**odacir** 7 months ago

**Selected Answer: B**

https://cloud.google.com/storage/docs/encryption/customer-managed-keys#key-rotation

upvoted 1 times

**vc1011** 8 months, 1 week ago

**Selected Answer: B**

The following restrictions apply when using customer-managed encryption keys:

You cannot encrypt an object with a customer-managed encryption key by updating the object's metadata. Include the key as part of a rewrit the object instead.

gcloud storage uses the objects update command to set encryption keys on objects, but the command rewrites the object as part of the requ this makes rotating keys difficult

upvoted 2 times

**someone2011** 9 months, 3 weeks ago

Probably B:
https://cloud.google.com/storage/docs/encryption/customer-managed-keys#key-replacement

upvoted 1 times

**BiddlyBdoyng** 1 year ago

It says customer wants to manage the rotation not the supplying of key. Hence B not D. Seen some people say with customer managed you cannot rotate but this document suggests you can https://cloud.google.com/storage/docs/encryption/customer-managed-keys#key-rotation.

upvoted 1 times

**jlambdan** 1 year, 2 months ago

B does not allow to rotate assymetric key.
https://cloud.google.com/kms/docs/key-rotation
=> Cloud Key Management Service does not support automatic rotation of asymmetric keys. See Considerations for asymmetric keys below.

I go for D.

upvoted 1 times

**medi01** 1 year, 1 month ago

GC uses symmetric key.

upvoted 1 times

**JC0926** 1 year, 2 months ago

**Selected Answer: B**

B. Create a key with Cloud Key Management Service (KMS). Set the encryption key on the bucket to the Cloud KMS key.

To rotate the encryption key used to encrypt data in a Cloud Storage bucket, it is recommended to use Cloud KMS. You can create a new key version, set it as the primary version, and update the bucket's default KMS key to the new key version. This allows you to rotate the encryptio key while still allowing access to the data. You can then process the data in Dataproc while the encryption key is being rotated. This approach provides security and compliance with regulations, as well as easy key rotation without disrupting access to data.

upvoted 4 times

**JC0926** 1 year, 2 months ago

**Selected Answer: B**

Your organization has stored sensitive data in a Cloud Storage bucket. For regulatory reasons, your company must be able to rotate the encryption key used to encrypt the data in the bucket. The data will be processed in Dataproc. You want to follow Google-recommended practices for security. What should you do?
A. Create a key with Cloud Key Management Service (KMS). Encrypt the data using the encrypt method of Cloud KMS.
B. Create a key with Cloud Key Management Service (KMS). Set the encryption key on the bucket to the Cloud KMS key.
C. Generate a GPG key pair. Encrypt the data using the GPG key. Upload the encrypted data to the bucket.
D. Generate an AES-256 encryption key. Encrypt the data in the bucket using the customer-supplied encryption keys feature.

upvoted 1 times

**examch** 1 year, 5 months ago

**Selected Answer: B**

B is the correct answer, we can encrypt the data in the bucket using CMEK. And the key can be rotated as per requirement.
https://cloud.google.com/storage/docs/encryption/using-customer-managed-keys#add-object-key

https://cloud.google.com/storage/docs/samples/storage-rotate-encryption-key#storage_rotate_encryption_key-python

upvoted 1 times

**nhorcajada** 1 year, 7 months ago

**Selected Answer: C**

B is ok

upvoted 1 times

**megumin** 1 year, 7 months ago

**Selected Answer: B**

B is ok

upvoted 1 times

**KongsMom** 1 year, 7 months ago

B. rotation and dataproc ... trendmicro talk about this in https://www.trendmicro.com/cloudoneconformity/knowledge-base/gcp/Dataproc/enable-encryption-with-cmks-for-dataproc-clusters.html

Ensure that your Google Cloud Dataproc clusters on Compute Engine are encrypted with Customer-Managed Keys (CMKs) in order to contro cluster data encryption/decryption process. You can create and manage your own Customer-Managed Keys (CMKs) with Cloud Key Management Service (Cloud KMS). Cloud KMS provides secure and efficient encryption key management, controlled key rotation, and revoca mechanisms.
This rule resolution is part of the Conformity Security & Compliance tool for GCP.

