

Question #110

Topic 1

Your company has announced that they will be outsourcing operations functions. You want to allow developers to easily stage new versions of a cloud-based application in the production environment and allow the outsourced operations team to autonomously promote staged versions to production. You want to minimize the operational overhead of the solution. Which Google Cloud product should you migrate to?

- A. App Engine
- B. GKE On-Prem
- C. Compute Engine
- D. Google Kubernetes Engine

  **kopper2019** Highly Voted 3 years, 5 months ago

A. App Engine
upvoted 36 times

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

Answer should be A as only with App Engine we have a default service account which allows the user to deploy the changes per project. for C we may have to configure additional permission for both DEV and Operations team to deploy the changes.

<https://cloud.google.com/appengine/docs/standard/php/service-account>
upvoted 24 times

  **Septhethus** Most Recent 6 months ago


A. App Engine.

Explanation:
Why A is correct:

App Engine: Google App Engine is a fully managed platform-as-a-service (PaaS) that allows developers to build and deploy applications quickly and easily without worrying about managing the underlying infrastructure. It supports continuous integration and continuous deployment (CI/CD) processes, enabling developers to stage new versions of applications easily.

Staging and Promotion: App Engine has built-in support for traffic splitting and versioning, which allows you to stage new versions of your application and gradually promote them to production. This can be done with minimal operational overhead, making it ideal for scenarios where operational functions are outsourced.


Minimal Operational Overhead: Since App Engine is fully managed, it reduces the operational burden significantly, making it easier for the outsourced operations team to handle promotions and manage the application.
upvoted 1 times

  **JaimeMS** 6 months, 2 weeks ago

Selected Answer: A
A. App Engine
upvoted 1 times

  **jaisonPathiyil** 8 months ago

Is this answers are really correct or misleading to us..?
upvoted 3 times

  **mesodan** 9 months, 2 weeks ago

Selected Answer: A
While both GKE and App Engine offer functionalities for deploying cloud-based applications, App Engine is more managed service compared GKE, resulting in lower operational overhead.
upvoted 2 times

🗲️ 👤 **Anandmrk** 10 months ago

Selected Answer: A

I did my exam today and saw this question. But I am sure A was the answer due to the operational overhead phrase
upvoted 3 times

🗲️ 👤 **[Removed]** 11 months, 3 weeks ago

A

why not D?

It requires more operational overhead compared to App Engine, as it involves managing the Kubernetes infrastructure.
upvoted 2 times

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

Selected Answer: D

In the question, we see "cloud-based application" - I assume, it means cloud native -> dockers/containers -> K8s -> GKE.
Hence, D is my option.
upvoted 2 times

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

Selected Answer: D

I agreed with "omermahgoub" the answer should be D.
As you will bundle the application and its dependencies into container image and deploy. All environments will have same image deployed from Dev, TEST, Staging to PROD. There will be less operational overhead for operations team.
upvoted 1 times

🗲️ 👤 **nocrush** 1 year, 3 months ago

Selected Answer: A

A

App Engine reduces ops overhead
upvoted 2 times

🗲️ 👤 **Frusci** 1 year, 3 months ago

Selected Answer: A

A. You deploy your new version to App Engine without setting it as the default version. The ops team then just has to make it the default version when they want to promote it. Simplest answer.
upvoted 2 times

🗲️ 👤 **heretolearnazure** 1 year, 3 months ago

App Engine because of less overhead.
upvoted 1 times

🗲️ 👤 **JohnWick2020** 1 year, 6 months ago

Answer is A.
By process of elimination you arrive at App Engine or GKE. Now the requirement is to "to minimize the operational overhead of the solution".
On the IaaS to PaaS spectrum, this can only be App Engine!

IaaS = Compute Engine.
Hybrid = GKE (engineering heavy).
PaaS = App Engine.
upvoted 3 times

🗲️ 👤 **Atanu** 1 year, 6 months ago

Selected Answer: A

"You want to minimize the operational overhead of the solution" ..This sentence is the key to go with Option A. GKE carries overhead as it's not purely PaaS.
upvoted 3 times

🗲️ 👤 **Sur_Nikki** 1 year, 7 months ago

It should be D. As GKE is considered to be the master product/service for creating a deployment and managing and keeping all the environments in SYNC
upvoted 1 times

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

Selected Answer: A

A is right as the requirement is to deploy new changes and manage the application with no operational overhead.
upvoted 1 times

Question #111

Topic 1

Your company is running its application workloads on Compute Engine. The applications have been deployed in production, acceptance, and development environments. The production environment is business-critical and is used 24/7, while the acceptance and development environments are only critical during office hours. Your CFO has asked you to optimize these environments to achieve cost savings during idle times. What should you do?

- A. Create a shell script that uses the `gcloud` command to change the machine type of the development and acceptance instances to a smaller machine type outside of office hours. Schedule the shell script on one of the production instances to automate the task.
- B. Use Cloud Scheduler to trigger a Cloud Function that will stop the development and acceptance environments after office hours and start them just before office hours.
- C. Deploy the development and acceptance applications on a managed instance group and enable autoscaling.
- D. Use regular Compute Engine instances for the production environment, and use preemptible VMs for the acceptance and development environments.

🗨️ **pamepadero** **Highly Voted** 3 years, 5 months ago

B is the answer.

<https://cloud.google.com/blog/products/it-ops/best-practices-for-optimizing-your-cloud-costs>

Schedule VMs to auto start and stop: The benefit of a platform like Compute Engine is that you only pay for the compute resources that you use. Production systems tend to run 24/7; however, VMs in development, test or personal environments tend to only be used during business hours and turning them off can save you a lot of money!

