

Question #51

Topic 1

You have found an error in your App Engine application caused by missing Cloud Datastore indexes. You have created a YAML file with the required indexes and want to deploy these new indexes to Cloud Datastore. What should you do?

- A. Point gcloud datastore create-indexes to your configuration file
- B. Upload the configuration file to App Engine's default Cloud Storage bucket, and have App Engine detect the new indexes
- C. In the GCP Console, use Datastore Admin to delete the current indexes and upload the new configuration file
- D. Create an HTTP request to the built-in python module to send the index configuration file to your application

🗲️ 👤 **jcmoranp** Highly Voted 👍 5 years, 1 month ago

Correct A, you have to recreate the indexes
upvoted 30 times

🗲️ 👤 **nitinz** 3 years, 9 months ago

A, if index is missing then create it.
upvoted 4 times

🗲️ 👤 **tartar** 4 years, 4 months ago

A is ok
upvoted 11 times

🗲️ 👤 **kumarp6** 4 years, 1 month ago

Yes, use this command in cloud shell to create indexes.
gcloud datastore create indexes
upvoted 4 times

🗲️ 👤 **Eroc** Highly Voted 👍 5 years, 1 month ago

A is incorrect because the command is actually gcloud datastore indexes create.
(<https://cloud.google.com/sdk/gcloud/reference/datastore/indexes/create>).
upvoted 17 times

🗲️ 👤 **bogd** 3 years, 10 months ago

It might have changed recently - I was able to find documentation mentioning "datastore create-indexes":

<https://cloud.google.com/appengine/docs/standard/python/datastore/indexes>
upvoted 15 times

🗲️ 👤 **sim7243** Most Recent 🕒 1 month, 1 week ago

Selected Answer: A

A, option
upvoted 1 times

🗨️ **james2033** 6 months, 3 weeks ago

Selected Answer: A

To deploy new Cloud Datastore indexes using the YAML file you created, you should use the `gcloud` command-line tool. Specifically, the correct option is:

****A. Point gcloud datastore create-indexes to your configuration file****

Here's how you can do it:

1. ****Ensure you have the `gcloud` CLI installed****: You need the Google Cloud SDK installed and set up on your local machine. If you haven't done this yet, follow the [installation guide](https://cloud.google.com/sdk/docs/install).
2. ****Navigate to the directory containing your `index.yaml` file****: This file contains the definitions of the indexes you want to deploy.
3. ****Run the following command****:

```
bash
gcloud datastore indexes create index.yaml
```

This command will deploy the indexes defined in the `index.yaml` file to Cloud Datastore.

upvoted 1 times

🗨️ **thewalker** 1 year, 1 month ago

A is correct: <https://cloud.google.com/sdk/gcloud/reference/datastore/indexes/create>

upvoted 3 times

🗨️ **jlambdan** 1 year, 9 months ago

A)

https://cloud.google.com/datastore/docs/tools/indexconfig#Datastore_Updating_indexes

upvoted 2 times

🗨️ **MestreCholas** 1 year, 9 months ago

Selected Answer: A

A. Point gcloud datastore create-indexes to your configuration file.

To deploy new indexes to Cloud Datastore, you can use the `gcloud datastore create-indexes` command and point it to the YAML configuration file containing the required indexes. This command will create the new indexes in Cloud Datastore for your application.

Option B is not correct because App Engine does not automatically detect and create indexes from uploaded configuration files in Cloud Storage.

Option C is also not correct because deleting current indexes in Datastore Admin is not necessary to upload new indexes.

Option D is not correct because there is no built-in Python module that can send the index configuration file to your application

upvoted 11 times

🗨️ **omermahgoub** 1 year, 12 months ago

To deploy new indexes to Cloud Datastore, you should use the `gcloud datastore create-indexes` command and point it to your configuration file. The correct option is therefore A: Point gcloud datastore create-indexes to your configuration file.

Here's the general format of the `gcloud datastore create-indexes` command:

Copy code

```
gcloud datastore create-indexes [FILE]
```

Where [FILE] is the path to your configuration file. The configuration file should be in YAML format and contain a list of indexes that you want to create.

For example:

Copy code

```
gcloud datastore create-indexes index.yaml
```

This command will create the indexes specified in the `index.yaml` file in Cloud Datastore.

upvoted 6 times

🗨️ **megumin** 2 years, 1 month ago

Selected Answer: A

ok for A

upvoted 1 times

🗨️ **Mahmoud_E** 2 years, 1 month ago

Selected Answer: A

A is correct answer
upvoted 1 times

🗨️ **AzureDP900** 2 years, 2 months ago

A is correct
upvoted 1 times

🗨️ **minmin2020** 2 years, 2 months ago

Selected Answer: A

gcloud app deploy index.yaml
upvoted 2 times

🗨️ **AMEJack** 2 years, 2 months ago

Answer is A.
Option C: no create index from configuration file in the firestore console.
upvoted 1 times

🗨️ **Najmuddoja** 2 years, 2 months ago

Is A still the valid answer, many other website resources saying C is the right answer
upvoted 1 times

🗨️ **holerina** 2 years, 2 months ago

A looks like more logical answer
upvoted 1 times

🗨️ **[Removed]** 2 years, 8 months ago

A is incorrect.
There is no correct answer, in fact. In 2022, the gcloud parameter "create-index" doesn't exist anymore. However, that was in 2017*. Today, the right CLI command** should be gcloud datastore "indexes create".

Evidences:

* <https://stackoverflow.com/questions/43041126/how-to-create-datastore-composite-indexes-with-just-cloud-functions>)

** <https://cloud.google.com/sdk/gcloud/reference/datastore/indexes/create>

upvoted 7 times

🗨️ **vincy2202** 2 years, 11 months ago

Selected Answer: A

A is the correct answer
upvoted 1 times

Question #52

Topic 1

You have an application that will run on Compute Engine. You need to design an architecture that takes into account a disaster recovery plan that requires your application to fail over to another region in case of a regional outage. What should you do?