upvoted 1 times

**RitwickKumar** 1 year, 10 months ago

**Selected Answer: B**

As per question: " your company must be able to rotate the encryption key"
It is easily possible with KMS: https://cloud.google.com/kms/docs/rotating-keys#kms-create-key-rotation-schedule-gcloud

upvoted 3 times

**Ric350** 1 year, 10 months ago

"Your company must be able to rotate the encryption key" is the requirement which eliminates CMEK and why you need a CSEK. You have to use a boto config file to do this and is part of one of the labs.

upvoted 2 times

Question #150 *Topic 1*

Your team needs to create a Google Kubernetes Engine (GKE) cluster to host a newly built application that requires access to third-party services on the internet.
Your company does not allow any Compute Engine instance to have a public IP address on Google Cloud. You need to create a deployment strategy that adheres to these guidelines. What should you do?

A. Configure the GKE cluster as a private cluster, and configure Cloud NAT Gateway for the cluster subnet.

B. Configure the GKE cluster as a private cluster. Configure Private Google Access on the Virtual Private Cloud (VPC).

C. Configure the GKE cluster as a route-based cluster. Configure Private Google Access on the Virtual Private Cloud (VPC).

D. Create a Compute Engine instance, and install a NAT Proxy on the instance. Configure all workloads on GKE to pass through this proxy to access third-party services on the Internet.

**ACE_ASPIRE** Highly Voted 3 years, 3 months ago

Cloud NAT is the correct answer

upvoted 32 times

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

Selected Answer: A

** Admins: More than 60% of the answers you have selected are wrong. Please correct them ASAP. I must appreciate community here for taki out time to share their perspective and help fellow learners.

"B" can never be an answer here as the Private Google Access enables internal access to Google APIs only whereas in question the ask is "access to third-party services on the internet"

upvoted 26 times

**ArtistS** 1 year, 1 month ago

If they provide the correct answer, you will never see this website any more

upvoted 7 times

**Sephethus** 6 months ago

True, but then if it were shut down literally nobody could pass this ridiculous test where half the questions are so badly worded and confusing with debatable options.

upvoted 2 times

**jlambdan** 1 year, 8 months ago

This is most likely on purpose. Otherwise google will do something in order for the exam dump to be shutdown.

upvoted 13 times

**19040e5** Most Recent 7 months ago

Selected Answer: A

Cloud NAT, Private Service Connect is for Google API Access.

upvoted 1 times

**kahinah** 9 months, 1 week ago

Selected Answer: A

Cloud NAT to access to the internet

upvoted 1 times

**didek1986** 11 months ago

Selected Answer: A

It is A

upvoted 1 times

**techtitan** 1 year ago

Selected Answer: A

Needs Nat to connect to 3rd party apps

upvoted 1 times

**6b13108** 1 year ago

B is only part of the solution, but needs Cloud Nat to get access on the internet with third-party services, then the correct answer is A . See d https://cloud.google.com/kubernetes-engine/docs/concepts/private-cluster-concept

upvoted 1 times

**tamj123** 1 year, 2 months ago

Selected Answer: A

go for Cloud NAT

upvoted 1 times

**RaviRS** 1 year, 3 months ago

Selected Answer: A

I am not sure who's writing these answers
Private Google Access is useful for allowing Google Cloud resources, including GKE clusters, to access Google services without public IPs, b doesn't provide access to third-party services on the internet.

upvoted 2 times

**[Removed]** 1 year, 5 months ago

Selected Answer: A

Cloud NAT A

upvoted 1 times

**DS2023** 1 year, 6 months ago

Selected Answer: A

Cloud NAT allows the resources in private subnet to access the internet—for updates, patching, config management, and more—in a controll and efficient manner.

upvoted 1 times

**LaxmanTiwari** 1 year, 6 months ago

Yeah agree as GKE admin

upvoted 1 times

**DS2023** 1 year, 6 months ago

Selected Answer: A. Cloud NAT allows the resources in private subnet to access the internet—for updates, patching, config management, an more—in a controlled and efficient manner.