<https://cloud.google.com/blog/products/storage-data-transfer/save-money-by-stopping-and-starting-compute-engine-instances-on-schedule>

Cloud Scheduler, GCP's fully managed cron job scheduler, provides a straightforward solution for automatically stopping and starting VMs. By employing Cloud Scheduler with Cloud Pub/Sub to trigger Cloud Functions on schedule, you can stop and start groups of VMs identified with labels of your choice (created in Compute Engine). Here you can see an example schedule that stops all VMs labeled "dev" at 5pm and restarts them at 9am, while leaving VMs labeled "prod" untouched

upvoted 36 times

🗨️ **sgofficial** 2 years, 4 months ago

Excellenteven the good CFO is telling leave the office after 5.00 and come next day to work :)

upvoted 16 times

🗨️ **Ric350** 2 years, 5 months ago

Great answer and documentation. Def B

upvoted 2 times

🗨️ **rzygor** 2 years, 4 months ago

Question says that dev/test are "not critical", it doesn't mean that they are not needed at all ...

upvoted 17 times

🗨️ **kopper2019** **Highly Voted** 3 years, 5 months ago

Ans) B , assuming VM doesn't need to be up after office hours .

upvoted 25 times

🗲️ 👤 **25lion52** Most Recent 2 months, 3 weeks ago

Selected Answer: C

Stop the dev and acceptance envs is super weird. Any critical problems or overtimes will be an issue with this approach. Simple auto scaling environment is a good solution IMHO

upvoted 1 times

🗲️ 👤 **Gino17m** 8 months ago

B is right answer

upvoted 1 times

🗲️ 👤 **dija123** 8 months, 2 weeks ago

Selected Answer: B

Agree with B

upvoted 1 times

🗲️ 👤 **spuyol** 10 months, 2 weeks ago

Answer D

A: too complex and maybe small or zero saving if you can't find a valid smaller machine type

B: Not valid. Question says that PRE environments are not critical after office hours. But it doesn't say no service at all

C: Some risk is introduced if you have different architecture on PRE than PRO envs

D: It's the only valid and reliable option. Simple and effective. It's my choice. In a real scenario I will first start with this and then review if the savings are enough before more complicated choices

upvoted 3 times

🗲️ 👤 **Gino17m** 8 months ago

Ad. "B: Not valid. Question says that PRE environments are not critical after office hours. But it doesn't say no service at all"

But the Question says that PRE environments are critical during office hours, so you can't use preemptible VMs - "Compute Engine might stop (preempt) these instances if it needs to reclaim the compute capacity for allocation to other VMs"

upvoted 1 times

🗲️ 👤 **the1dv** 11 months, 1 week ago

Selected Answer: C

MIG's with autoscaling will scale to Zero if not needed

upvoted 3 times

🗲️ 👤 **spuyol** 10 months, 2 weeks ago

some risks are added if you have different architecture on PRO and PRE envs

upvoted 1 times

🗲️ 👤 **AWS_Sam** 11 months, 3 weeks ago

B for sure

upvoted 1 times

🗲️ 👤 **parthkulkarni998** 12 months ago

Selected Answer: C

Also managed instance group reduces instances in case of low/no-traffic incurring lesser charges. Ideally, its a cleaner approach considering ask is to optimize during "idle time". Incase people are working in different time zones, late shifts it doesn't make sense to trigger shutdown at predefined times.

upvoted 3 times

🗲️ 👤 **odacir** 1 year, 1 month ago

Selected Answer: B

B is the answer. But today, you don't need complicated CRON + CF. Auto shutdown by cron expression it's a feature built in:

<https://cloud.google.com/compute/docs/instances/schedule-instance-start-stop>

upvoted 1 times

- 🗨️ 👤 **werdy92** 1 year, 1 month ago
really wondering why not C...Not critical is not equivalent with not running at all....
upvoted 5 times
- 🗨️ 👤 **parthkulkarni998** 12 months ago
Also managed instance group reduces instances in case of low/no-traffic incurring lesser charges. Ideally, its a cleaner approach consider the ask is to optimize during "idle time". Incase people are working in different time zones, late shifts it doesnt make sense to trigger shutdown at a predefined times.
upvoted 2 times
- 🗨️ 👤 **wooloo** 1 year, 4 months ago
"are only critical during office hours" does not mean it could be completely stopped. So may the option C correct?
upvoted 6 times
- 🗨️ 👤 **mifrah** 1 year, 9 months ago
In my opinion B is over-engineered:
Why not just add an "instance schedule" for start/stop the Compute Engines?
Why creating a scheduler and writing a Cloud Function...
upvoted 3 times
- 🗨️ 👤 **ccpmad** 6 months, 1 week ago
Just exactly what I have thought. It is enough with instance schedule". But GCP wants you to spend money and use cloud functions LOL
upvoted 1 times
- 🗨️ 👤 **MaryMei** 1 year, 9 months ago
Selected Answer: B
<https://cloud.google.com/compute/docs/instances/viewing-and-applying-idle-vm-recommendations>
B seems close to this Google provided service option, the extra step should be using idle VM recommendations to find and stop idle VM instances to reduce waste of resources
upvoted 1 times
- 🗨️ 👤 **PAUGURU** 1 year, 10 months ago
Since the price of preemptibles is 1/4 the price of a standard machine D costs far less than B since office hours are 1/3 of whole day. It costs to keep them running 24h as preemptibles.
upvoted 3 times
- 🗨️ 👤 **DevOpsifier** 1 year, 6 months ago
Yes, but preemptibles use GCP excess resources so you will achieve the opposite of the desired effect, during office hours, they will underperform in the best case (worst case will stop altogether) and, during non-office hours, preemptibles will work well...
upvoted 1 times
- 🗨️ 👤 **windsor_43** 1 year, 11 months ago
The Answer is B.

Just had my exam today with a pass, this question was in the exam. Dated 31/12/22
Thanks to this site it was by far my most valuable
upvoted 3 times

You are moving an application that uses MySQL from on-premises to Google Cloud. The application will run on Compute Engine and will use Cloud SQL. You want to cut over to the Compute Engine deployment of the application with minimal downtime and no data loss to your customers. You want to migrate the application with minimal modification. You also need to determine the cutover strategy. What should you do?