- A. Deploy the application on two Compute Engine instances in the same project but in a different region. Use the first instance to serve traffic, and use the HTTP load balancing service to fail over to the standby instance in case of a disaster.
- B. Deploy the application on a Compute Engine instance. Use the instance to serve traffic, and use the HTTP load balancing service to fail over to an instance on your premises in case of a disaster.
- C. Deploy the application on two Compute Engine instance groups, each in the same project but in a different region. Use the first instance group to serve traffic, and use the HTTP load balancing service to fail over to the standby instance group in case of a disaster.
- D. Deploy the application on two Compute Engine instance groups, each in a separate project and a different region. Use the first instance group to serve traffic, and use the HTTP load balancing service to fail over to the standby instance group in case of a disaster.

🗨️ **Eroc** **Highly Voted** 👍 4 years, 7 months ago

Groups are better for management than non-groups so A and B are eliminated. Keeping the instances in the same project will help maintain

consistency, so C is better than D.

upvoted 37 times

  **nitinz** 3 years, 3 months ago

C, because external LB needs **IG** period. It can either be managed or un-managed. You can not do External HTTP LB on instances. Also External HTTP LB is a Regional resource.

upvoted 14 times

  **LaxmanTiwari** 1 year ago

make sense.

upvoted 1 times

  **gigibit**  2 years, 9 months ago

Yes, but why not choose a cost-effective solution like A, preferring a not required performance optimization solution like C? The question it's asking for a simple fail over

upvoted 13 times

  **Terryhsieh** 5 months, 3 weeks ago

Use two groups, each group contain one instance would be more flexible than answer A.

upvoted 2 times

  **hellosam** 10 months, 3 weeks ago

LB does not work without MIG

upvoted 4 times

  **todos213** 2 years, 2 months ago

In real word situation, I'd choose A for a customer. The question doesn't mention performance to be enhanced or scalability.

upvoted 6 times

  **yilexar**  8 months, 1 week ago


Now you can use regional load balancer to route traffic to instance groups in different GCP projects. Welcome to cloud :-)
<https://cloud.google.com/blog/products/networking/cloud-load-balancing-gets-cross-project-service-referencing>

upvoted 4 times

  **heretolearnazure** 10 months ago

C is correct

upvoted 1 times

  **BeCalm** 1 year, 3 months ago

To set up a load balancer with a Compute Engine backend, your VMs need to be in an instance group. The managed instance group provides VMs running the backend servers of an external HTTP load balancer



Therefore C

upvoted 5 times

  **LaxmanTiwari** 1 year ago

good catch .

upvoted 2 times

  **BeCalm** 1 year, 3 months ago



Why can't this be A since there is no mention of scaling?

upvoted 1 times

  **hellosam** 10 months, 3 weeks ago

LB does not work without MIG

upvoted 1 times

  **axle818** 6 months, 2 weeks ago

You can use either MIG or unmanaged..

<https://cloud.google.com/compute/docs/instance-groups/creating-groups-of-unmanaged-instances>

upvoted 2 times

🗨️ **n_nana** 1 year, 5 months ago

Selected Answer: C

Google recommend using MIG for Zonal outage and multiple MIG for regional outage
<https://cloud.google.com/architecture/disaster-recovery#compute-engine>
 sentence says:

Compute Engine instances are zonal resources, so in the event of a zone outage instances are unavailable by default. Compute Engine does offer managed instance groups (MIGs) which can automatically scale up additional VMs from pre-configured instance templates, both within a single zone and across multiple zones within a region. MIGs are ideal for applications that require resilience to zone loss and are stateless, but require configuration and resource planning. Multiple regional MIGs can be used to achieve region outage resilience for stateless applications.

upvoted 8 times

🗨️ **roaming_panda** 1 year, 5 months ago

Selected Answer: C

MIG , in 1 project

upvoted 1 times

🗨️ **sameer2803** 1 year, 5 months ago

the only solution that they want is to address regional outage. scalability or performance is not a concern at this point. MIG is better but that's what is solving the regional outage.

upvoted 1 times

🗨️ **n_nana** 1 year, 5 months ago

According to this link, MIG is not only for performance and scalability. It is also for reliability
<https://cloud.google.com/architecture/disaster-recovery#compute-engine>
 sentence says:

Compute Engine instances are zonal resources, so in the event of a zone outage instances are unavailable by default. Compute Engine does offer managed instance groups (MIGs) which can automatically scale up additional VMs from pre-configured instance templates, both within a single zone and across multiple zones within a region. MIGs are ideal for applications that require resilience to zone loss and are stateless, require configuration and resource planning. Multiple regional MIGs can be used to achieve region outage resilience for stateless applications.

upvoted 1 times

🗨️ **omermahgoub** 1 year, 6 months ago

The correct answer is D: Deploy the application on two Compute Engine instance groups, each in a separate project and a different region. Use the first instance group to serve traffic, and use the HTTP load balancing service to fail over to the standby instance group in case of a disaster.

To implement a disaster recovery plan that requires your application to fail over to another region in case of a regional outage, you should deploy the application on two Compute Engine instance groups, each in a separate project and a different region. This will ensure that the application is running in at least two regions, so that if one region experiences an outage, the application can still be accessed from the other region.

You can use the HTTP load balancing service to distribute traffic between the two instance groups and to fail over to the standby instance group in case of a disaster. This will ensure that your application is always available, even in the event of a regional outage.

upvoted 2 times

🗨️ **omermahgoub** 1 year, 6 months ago

Option A: Deploying the application on two Compute Engine instances in the same project but in a different region will not provide enough redundancy, as the instances are still in the same project and could be affected by the same regional outage.

Option B: Deploying the application on a Compute Engine instance and using the HTTP load balancing service to fail over to an instance on your premises in case of a disaster is not a valid option, as it does not provide the required disaster recovery capability.