upvoted 1 times

**dbsmk** 1 year, 8 months ago

A.

https://cloud.google.com/kubernetes-engine/docs/how-to/private-clusters#workloads_on_private_clusters_unable_to_access_internet

upvoted 3 times

**JC0926** 1 year, 9 months ago

Selected Answer: B

Private Google Access allows resources in a VPC network to access Google Cloud services without an external IP address. By configuring th GKE cluster as a private cluster, the nodes and services inside the cluster will not have a public IP address, and only resources within the VPC network will be able to communicate with them. With Private Google Access enabled, the GKE cluster can access third-party services on the internet via Google APIs and services without requiring a public IP address.

Therefore, the correct option is:

B. Configure the GKE cluster as a private cluster. Configure Private Google Access on the Virtual Private Cloud (VPC).

upvoted 1 times

**r1ck** 1 year, 10 months ago

answer should be "B"
https://cloud.google.com/vpc/docs/private-access-options

upvoted 2 times

**examch** 1 year, 11 months ago

Selected Answer: A

A is the correct answer,

Granting private nodes outbound internet access
To provide outbound internet access for your private nodes, such as to pull images from an external registry, use Cloud NAT to create and configure a Cloud Router. Cloud NAT lets private clusters establish outbound connections over the internet to send and receive packets.

The Cloud Router allows all your nodes in the region to use Cloud NAT for all primary and alias IP ranges. It also automatically allocates the external IP addresses for the NAT gateway.

For instructions to create and configure a Cloud Router, refer to Create a Cloud NAT configuration using Cloud Router in the Cloud NAT documentation.

https://cloud.google.com/kubernetes-engine/docs/how-to/private-clusters#private-nodes-outbound

upvoted 3 times

**surajkrishnamurthy** 2 years ago

Selected Answer: A

A is the correct answer

upvoted 2 times

Question #151 *Topic 1*

Your company has a support ticketing solution that uses App Engine Standard. The project that contains the App Engine application already has a Virtual Private
Cloud (VPC) network fully connected to the company's on-premises environment through a Cloud VPN tunnel. You want to enable the App Engine application to communicate with a database that is running in the company's on-premises environment. What should you do?

A. Configure private Google access for on-premises hosts only.

B. Configure private Google access.

C. Configure private services access.

D. Configure serverless VPC access.

**Roncy** Highly Voted 👍 2 years, 2 months ago
D is right , refer to https://cloud.google.com/vpc/docs/serverless-vpc-access#use_cases
upvoted 41 times

> **cloudguy2** 2 years ago
> D) is correct. Use case example: Your serverless environment needs to access data from your on-premises database through Cloud VPN.
> upvoted 10 times

**Besss** Highly Voted 👍 2 years, 3 months ago
D. Configuring serverless VPC access App Engine can connect to the VPC and then through VPN tunnel to the on-prem DB
upvoted 18 times

**PKKim** Most Recent 🕘 3 weeks, 4 days ago
The answer is D.
The option B is for the other way. The option B is for the on-premise services to be able to use Google API through VPN
upvoted 3 times

**theBestStudent** 1 month ago

Selected Answer: D

Answer is D. Here the explanation since I didn't see any good answer:
1- We have a VPC.
2- We have an onpremisses DB.
3- We have App Engine (that runs on a isolated network that does not belong to the VPC).
4- We can connect the VPC to the onpremisses network using Cloud VPN, which is the main purpose of Cloud VPN (let's say to simplify this answer).
5 - Now how we connect the AppEngine that is isolated from the VPC and needs to use "something" to reach out the onpremisses DB directl (no public ip, only private ip)? Here we will have to have somehow access to the VPC and then the VPN and then the on premisses DB. That i the serverless vpc access.
6- So flow can be something like app engine --> serverless vpc access --> cloud VPN ---> on premessises db through private ip.

upvoted 11 times

**odacir** 1 month ago

Selected Answer: D

D:
Use cases
...
Your serverless environment needs to access data from your on-premises database through Cloud VPN.
https://cloud.google.com/vpc/docs/serverless-vpc-access#use_cases

upvoted 1 times

**thewalker** 1 month ago

Selected Answer: D

Read this article: https://cloud.google.com/vpc/docs/serverless-vpc-access
That makes me conclude for D.