- A. 1. Set up Cloud VPN to provide private network connectivity between the Compute Engine application and the on-premises MySQL server. 2. Stop the on-premises application. 3. Create a mysqldump of the on-premises MySQL server. 4. Upload the dump to a Cloud Storage bucket. 5. Import the dump into Cloud SQL. 6. Modify the source code of the application to write queries to both databases and read from its local database. 7. Start the Compute Engine application. 8. Stop the on-premises application.
- B. 1. Set up Cloud SQL proxy and MySQL proxy. 2. Create a mysqldump of the on-premises MySQL server. 3. Upload the dump to a Cloud Storage bucket. 4. Import the dump into Cloud SQL. 5. Stop the on-premises application. 6. Start the Compute Engine application.
- C. 1. Set up Cloud VPN to provide private network connectivity between the Compute Engine application and the on-premises MySQL server. 2. Stop the on-premises application. 3. Start the Compute Engine application, configured to read and write to the on-premises MySQL server. 4. Create the replication configuration in Cloud SQL. 5. Configure the source database server to accept connections from the Cloud SQL replica. 6. Finalize the Cloud SQL replica configuration. 7. When replication has been completed, stop the Compute Engine application. 8. Promote the Cloud SQL replica to a standalone instance. 9. Restart the Compute Engine application, configured to read and write to the Cloud SQL standalone instance.
- D. 1. Stop the on-premises application. 2. Create a mysqldump of the on-premises MySQL server. 3. Upload the dump to a Cloud Storage bucket. 4. Import the dump into Cloud SQL. 5. Start the application on Compute Engine.

 **victory108** Highly Voted 2 years, 11 months ago

C. 1. Set up Cloud VPN to provide private network connectivity between the Compute Engine application and the on-premises MySQL server. Stop the on-premises application. 3. Start the Compute Engine application, configured to read and write to the on-premises MySQL server. 4. Create the replication configuration in Cloud SQL. 5. Configure the source database server to accept connections from the Cloud SQL replica. Finalize the Cloud SQL replica configuration. 7. When replication has been completed, stop the Compute Engine application. 8. Promote the Cloud SQL replica to a standalone instance. 9. Restart the Compute Engine application, configured to read and write to the Cloud SQL standalone instance.

upvoted 33 times

 **don_v** 5 months ago

Agree with C.

The only confusing is step "5. Configure the source database server to accept connections from the Cloud SQL replica."

Is that not replication should go in the opposite direction from the on-premise (a.k.a. "source") database to Cloud SQL replica (presuming the latter is configured with a public IP address)?

upvoted 1 times

 **kopper2019** Highly Voted 2 years, 11 months ago

Ans C, from this guy muhasinem

External replica promotion migration

In the migration strategy of external replica promotion, you create an external database replica and synchronize the existing data to that replica. This can happen with minimal downtime to the existing database.

When you have a replica database, the two databases have different roles that are referred to in this document as primary and replica. After the data is synchronized, you promote the replica to be the primary in order to move the management layer with minimal impact to database uptime.

In Cloud SQL, an easy way to accomplish the external replica promotion is to use the automated migration workflow. This process automates many of the steps that are needed for this type of migration.

upvoted 20 times

 **de1001c** Most Recent 1 week, 4 days ago

Selected Answer: C

Minimal downtime. Downtime in A is time to take mysql dump + fix potential failures, not good. Downtime in C is just the time from restart the service.

upvoted 1 times

🗲️ 👤 **Gino17m** 2 months ago

Selected Answer: C

I wonder how Examtopics determines the so-called "Correct Answer" C is correct
upvoted 1 times

🗲️ 👤 **heretolearnazure** 9 months, 3 weeks ago

Answer is C
upvoted 1 times

🗲️ 👤 **aliounegdiop** 1 year ago

B is the correct answ
upvoted 2 times

🗲️ 👤 **BiddlyBdoynng** 1 year, 1 month ago

Option A, writing to two databases form the app :(
Option C all the way, it also aligns to GCP Data Migration Service.
upvoted 2 times

🗲️ 👤 **DRK8109** 1 year, 2 months ago

mysql dump always causes long downtime.
upvoted 4 times

🗲️ 👤 **musumusu** 1 year, 2 months ago

Correct Answer A
C is unnecceory expensive and loss of data at after step 3
upvoted 2 times

🗲️ 👤 **BeCalm** 1 year, 3 months ago

C seems to be the best answer but it is still a bit confusing.

So basically there's a bi-directional sync between the 2 databases? Cloud instance is the primary and is writing into the on-prem and on-prem being replicated into the Cloud.

upvoted 2 times

🗲️ 👤 **NodummyIQ** 1 year, 5 months ago

Option C is not the correct answer because it involves modifying the application to read and write to both the on-premises MySQL server and Cloud SQL, which would involve significant modification to the application and could introduce potential complications or errors. It is generally better to minimize modification to the application when performing a migration. Option D, on the other hand, involves simply importing a mysqldump of the on-premises MySQL server into Cloud SQL and starting the application on Compute Engine, which is a simpler and more straightforward approach that involves minimal modification to the application.

upvoted 2 times

🗲️ 👤 **SureshbabuK** 1 year, 5 months ago

Selected Answer: C

Examtopic providing A as correct answer is causing confusion,
upvoted 6 times

🗲️ 👤 **Jose56** 1 year, 6 months ago

Selected Answer: C

C for minimal downtime
upvoted 2 times

🗲️ 👤 **megumin** 1 year, 7 months ago

Selected Answer: C

C is ok
upvoted 1 times

🗲️ 👤 **zr79** 1 year, 8 months ago

Answer is C
we have a new service <https://cloud.google.com/database-migration>
upvoted 7 times

 **minmin2020** 1 year, 8 months ago

Selected Answer: C

C because it has minimal modification to the application or database. Also it's easier to fail back to the original solution if the cloud implementation has issues (assuming that there will be a "post-go-live" monitoring period).

upvoted 2 times

 **minmin2020** 1 year, 8 months ago

C because it has minimal modification to the application or database. Also it's easier to fail back to the original solution if the cloud implementation has issues (assuming that there will be a "post-go-live" monitoring period).

upvoted 1 times

Question #113

Topic 1

Your organization has decided to restrict the use of external IP addresses on instances to only approved instances. You want to enforce this requirement across all of your Virtual Private Clouds (VPCs). What should you do?