Option C: Deploying the application on two Compute Engine instance groups, each in the same project but in a different region, is not a valid option, as it does not provide the required disaster recovery capability.

upvoted 2 times

🗨️ **oms_muc** 1 year, 6 months ago

IMHO A would also work (test env). In production relying on instances from other regions (introducing latency) just for possible expected zone outages, would not be my best practice.

upvoted 1 times

🗨️ **AniketD** 1 year, 7 months ago

Selected Answer: C

Correct answer is C. No need to host MIG in separate projects.

upvoted 2 times

🗨️ 👤 **megumin** 1 year, 7 months ago

Selected Answer: C

ok for C

upvoted 1 times

🗨️ 👤 **AzureDP900** 1 year, 8 months ago

C is right choice

upvoted 1 times

🗨️ 👤 **minmin2020** 1 year, 8 months ago

Selected Answer: C

C - using instance groups when planning for DR is better than having single vm's (<https://cloud.google.com/architecture/disaster-recovery>). Having the resources in the same project is probably good for resource management.

upvoted 1 times

🗨️ 👤 **arjunvijayvargiya** 1 year, 8 months ago

Answer should have been A as autoscaling requirements are not mentioned.

upvoted 1 times

🗨️ 👤 **BiddlyBdoyn** 1 year, 8 months ago

I think you need an group for the load balancer so A no good?

upvoted 2 times

Question #53

Topic 1

You are deploying an application on App Engine that needs to integrate with an on-premises database. For security purposes, your on-premises database must not be accessible through the public internet. What should you do?

- A. Deploy your application on App Engine standard environment and use App Engine firewall rules to limit access to the open on-premises database.
- B. Deploy your application on App Engine standard environment and use Cloud VPN to limit access to the on-premises database.
- C. Deploy your application on App Engine flexible environment and use App Engine firewall rules to limit access to the on-premises database.
- D. Deploy your application on App Engine flexible environment and use Cloud VPN to limit access to the on-premises database.

🗨️ 👤 **MyPractice** **Highly Voted** 👍 4 years, 11 months ago

Agree with D - "When to choose the flexible environment" "Accesses the resources or services of your Google Cloud project that reside in the Compute Engine network."

<https://cloud.google.com/appengine/docs/the-appengine-environments>

upvoted 54 times

🗨️ 👤 **AWS56** 4 years, 11 months ago

Why not B ? <https://cloud.google.com/appengine/docs/flexible/python/using-third-party-databases>

upvoted 7 times

🗨️ 👤 **areza** 3 years, 6 months ago

because app engine standard cant connect to on-prem db

upvoted 29 times

🗨️ 👤 **VSMu** 1 year, 10 months ago

Where does it say appengine cannot connect to on-prem db? With CloudVPN, it should connect as per this

https://cloud.google.com/appengine/docs/flexible/storage-options#on_premises

Also going with D will require app to be containerized. That is not listed in the requirement.

upvoted 6 times

🗨️ 👤 **Cloudcrawler** 1 year, 4 months ago

This is the link for Standard Env

<https://cloud.google.com/appengine/docs/standard/storage-options>

Both standard and Flexible can connect to a VPC with Serverless VPC connector. Once it connects to a VPC, connecting to on-prem is same for any service.

upvoted 4 times

🗨️ 👤 **jrisl1991** 1 year, 2 months ago

I just had the same confusion. Serverless VPC Connector is something relatively newer than this question on the exam, so probably it's safer to assume that a VPC connection is not supported (at least directly) by App Engine Standard.

Besides, this would add extra overhead, and would also increase the costs for the solution.

Most of these questions haven't been updated or repurposed according to newer products and services. For this particular question, using a Serverless VPC Connector would add unnecessary complexity and the solution would become more expensive.

I swore to god it was B lol, but after a few hours of reading the documentation, I changed my mind and switched to option D. I might want to do the same.

upvoted 4 times

🗨️ 👤 **elaineshi** 2 years, 6 months ago

Isn't the question said "not public internet access"?

upvoted 2 times

🗨️ 👤 **mnsait** 7 months ago

Yes, that phrase in the question bothers me too. However, when I check this:

<https://cloud.google.com/appengine/docs/flexible/storage-options#:~:text=On%20premises,-If%20you%20have&text=Because%20App%20Engine%20and%20Compute,database%20server's%20internal%20IP%20address.>

It says "If you have existing on-premises databases that you want to make accessible to your App Engine app, you can either configure your internal network and firewall to give the database a public IP address or connect using a VPN."

it says "If you have existing on-premises databases that you want to make accessible to your App Engine app, you can either configure your internal network and firewall to give the database a public IP address or connect using a VPN."

So I think the question should have skipped the words "not public internet access" if they want us to choose VPN.

upvoted 2 times

🗨️ 👤 **haroldbenites** 3 years ago

In a forum mentions that GCE and CAP flex are designed to connect to VPC. With GAP standard is needed a proxy.

<https://stackoverflow.com/questions/47537204/how-to-connect-app-engine-and-on-premise-server-through-vpn>

upvoted 5 times

  **jcmoranp** Highly Voted 5 years, 1 month ago

Right is D:



<https://stackoverflow.com/questions/37137914/is-it-possible-to-use-google-app-engine-with-google-cloud-vpn>

upvoted 18 times

  **amxexam** 2 years, 7 months ago

Question is can we restrict access with VP N ?

upvoted 5 times

  **moiradavis** 2 years, 5 months ago

The stackoverflow reference is older than the answer (6 years) I think that has changed.

upvoted 1 times

  **deep316** Most Recent 1 week ago

Selected Answer: D

Standard requires more setup compared to Flexible.

Standard Environment:

To connect from the standard environment, you primarily use "Serverless VPC Access" which allows your App Engine app to reach your VPC network over private IP addresses without exposing it directly to the public internet.

Flexible Environment:

In the flexible environment, you can directly connect to your VPC network by deploying your app within the same VPC as your Cloud VPN gateway, enabling a more seamless connection using the private IP addresses of your network resources.

upvoted 1 times

  **Nimeshv** 2 weeks ago

Selected Answer: D

App Engine Standard Environment:

Limited Customization: It runs on predefined runtime environments with limited flexibility.

No Access to Compute Engine Network: It does not support integration with the VPC network, which is necessary for setting up VPN connections.

App Engine Flexible Environment:

Customizable Runtimes: Allows you to run custom runtimes and use your own Docker containers.