upvoted 1 times

**Prakzz** 2 months, 2 weeks ago

It's App Engine Standard and VPN cannot be used with Standard version

upvoted 1 times

**RaviRS** 3 months, 1 week ago

Selected Answer: D

That's the whole purpose of serverless google access

upvoted 1 times

**sampon279** 5 months, 3 weeks ago

Selected Answer: D

Private google service and private google access seem to provide same level of access: https://googlecloudarchitect.us/private-service-acce vs-google-private-access/ Based on elimination both can be eliminated. Hence D.

upvoted 1 times

**natpilot** 8 months ago

D is Right . You can use a Serverless VPC Access connector to let Cloud Run, App Engine standard, and Cloud Functions environments send packets to the internal IPv4 addresses of resources in a VPC network. Serverless VPC Access also supports sending packets to other networ connected to the selected VPC network.

upvoted 3 times

**JC0926** 9 months ago

Selected Answer: D

Private Google Access (option B) is used to enable VM instances in a VPC network to reach Google APIs and services using an internal IP address, but it does not allow communication to on-premises resources.

Private Services Access (option C) allows you to access supported Google Cloud services through private IP addresses rather than public IP addresses, but it does not help in communicating with on-premises resources.

Configuring Private Google Access for on-premises hosts only (option A) is not a valid option as this configuration is not available.

upvoted 6 times

**Mohtasham9** 10 months ago

C. Configure private services access.
To enable an App Engine application to communicate with a database running in the company's on-premises environment over a VPC networ that is fully connected to the company's on-premises environment through a Cloud VPN tunnel, the recommended approach is to use Private Service Access (PSA). Therefore, the correct answer is C. Configure private services access.

Private Service Access (PSA) allows you to create private connections between your VPC network and services like Cloud SQL, Cloud Storag and other Google APIs and services. With PSA, you can access these services using their private IP addresses, which are only accessible fror within your VPC network, and not over the public internet. This provides better security and reduces the risk of data exfiltration or unauthorize access.

upvoted 1 times

**SLChief** 10 months, 1 week ago

D is right. Configuring serverless VPC access is the option for app engine to have Google private access

upvoted 1 times

**[Removed]** 10 months, 2 weeks ago

Selected Answer: D

You can use a Serverless VPC Access connector to let Cloud Run, App Engine standard, and Cloud Functions environments send packets to internal IPv4 addresses of resources in a VPC network. Serverless VPC Access also supports sending packets to other networks connected t the selected VPC network.

https://cloud.google.com/vpc/docs/private-access-options

upvoted 1 times

**jay9114** 10 months, 2 weeks ago

Upvote if there was no mention of "serverless VPC access" in the training videos and study guides you used to prepare for this exam.

upvoted 9 times

**GopeshSahu** 10 months, 4 weeks ago

Selected Answer: B

I am surprised 95% selected option D without understanding the use case. Very basic ask

AppEngine ->Private Google Access->On-Prem DB
Google Private Access to so enable any Services no matter running in VPC to connect to on-prem DB via VPN tunnel.
https://cloud.google.com/vpc/docs/private-google-access-hybrid
https://cloud.google.com/vpc/docs/configure-private-google-access-hybrid

AppEngine -> Serveless-VPV-Access -> Any GCP Resources/Services(with private IPs)

upvoted 3 times

**jake_edman** 10 months, 3 weeks ago

I still think it is D - the example you linked to for Private Google Access is to allow on-prem resources to contact Google Services, not the other way round.
https://cloud.google.com/vpc/docs/private-google-access-hybrid

But the example others link to explicitly says a use case is "Your serverless environment needs to access data from your on-premises database through Cloud VPN
https://cloud.google.com/vpc/docs/serverless-vpc-access#use_cases

upvoted 2 times

**gcppandit** 10 months, 3 weeks ago

Private Google Access provides access to Google Services via Private IP and this can be used to call the App Engine from On-Prem. Here usecase is exactly the opposite. Here only option to set up the Serverless VPC access to allow Serverless components to access Private resources (including on-Prem if proper VPN is already setup)

upvoted 3 times

**examch** 11 months, 2 weeks ago

**Selected Answer: D**

D is the correct answer,

Serverless VPC Access

bookmark_border
Serverless VPC Access makes it possible for you to connect directly to your Virtual Private Cloud network from serverless environments such Cloud Run, App Engine, or Cloud Functions. Configuring Serverless VPC Access allows your serverless environment to send requests to your VPC network using internal DNS and internal IP addresses (as defined by RFC 1918 and RFC 6598). The responses to these requests also us your internal network.