- A. Remove the default route on all VPCs. Move all approved instances into a new subnet that has a default route to an internet gateway.
- B. Create a new VPC in custom mode. Create a new subnet for the approved instances, and set a default route to the internet gateway on this new subnet.
- C. Implement a Cloud NAT solution to remove the need for external IP addresses entirely.
- D. Set an Organization Policy with a constraint on constraints/compute.vmExternalIpAccess. List the approved instances in the allowedValues list.

 **victory108** **Highly Voted** 2 years, 11 months ago

D. Set an Organization Policy with a constraint on constraints/compute.vmExternalIpAccess. List the approved instances in the allowedValues list.

upvoted 24 times

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

Ans - D, <https://cloud.google.com/compute/docs/ip-addresses/reserve-static-external-ip-address#disableexternalip>

you might want to restrict external IP address so that only specific VM instances can use them. This option can help to prevent data exfiltration maintain network isolation. Using an Organization Policy, you can restrict external IP addresses to specific VM instances with constraints to control use of external IP addresses for your VM instances within an organization or a project.

upvoted 19 times

 **james2033** **Most Recent** 3 weeks ago

Selected Answer: D

<https://cloud.google.com/compute/docs/ip-addresses/configure-static-external-ip-address#disableexternalip>

upvoted 1 times

 **odacir** 3 months, 3 weeks ago

"You cannot apply the constraint retroactively. All VMs that have external IP addresses before you enable the policy retain their external IP addresses."

<https://cloud.google.com/compute/docs/ip-addresses/reserve-static-external-ip-address#disableexternalip>

It shouldn't be option D then

upvoted 1 times

- 🗳️ 👤 **beehive** 1 year, 5 months ago
D is correct one.
<https://cloud.google.com/compute/docs/ip-addresses/reserve-static-external-ip-address#disableexternalip>
upvoted 3 times
- 🗳️ 👤 **rascalbrick** 1 year, 6 months ago
Show on my Exam,unfortunatekt im failed...:(
upvoted 2 times
- 🗳️ 👤 **megumin** 1 year, 7 months ago
Selected Answer: D
D is ok
upvoted 1 times
- 🗳️ 👤 **AzureDP900** 1 year, 8 months ago
D is correct
upvoted 1 times
- 🗳️ 👤 **2M** 1 year, 9 months ago
Selected Answer: D
option D
upvoted 2 times
- 🗳️ 👤 **ACE_ASPIRE** 1 year, 10 months ago
I got this question in exam.
upvoted 2 times
- 🗳️ 👤 **Sur_Nikki** 1 year, 1 month ago
Answer pleaase
upvoted 1 times
- 🗳️ 👤 **AzureDP900** 1 year, 11 months ago
D is right. constraints/compute.vmExternalIpAccess
upvoted 1 times
- 🗳️ 👤 **JoeyCASD** 2 years, 1 month ago
vote for D
<https://cloud.google.com/compute/docs/ip-addresses/reserve-static-external-ip-address#disableexternalip>
upvoted 2 times
- 🗳️ 👤 **ss909098** 2 years, 3 months ago
Selected Answer: D
D it is
upvoted 1 times
- 🗳️ 👤 **[Removed]** 2 years, 4 months ago
Selected Answer: D
I got similar question on my exam. Answered D.
upvoted 3 times
- 🗳️ 👤 **technodev** 2 years, 5 months ago
Got this question in my exam, answered D
upvoted 2 times
- 🗳️ 👤 **haroldbenites** 2 years, 6 months ago
Go for D.
<https://cloud.google.com/compute/docs/ip-addresses/reserve-static-external-ip-address#disableexternalip>
upvoted 2 times
- 🗳️ 👤 **vincy2202** 2 years, 6 months ago
D is the correct answer
<https://cloud.google.com/compute/docs/ip-addresses/reserve-static-external-ip-address#disableexternalip>
upvoted 1 times

Question #114

Topic 1

Your company uses the Firewall Insights feature in the Google Network Intelligence Center. You have several firewall rules applied to Compute Engine instances.

You need to evaluate the efficiency of the applied firewall ruleset. When you bring up the Firewall Insights page in the Google Cloud Console, you notice that there are no log rows to display. What should you do to troubleshoot the issue?

- A. Enable Virtual Private Cloud (VPC) flow logging.
- B. Enable Firewall Rules Logging for the firewall rules you want to monitor.
- C. Verify that your user account is assigned the compute.networkAdmin Identity and Access Management (IAM) role.
- D. Install the Google Cloud SDK, and verify that there are no Firewall logs in the command line output.

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

Answer is B

when you create a firewall rule there is an option for firewall rule logging on/off. It is set to off by default.

To get firewall insights or view the logs for a specific firewall rule you need to enable logging while creating the rule or you can enable it by editing that rule.

<https://cloud.google.com/network-intelligence-center/docs/firewall-insights/how-to/using-firewall-insights#enabling-fw-rules-logging>

upvoted 35 times

  **victory108** Highly Voted 3 years, 5 months ago

B. Enable Firewall Rules Logging for the firewall rules you want to monitor.

upvoted 15 times

  **GlebG** Most Recent 5 months ago

First D, then B



upvoted 1 times

  **Gino17m** 8 months ago

Selected Answer: B

Corrent answer is B

upvoted 2 times

  **RVivek** 1 year, 10 months ago

Selected Answer: B

<https://cloud.google.com/vpc/docs/firewall-rules-logging>

upvoted 1 times

  **windsor_43** 1 year, 11 months ago

The Answer is B

Just had my exam today with a pass, this question was in the exam. Dated 31/12/22

Thanks to this site it was by far my most valuable

upvoted 5 times

  **jay9114** 1 year, 12 months ago

Selected Answer: B

You have to enable logging for a firewall rule in order to see the rows.