VPC Integration: Fully supports VPC networking, enabling you to set up Cloud VPN to securely connect to your on-premises database.

Greater Flexibility: More control over the instance types, scaling, and networking options.

upvoted 1 times

  **desertlotus1211** 2 weeks ago

Selected Answer: D

Per google:

For using Cloud VPN, App Engine Flexible is generally considered better than App Engine Standard because it offers more customization and control over your virtual machine environment, allowing you to configure network settings and access on-premises resources more easily through the VPN

Answer is D

upvoted 1 times

🗲️ 👤 **desertlotus1211** 3 weeks, 2 days ago

Selected Answer: D

The answer is BOTH B&D...

Answer: BD

I'm not sure what is the point of the question or the problem.

The standard environment can scale from zero instances up to thousands very quickly. In contrast, the flexible environment must have at least one instance running for each active version and can take longer to scale out in response to traffic. Standard environment uses a custom-designed autoscaling algorithm.

But the question doesn't address this.

upvoted 1 times

🗲️ 👤 **desertlotus1211** 3 weeks, 2 days ago

Sorry I have to mark an answer. I wanted to choose B&D, but it won't let me

upvoted 1 times

🗲️ 👤 **icarogsm** 3 weeks, 6 days ago

Selected Answer: D

D, just App Engine Flex can connect to onprem.

upvoted 1 times

🗲️ 👤 **Ekramy_Elnaggar** 1 month ago

Selected Answer: D

The flexible environment gives you more control over the networking configuration of your application. This is crucial for setting up a secure connection to your on-premises database.

upvoted 1 times

🗲️ 👤 **yocixim836** 1 month, 1 week ago

Selected Answer: B

https://cloud.google.com/appengine/docs/standard/storage-options#on_premises

upvoted 2 times

🗲️ 👤 **dpttpd** 1 month, 4 weeks ago

Selected Answer: B

https://cloud.google.com/appengine/docs/standard/storage-options#on_premises

upvoted 2 times

🗲️ 👤 **raghupothula** 2 months, 3 weeks ago

B and C are not appropriate and wherein in App Engine flex resources reside in VPC NETwo

<https://cloud.google.com/appengine/docs/the-appengine-environments#app-engine-environments>

D

upvoted 1 times

🗲️ 👤 **maxdanny** 3 months, 2 weeks ago

Selected Answer: D

App Engine flexible environment provides more flexibility and supports VPC (Virtual Private Cloud) connectivity, which allows you to set up a Cloud VPN connection. The VPN can be used to securely connect your App Engine application to the on-premises database without exposing to the public internet.

upvoted 2 times

🗲️ 👤 **joecloud12** 4 months, 2 weeks ago

Selected Answer: B

flexible is more expensive. standard will suffice

upvoted 1 times

🗲️ 👤 **janji456** 4 months, 3 weeks ago



D

et up a VPN connection between your on-premises network and Google Cloud.

This establishes a secure tunnel for communication.



Your App Engine

upvoted 1 times

  **neha_pallod** 5 months, 2 weeks ago



Selected Answer: B

right answer is B
upvoted 1 times

  **nhatne** 5 months, 3 weeks ago

Selected Answer: D

"your on-premises database must not be accessible through the public internet"
=> definitely C
upvoted 1 times

  **nhatne** 5 months, 3 weeks ago

Question #54


Topic 1

You are working in a highly secured environment where public Internet access from the Compute Engine VMs is not allowed. You do not yet have a VPN connection to access an on-premises file server. You need to install specific software on a Compute Engine instance. How should you install the software?


- A. Upload the required installation files to Cloud Storage. Configure the VM on a subnet with a Private Google Access subnet. Assign only an internal IP address to the VM. Download the installation files to the VM using gsutil.
- B. Upload the required installation files to Cloud Storage and use firewall rules to block all traffic except the IP address range for Cloud Storage. Download the files to the VM using gsutil.
- C. Upload the required installation files to Cloud Source Repositories. Configure the VM on a subnet with a Private Google Access subnet. Assign only an internal IP address to the VM. Download the installation files to the VM using gcloud.
- D. Upload the required installation files to Cloud Source Repositories and use firewall rules to block all traffic except the IP address range for Cloud Source Repositories. Download the files to the VM using gsutil.

  **zaki_b** **Highly Voted**  5 years, 1 month ago



Internet access is not allowed so it should be A. CMIIW
upvoted 55 times

  **tartar** 4 years, 4 months ago

A is ok
upvoted 10 times

  **kumarp6** 4 years, 1 month ago

A is the answer
upvoted 3 times

  **nitinz** 3 years, 9 months ago

A is the best answer.
upvoted 3 times

  **KNG** **Highly Voted**  4 years, 10 months ago

Should be A
<https://cloud.google.com/vpc/docs/configure-private-services-access>
Note: Even though the IP addresses for Google APIs and services are public, the traffic path from instances that are using Private Google Access to the Google APIs remains within Google's network.
upvoted 20 times

  **Ekramy_Elnaggar** **Most Recent**  1 month ago

Selected Answer: A

Private Google Access allows your VM to access Google APIs and services (like Cloud Storage) without needing a public IP address. This is crucial in your restricted environment.
upvoted 1 times

🗨️ **maxdanny** 3 months, 2 weeks ago

Selected Answer: A

Private Google Access ensures the VM can reach Cloud Storage using its internal IP, while still restricting public internet access.
upvoted 3 times

🗨️ **arotesa** 3 months, 2 weeks ago

The Answer is D
upvoted 1 times

🗨️ **AdityaGupta** 1 year, 2 months ago

Selected Answer: A

A. Upload the required installation files to Cloud Storage. Configure the VM on a subnet with a Private Google Access subnet. Assign only an internal IP address to the VM. Download the installation files to the VM using gsutil.
upvoted 1 times

🗨️ **ppandher** 1 year, 11 months ago

Those who are opting for B, Can please explain without Internet access and without Private Google Access enabled how will they communicate with Cloud Storage ? :)
upvoted 5 times

🗨️ **omermahgoub** 1 year, 12 months ago

The correct answer is A: Upload the required installation files to Cloud Storage. Configure the VM on a subnet with a Private Google Access subnet. Assign only an internal IP address to the VM. Download the installation files to the VM using gsutil.