There are two main benefits to using Serverless VPC Access:

Requests sent to your VPC network are never exposed to the internet.
Communication through Serverless VPC Access can have less latency compared to the internet.

https://cloud.google.com/vpc/docs/serverless-vpc-access#use_case

Question #152 *Topic 1*

Your company is planning to upload several important files to Cloud Storage. After the upload is completed, they want to verify that the uploaded content is identical to what they have on-premises. You want to minimize the cost and effort of performing this check. What should you do?

A. 1. Use Linux shasum to compute a digest of files you want to upload. 2. Use gsutil -m to upload all the files to Cloud Storage. 3. Use gsutil cp to download the uploaded files. 4. Use Linux shasum to compute a digest of the downloaded files. 5. Compare the hashes.

B. 1. Use gsutil -m to upload the files to Cloud Storage. 2. Develop a custom Java application that computes CRC32C hashes. 3. Use gsutil ls -L gs://[YOUR_BUCKET_NAME] to collect CRC32C hashes of the uploaded files. 4. Compare the hashes.

C. 1. Use gsutil -m to upload all the files to Cloud Storage. 2. Use gsutil cp to download the uploaded files. 3. Use Linux diff to compare the content of the files.

D. 1. Use gsutil -m to upload the files to Cloud Storage. 2. Use gsutil hash -c FILE_NAME to generate CRC32C hashes of all on-premises files. 3. Use gsutil ls -L gs://[YOUR_BUCKET_NAME] to collect CRC32C hashes of the uploaded files. 4. Compare the hashes.

**vladik820** Highly Voted 2 years, 3 months ago

D is ok .
https://cloud.google.com/storage/docs/gsutil/commands/hash

upvoted 39 times

**Bahubali1988** Highly Voted 1 year, 3 months ago

Seems most of the questions are having wrong answers.. If there is no discussion , its highly difficult to get the right answers.

upvoted 17 times

**tamj123** Most Recent 2 months ago

**Selected Answer: D**

created hash and compare after is way to go.

upvoted 2 times

**RaviRS** 3 months, 1 week ago

**Selected Answer: D**

I am losing faith on the answers given... Option C is downright absurd.

upvoted 1 times

**Jerar** 4 months, 2 weeks ago

**Selected Answer: D**

https://cloud.google.com/storage/docs/gsutil/commands/hash
Calculate hashes on local files, which can be used to compare with gsutil ls -L output.
-c
Calculate a CRC32c hash for the specified files.

upvoted 1 times

**BiddlyBdoyng** 6 months, 1 week ago

Downloading before hashing cannot be right. The upload might be fine but if the download could corrupt

upvoted 1 times

**[Removed]** 7 months ago

The correct answer should be D: https://cloud.google.com/storage/docs/gsutil/commands/hash

upvoted 1 times

**surajkrishnamurthy** 1 year ago

**Selected Answer: D**

D is the correct answer

upvoted 2 times

**megumin** 1 year, 1 month ago

**Selected Answer: D**

D is ok

upvoted 1 times

**Nuwan_SriLanka** 1 year, 1 month ago

**Selected Answer: D**

Calculate hashes on local files, which can be used to compare with gsutil ls -L output. If a specific hash option is not provided, this command calculates all gsutil-supported hashes for the files.

Note that gsutil automatically performs hash validation when uploading or downloading files, so this command is only needed if you want to v a script that separately checks the hash.