"When you enable logging for a firewall rule, Google Cloud creates an entry called a connection record each time the rule allows or denies traffic."

<https://cloud.google.com/vpc/docs/firewall-rules-logging>

upvoted 1 times

- 🗲️ 👤 **megumin** 2 years, 1 month ago
Selected Answer: B
B is ok
upvoted 1 times
- 🗲️ 👤 **minmin2020** 2 years, 2 months ago
Selected Answer: B
B. Enable Firewall Rules Logging for the firewall rules you want to monitor.
upvoted 1 times
- 🗲️ 👤 **AzureDP900** 2 years, 2 months ago
Enable firewall rules logging , B is right
upvoted 1 times
- 🗲️ 👤 **DrishaS4** 2 years, 4 months ago
Selected Answer: B
<https://cloud.google.com/network-intelligence-center/docs/firewall-insights/how-to/using-firewall-insights#enabling-fw-rules-logging>
upvoted 2 times
- 🗲️ 👤 **AzureDP900** 2 years, 5 months ago
B is most appropriate answer, I will choose B.
upvoted 1 times
- 🗲️ 👤 **AzureDP900** 2 years, 5 months ago
<https://cloud.google.com/vpc/docs/firewall-rules-logging>
upvoted 1 times
- 🗲️ 👤 **tannV** 2 years, 7 months ago
Answered B. Got this question!
upvoted 2 times
- 🗲️ 👤 **azureaspirant** 2 years, 10 months ago
02/15/21 exam
upvoted 1 times
- 🗲️ 👤 **haroldbenites** 3 years ago
Go for B
upvoted 1 times
- 🗲️ 👤 **vincy2202** 3 years ago
B is the correct answer
<https://cloud.google.com/network-intelligence-center/docs/firewall-insights/how-to/using-firewall-insights>
upvoted 1 times
- 🗲️ 👤 **pakilodi** 3 years ago
Selected Answer: B
B is the answer here
upvoted 1 times

Your company has sensitive data in Cloud Storage buckets. Data analysts have Identity Access Management (IAM) permissions to read the buckets. You want to prevent data analysts from retrieving the data in the buckets from outside the office network. What should you do?

- A. 1. Create a VPC Service Controls perimeter that includes the projects with the buckets. 2. Create an access level with the CIDR of the office network.
- B. 1. Create a firewall rule for all instances in the Virtual Private Cloud (VPC) network for source range. 2. Use the Classless Inter-domain Routing (CIDR) of the office network.
- C. 1. Create a Cloud Function to remove IAM permissions from the buckets, and another Cloud Function to add IAM permissions to the buckets. 2. Schedule the Cloud Functions with Cloud Scheduler to add permissions at the start of business and remove permissions at the end of business.
- D. 1. Create a Cloud VPN to the office network. 2. Configure Private Google Access for on-premises hosts.

  **TotoroChina** Highly Voted 2 years, 11 months ago

Should be A.

For all Google Cloud services secured with VPC Service Controls, you can ensure that:

Resources within a perimeter are accessed only from clients within authorized VPC networks using Private Google Access with either Google Cloud or on-premises.


<https://cloud.google.com/vpc-service-controls/docs/overview>

upvoted 71 times

  **ArtistS** 7 months ago

Enforce a security perimeter with VPC Service Controls to isolate resources of multi-tenant Google Cloud services—reducing the risk of data exfiltration or data breach.



upvoted 1 times

  **poseidon24** 2 years, 10 months ago

Correct, this is about data exfiltration.

See: <https://youtu.be/EXwJFL24QzY>

upvoted 14 times

  **Sivanaga** 1 year, 9 months ago

nice one, thank you man

upvoted 2 times

  **mv2000** 1 year, 11 months ago

Thanks for including the youtube video it was very helpful

upvoted 1 times

  **XDevX** Highly Voted 2 years, 11 months ago

IMHO c is wrong - the question is not to restrict access only for business hours but to restrict access to office network.

In my opinion the only realistic approach seems to be a)

https://cloud.google.com/vpc-service-controls/docs/supported-products#table_storage

upvoted 17 times

  **19040e5** Most Recent 4 weeks ago

Selected Answer: A

It's obviously A.

C mentions office hours which has nothing to do with the question!

upvoted 1 times

  **Gino17m** 2 months ago

Selected Answer: A

A is correct answer. Examtopics should change so-called "Correct Answer" from C to A to stop confusing users.

upvoted 2 times

🗨️ 👤 **kalyan_krishna742020** 2 months, 1 week ago

I'm preparing for a test and see that questions from 115 onwards are considered valid. Can anyone who's taken the test offer any insights or advice? Thank you!

upvoted 1 times

🗨️ 👤 **discuss24** 5 months, 2 weeks ago

A is the correct answer. The question is specific to accessing the data outside of the office network. If the question talked about outside of work business hours then, we can consider C

upvoted 1 times

🗨️ 👤 **JPA210** 8 months, 1 week ago

How can be possible that Examtopics say that the correct answer is C?! It doesn't make any sense! A is the correct one.

upvoted 2 times

🗨️ 👤 **heretolearnazure** 9 months, 3 weeks ago

A is correct answer

upvoted 1 times

🗨️ 👤 **RVivek** 1 year, 4 months ago

Selected Answer: A

<https://cloud.google.com/vpc-service-controls/docs/overview>

upvoted 1 times

🗨️ 👤 **vamgcp** 1 year, 4 months ago

A is correct because, For all Google Cloud services secured with VPC Service Controls, you can ensure that resources within a perimeter are accessed only from clients within authorized VPC networks using Private Google Access with either Google Cloud or on-premises.

upvoted 1 times

🗨️ 👤 **examch** 1 year, 5 months ago

Selected Answer: A

A is the correct answer,

<https://cloud.google.com/vpc-service-controls/docs/overview#isolate>

* A VM within a Virtual Private Cloud (VPC) network that is part of a service perimeter can read from or write to a Cloud Storage bucket in the same perimeter. However, VPC Service Controls doesn't allow VMs within VPC networks that are outside the perimeter to access Cloud Storage buckets that are inside the perimeter.