To install specific software on a Compute Engine instance in a highly secured environment where public Internet access is not allowed, you can follow these steps:

Upload the required installation files to Cloud Storage.

Configure the VM on a subnet with a Private Google Access subnet. This will allow the VM to access Google APIs and services, such as Cloud Storage, without requiring a public IP address or internet access.

Assign only an internal IP address to the VM. This will ensure that the VM is not accessible from the public internet.

Download the installation files to the VM using gsutil, which is a command-line tool that allows you to access Cloud Storage from the VM.

upvoted 6 times

🗨️ **omermahgoub** 1 year, 12 months ago

Option B: Uploading the required installation files to Cloud Storage and using firewall rules to block all traffic except the IP address range for Cloud Storage is not a valid option, as it does not allow the VM to access the installation files without public internet access.

Option C: Uploading the required installation files to Cloud Source Repositories and using gcloud to download the files to the VM is not a valid option, as Cloud Source Repositories does not support storing large binary files such as installation files.

Option D: Uploading the required installation files to Cloud Source Repositories and using firewall rules to block all traffic except the IP address range for Cloud Source Repositories is not a valid option, as it does not allow the VM to access the installation files without public internet access.

upvoted 6 times

🗨️ **habros** 2 years ago

Selected Answer: A

Eliminate B&D as it connects via public networks despite it being a Google Cloud service.
upvoted 1 times

🗨️ **megumin** 2 years, 1 month ago

Selected Answer: A

ok for A
upvoted 1 times

🗨️ **stevehlw** 2 years, 1 month ago

With private Google access subnet, the VM can reach external network. With this setting, it violates "public Internet access from the Compute Engine VMs is not allowed". Can someone explain why it's not B instead?

upvoted 2 times

🗨️ **ppandher** 2 years ago

Private Google access means - refer to <https://www.youtube.com/watch?v=yd5FtV8aJkk>
upvoted 3 times

🗨️ **AzureDP900** 2 years, 2 months ago

A is good

upvoted 1 times

🗨️ **minmin2020** 2 years, 2 months ago

Selected Answer: A

A. Upload the required installation files to Cloud Storage. Configure the VM on a subnet with a Private Google Access subnet. Assign only an internal IP address to the VM. Download the installation files to the VM using gsutil.

upvoted 1 times

🗨️ **munebarshad** 2 years, 3 months ago

Selected Answer: B

Configuring Private Google Access is the best way to access Google Services for VM that does not have access to the internet. In order to access Google Private APIs egress should be opened to the following IP Address restricted.googleapis.com (199.36.153.4/30). VM will leverage internal networking to access Cloud Storage

<https://cloud.google.com/vpc/docs/configure-private-google-access>

upvoted 4 times

🗨️ **6721sora** 2 years, 3 months ago

C because Cloud repositories is a private Git within Google cloud. Hence it is ideal for simple pull, push, clone type "git" operations. As this is within Google cloud and is a private git, you do not need public internet access

upvoted 1 times

🗨️ **BiddlyBdoyn** 2 years, 2 months ago

I think it's not this because Clouse Source Repositories is for source code. Sounds like we are looking for an executable?

upvoted 1 times

🗨️ **amxexam** 2 years, 7 months ago

Selected Answer: A

C&D we are all eliminating becoz of source storage repo

Between A& B B looks more tempting to select because it mentions fire wallrule But the problem with B is the statement is wrong the access happen from VM to storage and the statement mentions traffic from storage to Vm.

Hence A

upvoted 3 times

🗨️ **celina123123** 2 years, 11 months ago

Selected Answer: A

You have to set Private Google Access for communicating between VM and Storage

upvoted 3 times

Question #55

Topic 1

Your company is moving 75 TB of data into Google Cloud. You want to use Cloud Storage and follow Google-recommended practices. What should you do?

A. Move your data onto a Transfer Appliance. Use a Transfer Appliance Rehydrator to decrypt the data into Cloud Storage.

- B. Move your data onto a Transfer Appliance. Use Cloud Dataprep to decrypt the data into Cloud Storage.
- C. Install gsutil on each server that contains data. Use resumable transfers to upload the data into Cloud Storage.
- D. Install gsutil on each server containing data. Use streaming transfers to upload the data into Cloud Storage.

🗨️ 👤 **AshishK** Highly Voted 5 years ago

It should be 'A'

Transfer Appliance lets you quickly and securely transfer large amounts of data to Google Cloud Platform via a high capacity storage server that you lease from Google and ship to our datacenter. Transfer Appliance is recommended for data that exceeds 20 TB or would take more than 4 weeks to upload.

upvoted 34 times

🗨️ 👤 **MyPractice** 4 years, 11 months ago

where did u get that 20 TB number - can help to share link?

upvoted 1 times

🗨️ 👤 **onashwani** 4 years ago

Here is the link:

<https://cloud.google.com/transfer-appliance/docs/2.2/overview>

upvoted 4 times

🗨️ 👤 **gcp_learner** 3 years ago

But that link mentions a few hundred terabytes to 1 petabyte not 20TB or did I read that incorrectly?

upvoted 2 times

🗨️ 👤 **mindhoc** 1 year, 1 month ago

The request transfer appliance UI seems to suggest that it is not cost effective under 20TB of data.

upvoted 2 times

🗨️ 👤 **Yahowmy** 4 years, 5 months ago

To this date Transfer Appliance supported locations are only

United States

Canada

European Union

Norway

Switzerland.

What if data reside in a location other than this?

