C.
Failover is so old and deprecated

upvoted 4 times

LaxmanTiwari 1 year, 7 months ago

this Question is very Old and should be deleted from the exam , there is no Failover replica now , to do an HA we just confer it for the SQL instance that we have .. agreed tested as well

upvoted 1 times

JC0926 1 year, 8 months ago

Selected Answer: D

Option C is not the best choice because it suggests creating a read replica instance, which is designed to handle read traffic and provide bett performance in read-heavy workloads, but it is not intended for high availability.

On the other hand, Option D suggests creating a failover replica instance in the same region but in a different zone. Failover replicas are desig specifically for high availability, as they maintain an up-to-date copy of the primary instance's data. If the primary instance becomes unrespon or fails, Cloud SQL automatically switches to the failover replica with minimal downtime.

In summary, to introduce high availability for your Cloud SQL instance, you should create a failover replica instance in the same region but in a different zone (Option D) rather than creating a read replica instance (Option C), which doesn't provide high availability in case of primary insta failures.

upvoted 4 times

DevOpsifier 1 year, 6 months ago

thanks!

upvoted 1 times

JC0926 1 year, 9 months ago

Selected Answer: D

D
C is also not ideal for high availability because creating a read replica in the same region but in a different zone does not provide automatic failover. A read replica is used for scaling reads and can improve performance, but it is not a failover mechanism.

upvoted 1 times

Question #71 *Topic 1*

Your company is running a stateless application on a Compute Engine instance. The application is used heavily during regular business hours and lightly outside of business hours. Users are reporting that the application is slow during peak hours. You need to optimize the application's performance. What should you do?

A. Create a snapshot of the existing disk. Create an instance template from the snapshot. Create an autoscaled managed instance group from the instance template.

B. Create a snapshot of the existing disk. Create a custom image from the snapshot. Create an autoscaled managed instance group from the custom image.

C. Create a custom image from the existing disk. Create an instance template from the custom image. Create an autoscaled managed instance group from the instance template.

D. Create an instance template from the existing disk. Create a custom image from the instance template. Create an autoscaled managed instance group from the custom image.

sdsdfasdf4 Highly Voted 3 years, 12 months ago

The easiest way would be to create template from --source-instance, and then create MIG, but it is not listed here, also you cannot create a M from image directly, you need a template, so answer is C (image -> template -> mig).

upvoted 30 times

6721sora 2 years, 3 months ago

C is correct.
To sdsdfasd4's point - Not recommended to create template from --source-instance as If the existing instance contains a static external IF address, that address is copied into the instance template and might limit the use of the template.
Templates are best created from images or other templates. Creating the template from a running instance may require work to clean it up before it can be used for a MIG

upvoted 8 times

AWS56 Highly Voted 4 years, 11 months ago

C is the right answer

upvoted 12 times

heretolearnazure 1 year, 3 months ago

C is definitely the right answer

upvoted 1 times

nareshthumma Most Recent 1 month, 3 weeks ago

Answer A:

Create a snapshot of the existing disk. Create an instance template from the snapshot. Create an autoscaled managed instance group from tl instance template.

Here's why this option is the best:

1. Autoscaling: By creating an autoscaled managed instance group, you can automatically adjust the number of instances based on the load. This means that during peak business hours, additional instances will be created to handle the increased traffic, improving application performance. During off-peak hours, the number of instances can scale down to reduce costs.

2. Snapshot Creation: Taking a snapshot of the existing disk ensures that you have a backup of the current state of your application. This snapshot can be used to create the new instance template, ensuring that your autoscaled instances have the same configuration as the origir instance.

upvoted 1 times

46f094c 5 months, 3 weeks ago

Selected Answer: B

I prefer B, is better because I don't need to stop the instance to create the disk image.

upvoted 1 times

pakilodi 1 year ago

Selected Answer: C

C. The key here is stateless, so we don't need snapshot the actual instance, we can start from zero.

upvoted 3 times

thewalker 1 year ago

Selected Answer: C

C
We can create an instance from an image or a custom image or a snapshot but an instance template can be created using either image or custom image only.