* A copy operation between two Cloud Storage buckets succeeds if both buckets are in the same service perimeter, but if one of the buckets is outside the perimeter, the copy operation fails.

* VPC Service Controls doesn't allow a VM within a VPC network that is inside a service perimeter to access Cloud Storage buckets that are outside the perimeter.

upvoted 4 times

🗨️ 👤 **thamaster** 1 year, 5 months ago

Selected Answer: A

answer C will not prevent connection from outside of office network

upvoted 1 times

🗨️ 👤 **cshubham173** 1 year, 6 months ago

Selected Answer: A

For all Google Cloud services secured with VPC Service Controls, you can ensure that:

Resources within a perimeter are accessed only from clients within authorized VPC networks using Private Google Access with either Google Cloud or on-premises.

<https://cloud.google.com/vpc-service-controls/docs/overview>

upvoted 2 times

🗨️ 👤 **megumin** 1 year, 7 months ago

Selected Answer: A

A is ok

upvoted 1 times



  **minmin2020** 1 year, 8 months ago

Selected Answer: A

- A. Best option
 - B. Not all instances need this restriction
 - C. You are not restricting remote access. The users can still access remotely using their credentials during the business day. The ask is to restrict data retrieval from outside the office network (what if they are working from home...?)
 - D. VPN - too much overhead
- upvoted 1 times

  **minmin2020** 1 year, 8 months ago

- A. Best option
 - B. Not all instances need this restriction
 - C. You are not restricting remote access. The users can still access remotely using their credentials during the business day. The ask is to restrict data retrieval from outside the office network (what if they are working from home...?)
 - D. VPN - too much overhead
- upvoted 2 times

  **kazob** 1 year, 8 months ago

Selected Answer: A

- A for obvious reasons
- upvoted 1 times

Question #116

Topic 1

You have developed a non-critical update to your application that is running in a managed instance group, and have created a new instance template with the update that you want to release. To prevent any possible impact to the application, you don't want to update any running instances. You want any new instances that are created by the managed instance group to contain the new update. What should you do?

- A. Start a new rolling restart operation.
- B. Start a new rolling replace operation.
- C. Start a new rolling update. Select the Proactive update mode.
- D. Start a new rolling update. Select the Opportunistic update mode.

  **XDevX**  3 years, 5 months ago

IMHO the correct answer is d) opportunistic mode, not c) proactive mode.

The requirement is not to update any running instances.

see: <https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups>
For automated rolling updates, you must set the mode to proactive.

Alternatively, if an automated update is potentially too disruptive, you can choose to perform an opportunistic update. The MIG applies an opportunistic update only when you manually initiate the update on selected instances or when new instances are created. New instances can be created when you or another service, such as an autoscaler, resizes the MIG.

upvoted 57 times

  **victory108**  3 years, 5 months ago

- D. Start a new rolling update. Select the Opportunistic update mode.
- upvoted 12 times

🗲️ 👤 **Chang401** Most Recent 2 months, 4 weeks ago

Selected Answer: D

In Google Cloud, the main difference between proactive and opportunistic updates in a managed instance group (MIG) is when they are applied.
 Proactive updates: Automatically apply updates to existing VMs.
 Opportunistic updates: Only apply updates when you manually select a VM to update or when new instances are created.

for all those who think it's C please google and check it's a straightforward question and you guys are confusing people
 upvoted 1 times

🗲️ 👤 **shashii82** 9 months, 1 week ago

Option C. To release a non-critical update to your application without updating any running instances and ensuring that new instances created in the managed instance group contain the new update, you should choose option C: Start a new rolling update and select the Proactive update mode.

In the Proactive update mode, the managed instance group creates new instances with the updated template while keeping the existing instances running until they are eventually replaced. This allows you to roll out the update gradually without affecting the currently running instances.

upvoted 4 times

🗲️ 👤 **kip21** 11 months, 1 week ago

D - Correct

Managed instance groups support two types of update:

Automatic, or proactive, updates

Selective, or opportunistic, updates

If you want to apply updates automatically, set the type to proactive.

Alternatively, if an automated update is potentially too disruptive, you can choose to perform an opportunistic update. The MIG applies an opportunistic update only when you manually initiate the update on selected instances or when new instances are created.

upvoted 3 times

🗲️ 👤 **discuss24** 11 months, 2 weeks ago

D is correct, per Google's documentation (The MIG applies an opportunistic update only when you manually initiate the update on selected instances or when new instances are created. New instances can be created when you or another service, such as an autoscaler, resizes the MIG.)

upvoted 1 times

🗲️ 👤 **[Removed]** 11 months, 3 weeks ago

D

Because the question says: "you don't want to update any running instances. You want any new instances that are created by the managed instance group to contain the new update."

For the above case, we chose opportunistic

Proactive vs Opportunistic:

Proactive: If you want to apply updates automatically, set the type to proactive.

Opportunistic: Alternatively, if an automated update is potentially too disruptive, you can choose to perform an opportunistic update. The MIG applies an opportunistic update only when you manually initiate the update on selected instances or when new instances are created.

<https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups#type>

upvoted 1 times

🗲️ 👤 **spuyol** 1 year ago

Selected answer: D

"To prevent any possible impact to the application, you don't want to update any running instances"

this is automatic achievable only by using opportunistic applying it during autoscale actions as documentation says: if you want to selectively apply a new configuration only to new or to specific instances in a MIG, see Selectively apply VM configuration updates in a MIG

upvoted 2 times

🗨️ 👤 **6b13108** 1 year ago

In my opinion C is correct for Proactive update mode. Considering the following doc; "...Automated updates support up to two instance template versions in your MIG. This means that you can specify two different instance template versions for your group, which is useful for performing canary updates.