C is the most convenience for this scenario.

upvoted 11 times

🗨️ 👤 **ccpmad** 6 months ago

stupid answer

upvoted 2 times

🗨️ 👤 **NoCrapEva** 10 months, 3 weeks ago

There is NO mention of region - you dont assume anything NOT mentioned in the question therefore - Ans =A

upvoted 1 times

🗨️ 👤 **Ramheadhunter** 2 years, 4 months ago

Why assume a scenario no provided in the question. We need to choose the best case scenario based on available information instead making assumptions. So A should be good.

upvoted 5 times

🗳️ 👤 **KouShikyou** Highly Voted 👍 5 years, 1 month ago

Why not A?

upvoted 30 times

🗳️ 👤 **tartar** 4 years, 4 months ago

A is ok

upvoted 9 times

🗳️ 👤 **kumarp6** 4 years, 1 month ago

It is A

upvoted 2 times

🗳️ 👤 **nitinz** 3 years, 9 months ago

A, anything over 10TB goes via appliance.

upvoted 14 times

🗳️ 👤 **Begum** 2 years, 2 months ago

I have moved 120 TB using gsutil- cost effectively!

upvoted 1 times

🗳️ 👤 **zr79** 2 years, 2 months ago

takes longer though

upvoted 1 times

🗳️ 👤 **Koushick** 3 years, 7 months ago

Answer is A.

upvoted 4 times

🗳️ 👤 **kip21** Most Recent 🕒 11 months, 1 week ago

A - Correct

upvoted 1 times

🗳️ 👤 **AdityaGupta** 1 year, 2 months ago

Selected Answer: A

Sending 75 TB of data on reliable 1.5 Gbps line will take about 6 days to complete data transfer online at the same time it will consume entire bandwidth. Hence use of Transfer appliance is required.

upvoted 1 times

🗳️ 👤 **MaheshKaswan** 1 year, 6 months ago

Selected Answer: C

Option A is partially correct as you would not use a Transfer Appliance Rehydrator to decrypt the data. The Transfer Appliance itself is used to encrypt and decrypt the data. Option C is correct.

upvoted 2 times

🗳️ 👤 **RVivek** 1 year, 10 months ago

Selected Answer: A

gsutil is recommended for data size less than a TB. That rules out C and D

B says decrypt data using Dataprep not sure this is possible.

<https://cloud.google.com/solutions/migration-to-google-cloud-transferring-your-large-datasets#transfer-options>

upvoted 3 times

🗳️ 👤 **n_nana** 1 year, 11 months ago

Selected Answer: A

It will be more precise with info about the bandwidth

Google says:

The two main criteria to consider with Transfer Appliance are cost and speed. With reasonable network connectivity (for example, 1 Gbps), transferring 100 TB of data online takes over 10 days to complete. If this rate is acceptable, an online transfer is likely a good solution for your needs. If you only have a 100 Mbps connection (or worse from a remote location), the same transfer takes over 100 days. At this point, it's worth considering an offline-transfer option such as Transfer Appliance.

So even for such 100 TB google choose between transfer appliance or online transfer. not going with gsutil at all. it is clear gsutil is suitable for small to medium size (less than 1 TB)

so with no more details, google recommendation is A

upvoted 3 times

  **omermahgoub** 1 year, 12 months ago

The correct answer is A: Move your data onto a Transfer Appliance. Use a Transfer Appliance Rehydrator to decrypt the data into Cloud Storage.

To move large amounts of data into Google Cloud, it is recommended to use Transfer Appliance. Transfer Appliance is a physical storage device that you can use to transfer large amounts of data to Google Cloud quickly and securely. Once you have moved your data onto a Transfer Appliance, you can use a Transfer Appliance Rehydrator to decrypt the data and load it into Cloud Storage.

upvoted 3 times

  **omermahgoub** 1 year, 12 months ago

Option B: Using Cloud Dataprep to decrypt the data into Cloud Storage is not a valid option, as Cloud Dataprep is a data preparation tool that does not support data transfer or decryption.

Option C: Using resumable transfers to upload the data into Cloud Storage is not a recommended option for moving large amounts of data; resumable transfers are designed for smaller data sets and may not be efficient for transferring large amounts of data.

Option D: Using streaming transfers to upload the data into Cloud Storage is not a recommended option for moving large amounts of data; streaming transfers are designed for transferring real-time data streams and may not be efficient for transferring large amounts of data.

Therefore, the correct answer is A: Move your data onto a Transfer Appliance. Use a Transfer Appliance Rehydrator to decrypt the data into Cloud Storage.

upvoted 5 times

  **megumin** 2 years, 1 month ago

Selected Answer: A

ok for A

upvoted 1 times

  **AzureDP900** 2 years, 2 months ago

Option A Use a Transfer Appliance Rehydrator

upvoted 1 times

  **minmin2020** 2 years, 2 months ago

Selected Answer: A

A. Move your data onto a Transfer Appliance. Use a Transfer Appliance Rehydrator to decrypt the data into Cloud Storage.

upvoted 1 times

  **sgofficial** 2 years, 4 months ago

Selected Answer: A

A is correct ...

<https://cloud.google.com/architecture/migration-to-google-cloud-transferring-your-large-datasets#transfer-options>

1. gsutil is for less than <1 TB data with enough bandwidth, so C and D can be eliminated
2. option b can be eliminated since dataprep for decryption is not correct
3. so only left over is a and its offline transfer, since the question did not give any time line when the transfer to be completed

upvoted 3 times

  **[Removed]** 2 years, 7 months ago

Selected Answer: A

<https://cloud.google.com/transfer-appliance/docs/4.0/overview#suitability>

upvoted 1 times

  **amxexam** 2 years, 7 months ago

Selected Answer: A

I would eliminate B & C as the question clearly mentions Google's recommendations. About 10 TB or more, we need to use the transfer appliance. Let's not worry about what regions. OK for now.

Between A & B, B is overkill as the transfer appliance allows decryption. Hence A.

upvoted 1 times

  **meokey** 2 years, 8 months ago


Selected Answer: A

Is Transfer Appliance suitable for me?

"Your data size is greater than or equal to 10TB."

<https://cloud.google.com/transfer-appliance/docs/4.0/overview#suitability>

upvoted 3 times

  **awsarchitect5** 2 years, 10 months ago

Selected Answer: A

<https://cloud.google.com/blog/ja/topics/developers-practitioners/how-transfer-your-data-google-cloud>
upvoted 3 times

  **Narinder** 2 years, 11 months ago

A, is the correct option for transferring data of few TB to PB.
gsutil is viable option if the data size is about 1TB or less than that.