Also refer: https://cloud.google.com/compute/docs/instance-templates/create-instance-templates

upvoted 3 times

Deb2293 1 year, 9 months ago

Selected Answer: C

Option C is the correct choice because creating a custom image from the existing disk ensures that the application environment is consistent does not change between instances, which can reduce variability in performance. Creating an instance template from the custom image allow you to easily create new instances that are based on the same image, which can save time and effort. Finally, creating an autoscaled manage instance group allows you to automatically scale the number of instances based on demand, which can ensure that there are enough instanc to handle peak traffic while minimizing costs during periods of low traffic

upvoted 6 times

megumin 2 years, 1 month ago

Selected Answer: C

C is ok

upvoted 2 times

AzureDP900 2 years, 2 months ago

C is right.
Create a custom image from the existing disk. Create an instance template from the custom image. Create an autoscaled managed instance group from the instance template.

upvoted 1 times

abirroy 2 years, 3 months ago

Selected Answer: C

C is correct

upvoted 1 times

mv2000 2 years, 5 months ago

06/30/2022 Exam

upvoted 9 times

SHalgatti 2 years, 10 months ago

I think Snapshot option are not correct in this scenario as to take snapshot you need to stop the VM so C looks best option

upvoted 2 times

> **bargou** 10 months, 3 weeks ago
>
> it's possible to create a snapshot of running VM by reducing I/O disks
>
> upvoted 1 times

PhuocT 2 years, 11 months ago

Selected Answer: C

C is the answer

upvoted 1 times

Rajasa 2 years, 11 months ago

Selected Answer: C

C is the answer

upvoted 1 times

haroldbenites 3 years ago

Go for C.
Instance template can not be created from snapshot. Only from an image.

upvoted 3 times

vincy2202 3 years ago

C is the right answer.
https://cloud.google.com/compute/docs/instance-templates/create-instance-templates#using_custom_or_public_images_in_your_instance_templates

upvoted 3 times

joe2211 3 years ago

Selected Answer: C

vote C

upvoted 1 times

Question #72 *Topic 1*

Your web application has several VM instances running within a VPC. You want to restrict communications between instances to only the paths and ports you authorize, but you don't want to rely on static IP addresses or subnets because the app can autoscale. How should you restrict communications?

A. Use separate VPCs to restrict traffic

B. Use firewall rules based on network tags attached to the compute instances

C. Use Cloud DNS and only allow connections from authorized hostnames

D. Use service accounts and configure the web application to authorize particular service accounts to have access

AWS56 Highly Voted 3 years, 5 months ago

Agree B

upvoted 24 times

kumarp6 2 years, 7 months ago

Yes B it is

upvoted 2 times

nitinz 2 years, 3 months ago

B is correct

upvoted 2 times

omermahgoub Highly Voted 6 months ago

B. Use firewall rules based on network tags attached to the compute instances

To restrict communications between VM instances within a VPC without relying on static IP addresses or subnets, you can use firewall rules based on network tags attached to the compute instances. This will allow you to specify which instances are allowed to communicate with ea other and on which paths and ports. You can then attach the relevant network tags to the compute instances when they are created, allowing to control communication between the instances without relying on static IP addresses or subnets.

upvoted 11 times

omermahgoub 6 months ago

Option A, using separate VPCs to restrict traffic, would not be a suitable solution because it would not allow the instances to communicate with each other, which is likely necessary for the functioning of the web application.

Option C, using Cloud DNS and only allowing connections from authorized hostnames, would not be a suitable solution because it would r allow you to control communication between the instances based on their IP addresses or other characteristics.

Option D, using service accounts and configuring the web application to authorize particular service accounts to have access, would not b suitable solution because it would not allow you to control communication between the instances based on their IP addresses or other characteristics.

upvoted 4 times