To start a basic rolling update where the update is applied to all instances in the group, follow the instructions below...."

See Also:

"Update type

Managed instance groups support two types of update:

Automatic, or proactive, updates

Selective, or opportunistic, updates

If you want to apply updates automatically, set the type to proactive."

https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups#starting_a_basic_rolling_update

upvoted 2 times

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

Selected Answer: C

https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups#starting_a_basic_rolling_update

Automatic (proactive): Use this method if you want the MIG to automatically apply new configurations to all or to a subset of existing VMs in the group. The level of disruption to running VMs depends on the update policy that you configure. You can use this method to canary update new instance templates. To use this method, set the MIG's update type to "proactive".

Selective (opportunistic): Use this method if you want to apply the update manually or if you want to update all existing VMs in the group at once. You target any or all VMs to be updated to the latest configuration. To use this method, set the MIG's update type to "opportunistic".

Hence, C

upvoted 3 times

🗨️ 👤 **JPA210** 1 year, 2 months ago

It is option C, with proactive update, you are not updating the running instances, you start new ones with the new configuration template. And stop the old ones, so there is not disruption to the service.

upvoted 2 times

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

Selected Answer: D

To apply an updated configuration to existing VMs, you can set up an automatic update—also known as a proactive update type. The MIG automatically rolls out configuration updates to all or to a subset of the group's VMs.

Alternatively, if an automated update is potentially too disruptive, you can choose to perform an opportunistic update. The MIG applies an opportunistic update only when you manually initiate the update on selected instances or when new instances are created. New instances are created when you or another service, such as an autoscaler, resizes the MIG.

<https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups>

upvoted 2 times

🗨️ 👤 **duzapo** 1 year, 3 months ago

Selected Answer: D

<https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups>

no more explications needed

upvoted 1 times

🗨️ 👤 **jawulya** 1 year, 3 months ago

Selected Answer: D

The key here is "you don't want to update any running instances". Only opportunistic support this.

upvoted 1 times

🗨️ 👤 **heretolearnazure** 1 year, 3 months ago

D is correct

upvoted 1 times

🗨️ **abhi52** 1 year, 4 months ago

Selected Answer: D

Are the people creating these tests retarded? C is correct? how? Correct answer is D

Question #117

Topic 1

Your company is designing its application landscape on Compute Engine. Whenever a zonal outage occurs, the application should be restored in another zone as quickly as possible with the latest application data. You need to design the solution to meet this requirement. What should you do?

- A. Create a snapshot schedule for the disk containing the application data. Whenever a zonal outage occurs, use the latest snapshot to restore the disk in the same zone.
- B. Configure the Compute Engine instances with an instance template for the application, and use a regional persistent disk for the application data. Whenever a zonal outage occurs, use the instance template to spin up the application in another zone in the same region. Use the regional persistent disk for the application data.
- C. Create a snapshot schedule for the disk containing the application data. Whenever a zonal outage occurs, use the latest snapshot to restore the disk in another zone within the same region.
- D. Configure the Compute Engine instances with an instance template for the application, and use a regional persistent disk for the application data. Whenever a zonal outage occurs, use the instance template to spin up the application in another region. Use the regional persistent disk for the application data.

🗨️ **TotoroChina** **Highly Voted** 👍 2 years, 11 months ago

Answer is B, it only request zonal resiliency.

Regional persistent disk is a storage option that provides synchronous replication of data between two zones in a region. Regional persistent disks can be a good building block to use when you implement HA services in Compute Engine.

<https://cloud.google.com/compute/docs/disks/high-availability-regional-persistent-disk>
upvoted 50 times

🗨️ **AmitRBS** 2 years ago

B. Agree, clearly it's B. Focus on keyword "zone"
upvoted 4 times

🗨️ **Ssoumya** **Highly Voted** 👍 2 years, 11 months ago

Answer is B
upvoted 14 times

🗨️ **oscarcampos** **Most Recent** 🕒 1 month, 3 weeks ago

why D ?
upvoted 1 times

🗨️ **mesodan** 3 months, 2 weeks ago

Selected Answer: B

It is B. As for D: Spinning up the application in another region might be too geographically distant, leading to higher latency and potential issues.
upvoted 1 times

🗨️ **hzaoui** 4 months, 4 weeks ago

Selected Answer: B

A regional persistent disk is designed to provide synchronous replication of data between two zones in the same region, ensuring that data remains available even if one zone is affected by an outage. By using an instance template along with a regional disk, you can quickly create new instances in an available zone during a zonal outage and attach the regional persistent disk to continue operations with the latest application data.

upvoted 1 times

🗨️ 👤 **SSS987** 5 months ago

Can someone explain why not C - snapshot?

upvoted 1 times

🗨️ 👤 **xaqanik** 4 months, 2 weeks ago

B - uses instance template which is ready for deploy. Option C requires manual configuration and this may take more time . But we need a quickly as possible .

upvoted 1 times

🗨️ 👤 **thewalker** 7 months, 1 week ago

Selected Answer: D

Option D suggests using the same approach as Option B but restoring the application in another region instead of the same region. This approach provides high availability and disaster recovery across regions, making it suitable for applications that require high RTOs and minim data loss.

upvoted 1 times

🗨️ 👤 **convers39** 5 months, 2 weeks ago

can you use the regional persistent disk in a different region?

upvoted 3 times

🗨️ 👤 **don_v** 5 months ago

apparently, nope.

upvoted 1 times

🗨️ 👤 **JPA210** 8 months, 1 week ago

Of course it is answer B. I would like to understand who chooses the right answers in examtopics! Choosing here option D is completely wror This takes people less instructed to be mistaken.

upvoted 2 times

🗨️ 👤 **AdityaGupta** 8 months, 2 weeks ago

Selected Answer: B

B. Configure the Compute Engine instances with an instance template for the application, and use a regional persistent disk for the applicatio data. Whenever a zonal outage occurs, use the instance template to spin up the application in another zone in the same region. Use the regio persistent disk for the application data. Most Voted

Why to change the region as mentioned in Option D, when the ask is different zone only.

upvoted 1 times

🗨️ 👤 **duzapo** 9 months, 2 weeks ago

Selected Answer: B

Answer is B, it only request zonal resiliency

upvoted 1 times

🗨️ 👤 **heretolearnazure** 9 months, 3 weeks ago

It says restore in a zonal. Hence answer is B.

upvoted 1 times

🗨️ 👤 **mifrah** 1 year, 2 months ago

B. In my opinion, I cannot use a regional disk in a different region!!! So, it can only be another zone in the same region. Therefore D must be wrong!

upvoted 2 times

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

Answer B is Correct - since it talks about spin up application in different zone but same region.