Reference: <https://cloud.google.com/architecture/migration-to-google-cloud-transferring-your-large-datasets>
upvoted 2 times

Question #56

Topic 1



You have an application deployed on Google Kubernetes Engine using a Deployment named echo-deployment. The deployment is exposed using a Service called echo-service. You need to perform an update to the application with minimal downtime to the application. What should you do?

- A. Use kubectl set image deployment/echo-deployment <new-image>
- B. Use the rolling update functionality of the Instance Group behind the Kubernetes cluster
- C. Update the deployment yaml file with the new container image. Use kubectl delete deployment/echo-deployment and kubectl create <new-yaml-file>
- D. Update the service yaml file with the new container image. Use kubectl delete service/echo-service and kubectl create <new-yaml-file>

  **ffk**  5 years, 1 month ago

A is correct.



B is funny
upvoted 47 times

  **AmitAr** 2 years, 7 months ago

B looks most sensible (not funny). rolling update is a deployment strategy, which will deploy on pods 1 by 1, i.e. by the time first pod is getting newer version of application, other pods are running with older version... In this way, there will be no downtime of application.. which is the real ask from this question.
I recommend B
upvoted 6 times

  **monopfm** 7 months, 3 weeks ago

Use the rolling update functionality of the >[Instance Group behind the Kubernetes cluster]<. It's not a rolling update of a Deployment.
Read carefully.
upvoted 4 times

  **tartar** 4 years, 4 months ago

A is ok
upvoted 14 times

  **kumarp6** 4 years, 1 month ago

Yes A is correct
upvoted 3 times

  **nitin2** 3 years, 9 months ago

Only logical answer is A.
upvoted 1 times

  **jcmoranp**  5 years, 1 month ago

Correct is A
upvoted 13 times

🗨️ 👤 **sim7243** Most Recent 1 month, 1 week ago

Selected Answer: A

option A

upvoted 1 times

🗨️ 👤 **isa_pr** 5 months, 1 week ago

It's A. As per K8s documentation:

To update the image of the application to version 2, use the set image subcommand, followed by the deployment name and the new image version:

```
kubectl set image deployments/kubernetes-bootcamp kubernetes-bootcamp=docker.io/jocatalin/kubernetes-bootcamp:v2
```

The command notified the Deployment to use a different image for your app and initiated a rolling update."

"

upvoted 2 times

🗨️ 👤 **kip21** 11 months, 1 week ago

Option C - is the best option to perform an update to an application deployed on Google Kubernetes Engine with minimal downtime because provides control over the update process, ensures high availability, and minimizes disruption. Rolling update functionality can also be used but requires more effort to implement.

Option A and Option D may result in downtime if the new image is incompatible with the existing application.

upvoted 1 times

🗨️ 👤 **thewalker** 1 year, 1 month ago


A

https://cloud.google.com/kubernetes-engine/docs/how-to/updating-apps#updating_an_application

upvoted 4 times

🗨️ 👤 **AdityaGupta** 1 year, 2 months ago

Selected Answer: C

C. Update the deployment yaml file with the new container image. Use kubectl delete deployment/echo-deployment and kubectl create deployment/echo-deployment --image=f <yaml-file>

I agreed with omermahgoub with his explanation.

upvoted 1 times

🗨️ 👤 **cacharritos** 11 months, 3 weeks ago

delete.. minimal downtime.. A is correct ^_^U

upvoted 1 times

🗨️ 👤 **vamgcp** 1 year, 10 months ago

To perform an update to the application with minimal downtime on Google Kubernetes Engine (GKE), you can use a rolling update strategy, which involves updating the application incrementally, one pod at a time, while ensuring that the updated pods are functioning properly before updating the next set. Here's the general process:

```
kubectl set image deployment/echo-deployment echo=<new_image_tag>
```

upvoted 4 times

🗨️ 👤 **roaming_panda** 1 year, 11 months ago

Selected Answer: A

<https://cloud.google.com/kubernetes-engine/docs/how-to/updating-apps>

says rolling updates and mentions same command .

So 100 % A

upvoted 9 times

🗨️ **omermahgoub** 1 year, 12 months ago

The correct answer is C: Update the deployment yaml file with the new container image. Use `kubectl delete deployment/echo-deployment` and `kubectl create -f <yaml-file>`.

To perform an update to an application deployed on Google Kubernetes Engine with minimal downtime, you can follow these steps:

Update the deployment yaml file with the new container image.

Use the `kubectl delete deployment/echo-deployment` command to delete the existing deployment.

Use the `kubectl create -f <yaml-file>` command to create a new deployment using the updated yaml file.

This process, known as a rolling update, allows you to update your application with minimal downtime by replacing the old version of the application with the new version one pod at a time, while ensuring that there is always at least one pod available to serve traffic.

upvoted 3 times

🗨️ **omermahgoub** 1 year, 12 months ago

using `kubectl set image deployment/deployment <new-image>` will not allow you to perform an update to the application with minimal downtime, even if the deployment is exposed using a Service.

This command will update the image of the containers in the deployment, but it will not perform a rolling update. A rolling update allows you to update your application with minimal downtime by replacing the old version of the application with the new version one pod at a time, while ensuring that there is always at least one pod available to serve traffic. Without a rolling update, all of the pods in the deployment will be replaced at the same time, which may result in downtime for the application.

upvoted 1 times

🗨️ **omermahgoub** 1 year, 12 months ago

Option A: Using `kubectl set image deployment/echo-deployment <new-image>` will update the image of the containers in the deployment, it will not perform a rolling update and may result in downtime for the application.

Option B: Using the rolling update functionality of the Instance Group behind the Kubernetes cluster is not a valid option, as the rolling update functionality is used to update the instances in the instance group, not the containers in a deployment.