Whereas,D is incoorect , since its talking about spin up application in different region which is not our requirement.

upvoted 1 times

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

If it is a regional persistent disk created in region A for example. If I start the compute engine instance in the region B, how am I going to use a regional disk from region A (another region)? I do not think it is possible. So answer D should be excluded.

I do believe that the correct answer is B.

upvoted 2 times

🗨️ 👤 **windsor_43** 1 year, 5 months ago

The Answer is B

Just had my exam today with a pass, this question was in the exam. Dated 31/12/22
Thanks to this site it was by far my most valuable
upvoted 5 times

🗨️ 👤 **rascalbrick** 1 year, 6 months ago

14/12/22 Exam, but IM failed :(
upvoted 1 times

🗨️ 👤 **Praveen_G** 1 year, 5 months ago

Tomorrow 12/27/22 is my exam :)
upvoted 2 times

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

How was it?
upvoted 1 times

🗨️ 👤 **megumin** 1 year, 7 months ago

Selected Answer: B

B is ok
upvoted 1 times

Question #118

Topic 1

Your company has just acquired another company, and you have been asked to integrate their existing Google Cloud environment into your company's data center. Upon investigation, you discover that some of the RFC 1918 IP ranges being used in the new company's Virtual Private Cloud (VPC) overlap with your data center IP space. What should you do to enable connectivity and make sure that there are no routing conflicts when connectivity is established?

- A. Create a Cloud VPN connection from the new VPC to the data center, create a Cloud Router, and apply new IP addresses so there is no overlapping IP space.
- B. Create a Cloud VPN connection from the new VPC to the data center, and create a Cloud NAT instance to perform NAT on the overlapping IP space.
- C. Create a Cloud VPN connection from the new VPC to the data center, create a Cloud Router, and apply a custom route advertisement to block the overlapping IP space.
- D. Create a Cloud VPN connection from the new VPC to the data center, and apply a firewall rule that blocks the overlapping IP space.

🗨️ 👤 **VishalB** Highly Voted 👍 3 years, 4 months ago

Correct Answer: A
- IP Should not overlap so applying new IP address is the solution
upvoted 42 times

🗨️ 👤 **zanfo** 2 years, 9 months ago

A is not correct. "What should you do to enable connectivity and make sure that there are no routing conflicts when connectivity is established?" if you apply VPN con BGP, the actual IP address will be propagated to on prem environment with overlapping RFC1918 as result. B is correct with custom route
upvoted 7 times

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

Answer is C.



<https://cloud.google.com/network-connectivity/docs/router/how-to/advertising-custom-ip>

upvoted 36 times

  **meh009** 3 years, 2 months ago

The Q states to establish connectivity. This would merely prevent that. Ans is A

upvoted 5 times

  **don_v** 11 months, 1 week ago

I would also agree with C.

Still, this part is confusing: "C. Create a Cloud VPN connection from the new VPC to the data center, create a Cloud Router, and apply a custom route advertisement to *block* the overlapping IP space."

To *block*? Not to block. just to alias with advertised IP addresses.



upvoted 2 times

  **RKS_2021** 3 years, 5 months ago

ANS is B

<https://cloud.google.com/architecture/best-practices-vpc-design>

upvoted 8 times

  **imgcp** 3 years, 4 months ago

B is NOT correct. Cloud NAT is specifically used for translating the IP address of the outbound packets destined to the Internet. But this question is about using VPN communication between two private IP address spaces (RFC1918). Cloud NAT cannot achieve the purpose here, you can't use Cloud NAT to translate from one private IP to another private ip. I would vote for C.

upvoted 13 times

  **dija123** 8 months ago

You can use private or hybrid NAT

<https://cloud.google.com/nat/docs/overview#private-nat>

upvoted 2 times

  **Bill831231** 3 years, 2 months ago

Thanks for the clarification, just one question, without a solution like NAT or reip, the service on the devices with overlapping IP subnets will be unavailable for on-premise devices, not sure if the question also about this

upvoted 1 times

  **RKS_2021** 1 year, 2 months ago

It will be a NAT Router instance, which will route the traffic. I have practically applied the configuration.

upvoted 2 times

  **elenamatay** 2 years, 11 months ago

You can't use Cloud NAT according to this documentation: <https://cloud.google.com/nat/docs/troubleshooting#overlapping-ip-address>

"Can I use Cloud NAT to connect a VPC network to another network to work around overlapping IP addresses? No, Cloud NAT cannot apply to any custom route whose next hop is not the default internet gateway. For example, Cloud NAT cannot apply to traffic sent to a next hop Cloud VPN tunnel, even if the destination is a publicly routable IP address."

upvoted 16 times

  **andreacola** Most Recent 1 month, 2 weeks ago

Selected Answer: B

Assume that the resources in your VPC network need to communicate with the resources in a VPC network or an on-premises or other cloud provider network that is owned by a different business unit. However, that network contains subnets whose IP addresses overlap with the IP addresses of your VPC network. In this scenario, you create a Private NAT gateway that translates traffic between the subnets in your VPC network to the non-overlapping subnets of the other network.

upvoted 5 times