Option D: Updating the service yaml file with the new container image and using `kubectl delete service/echo-service` and `kubectl create -f <yaml-file>` is not a valid option, as the service is not responsible for running the application containers and updating the service will not update the application.

upvoted 3 times

🗨️ **CkWongCk** 1 year, 10 months ago

A is correct, update template spec image in deployment yaml will trigger rollout deploy

upvoted 1 times

🗨️ **_kartik_raj** 1 year, 2 months ago

Answer is A, you are wrong as hell, if you delete deployment its obvious app will face downtime

upvoted 3 times

🗨️ **jasenmornin** 2 years ago

Selected Answer: A

I think A is correct:

B. I don't understand the objective of this option.

C and D. These are eliminated because they involve suffering a downtime when the resources are eliminated, so they are not fulfilling one of the requirements.

upvoted 3 times

🗨️ **markus_de** 2 years ago

Selected Answer: A

Example from official Kubernetes docu (for NGINX):

`kubectl set image deployment/nginx-deployment nginx=nginx:1.16.1`

<https://kubernetes.io/docs/concepts/workloads/controllers/deployment/>

upvoted 5 times

🗨️ **megumin** 2 years, 1 month ago

Selected Answer: A

ok for A

upvoted 2 times

  **AzureDP900** 2 years, 2 months ago

A is right -- kubectl set image deployment/echo-deployment
upvoted 1 times

  **RitwickKumar** 2 years, 4 months ago

Selected Answer: A

Source: <https://kubernetes.io/docs/concepts/workloads/controllers/deployment/#updating-a-deployment>

Deployment ensures that only a certain number of Pods are down while they are being updated. By default, it ensures that at least 75% of the desired number of Pods are up (25% max unavailable).

Deployment also ensures that only a certain number of Pods are created above the desired number of Pods. By default, it ensures that at most 125% of the desired number of Pods are up (25% max surge).



upvoted 8 times

  **Mikado211** 2 years, 4 months ago

Selected Answer: A

Answer is A

It can't be C, if you delete and recreate the deployment you will have a downtime between the deletion and the recreation.
upvoted 2 times

  **Ric350** 2 years, 5 months ago

It's definitely A. See here under updating a deployment on the right hand side.

<https://kubernetes.io/docs/concepts/workloads/controllers/deployment/#updating-a-deployment>

upvoted 2 times

Question #57

Topic 1

Your company is using BigQuery as its enterprise data warehouse. Data is distributed over several Google Cloud projects. All queries on BigQuery need to be billed on a single project. You want to make sure that no query costs are incurred on the projects that contain the data. Users should be able to query the datasets, but not edit them.

How should you configure users' access roles?

- A. Add all users to a group. Grant the group the role of BigQuery user on the billing project and BigQuery dataViewer on the projects that contain the data.
- B. Add all users to a group. Grant the group the roles of BigQuery dataViewer on the billing project and BigQuery user on the projects that contain the data.
- C. Add all users to a group. Grant the group the roles of BigQuery jobUser on the billing project and BigQuery dataViewer on the projects that contain the data.
- D. Add all users to a group. Grant the group the roles of BigQuery dataViewer on the billing project and BigQuery jobUser on the projects that contain the data.

  **RitwickKumar**  1 year, 10 months ago

 **nitwickanur**  1 year, 10 months ago

Selected Answer: C

Both A & C are correct but using the principle of least privileges C is the most appropriate.

BigQuery User: (roles/bigquery.user)

When applied to a dataset, this role provides the ability to read the dataset's metadata and list tables in the dataset.

When applied to a project, this role also provides the ability to run jobs, including queries, within the project. A principal with this role can enumerate their own jobs, cancel their own jobs, and enumerate datasets within a project. Additionally, allows the creation of new dataset within the project; the creator is granted the BigQuery Data Owner role(roles/bigquery.dataOwner) on these new datasets.

Lowest-level resources where you can grant this role: Dataset

BigQuery Job User: (roles/bigquery.jobUser)

Provides permissions to run jobs, including queries, within the project.

Lowest-level resources where you can grant this role: Project

Source: <https://cloud.google.com/bigquery/docs/access-control>

upvoted 24 times

 **kimharsh**  2 years, 4 months ago

Selected Answer: C

C is the correct Answer ,

A is wrong because bq User Permission will allow you to edit the dataset, which is something that we don't want in this scenario.

B and D is wrong because "You want to make sure that no query costs are incurred on the projects that contain the data" so you don't want users to fire queries on the Project that contains the dataset , hence the "dataViewer" permission

<https://cloud.google.com/bigquery/docs/access-control>

upvoted 20 times

 **kratosmat** 1 year, 3 months ago


It seems that User Permission doesn't allow to edit data, isn't it?

upvoted 1 times

 **Edgo97**  4 months ago

The link to refer here: <https://cloud.google.com/bigquery/docs/access-control>

upvoted 1 times

 **SidsA** 1 year, 2 months ago

Selected Answer: C

The "roles/bigquery.jobUser" role provides the permission to run jobs, including querying, exporting and copying data, and creating views and materialized views. This role does not provide permissions to create, update, or delete BigQuery resources, such as datasets, tables, and models. Users with this role can only interact with BigQuery through jobs.

The "roles/bigquery.User" role, on the other hand, provides the permission to create, update, and delete BigQuery resources, as well as run jobs. This role includes all the permissions of the "roles/bigquery.jobUser" role, and in addition allows users to manage BigQuery resources, such as creating datasets, tables, and models, and modifying their schema and access controls.

upvoted 3 times


 **jlambdan** 1 year, 3 months ago

Selected Answer: C

A is wrong because <https://cloud.google.com/bigquery/docs/access-control#bigquery.user>

C is correct because <https://cloud.google.com/bigquery/docs/access-control#bigquery.jobUser>

upvoted 1 times

 **jay9114** 1 year, 5 months ago

Selected Answer: C

Important statements from the prompt

1. All queries need to be billed to a single project - one project that queries data stored on other projects. Let's call this our billing project.

a. jobUser is the best role to satisfy this need, because it provides permission to run jobs and queries within a project.

2. Other projects is where the data resides. These projects don't need much access besides the ability to be viewed (not edited).

a. The dataViewer role provide permission to read all datasets in the project.

upvoted 7 times