If you calculate a CRC32c hash for files without a precompiled crcmod installation, hashing will be very slow. See gsutil help crcmod for detai
https://cloud.google.com/storage/docs/gsutil/commands/hash

upvoted 5 times

**Mahmoud_E** 1 year, 2 months ago

**Selected Answer: D**

D is the right answer per this doc https://cloud.google.com/storage/docs/gsutil/commands/hash

upvoted 1 times

**Jay_Krish** 1 year, 3 months ago

**Selected Answer: C**

All those who answered D.. can one of you if you're genuine tell how is this even possible - The second step in the option D?
2. Use gsutil hash -c FILE_NAME to generate CRC32C hashes of all on-premises files.

upvoted 2 times

> **Jay_Krish** 1 year, 3 months ago
>
> Reading again it's probably not C because it talks about Linux commands but what if the environment is Windows..
> but I still have my doubts on D if someone could clarify?
>
> upvoted 2 times

**binpan** 1 year, 5 months ago

Correct Answer C
A- digest comparison does not gurantee file contents are same. moreover lot of extra steps. - not correct
B - custom Java code - lot of effort - not correct
D - gs util cannot be used for creating hash for on prem files stored on on prem filestore/database. Not correct
C - not the best option but right answer for the options available.

upvoted 2 times

**luamail** 1 year, 2 months ago

dowload file has cost, C no is a option

upvoted 1 times

**SIMMEAT** 1 year, 4 months ago

there is a hash options in gsutil for local files.
https://cloud.google.com/storage/docs/gsutil/commands/hash

upvoted 2 times

**kaito789** 1 year, 4 months ago

D is correct. you only need gs util to generate hash for cloud storage. you would use your own utility to create ash for on prem and then compare the two.

upvoted 1 times

**AzureDP900** 1 year, 5 months ago

D is correct , there is no need to build custom java script.

upvoted 2 times

**Superr** 1 year, 6 months ago

Selected Answer: D

D seems valid

upvoted 1 times

**amxexam** 1 year, 7 months ago

Selected Answer: D

I am eliminating tedious approaches that is downloading and doing custom coding so A B C are eliminated.
D is the solution.

upvoted 1 times

Question #153 *Topic 1*

You have deployed an application on Anthos clusters (formerly Anthos GKE). According to the SRE practices at your company, you need to be alerted if request latency is above a certain threshold for a specified amount of time. What should you do?

A. Install Anthos Service Mesh on your cluster. Use the Google Cloud Console to define a Service Level Objective (SLO), and create an alerting policy based on this SLO.

B. Enable the Cloud Trace API on your project, and use Cloud Monitoring Alerts to send an alert based on the Cloud Trace metrics.

C. Use Cloud Profiler to follow up the request latency. Create a custom metric in Cloud Monitoring based on the results of Cloud Profiler, and create an Alerting policy in case this metric exceeds the threshold.

D. Configure Anthos Config Management on your cluster, and create a yaml file that defines the SLO and alerting policy you want to deploy in your cluster.

**vladik820** Highly Voted 2 years, 3 months ago

A is ok.
https://cloud.google.com/service-mesh/docs/observability/slo-overview

upvoted 24 times

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

Selected Answer: B

"Google Cloud Console to define a Service Level Objective (SLO)" seems odd, B doesn't seem wrong

upvoted 4 times

**tamj123** 2 months ago

Answer A looks correct

upvoted 1 times

**examch** 11 months, 2 weeks ago

Selected Answer: A

Cloud Monitoring can trigger an alert when a Service is on track to violate an SLO. You can create an alerting policy based on the rate of consumption of your error budget. All alerts on error budgets have the same basic condition: a specified percentage of the error budget for th compliance period is consumed in a lookback period, which is a time period, such as the previous 60 minutes. When you create the alerting policy, Anthos Service Mesh automatically sets most of the conditions for the alert based on the settings in the SLO. You specify the lookback period and the consumption percentage.

https://cloud.google.com/service-mesh/docs/observability/alert-policy-slo

upvoted 4 times

**megumin** 1 year, 1 month ago

Selected Answer: A

A is ok

upvoted 2 times

**Jay_Krish** 1 year, 3 months ago

Selected Answer: A

A seems correct

upvoted 2 times

**RitwickKumar** 1 year, 4 months ago

Selected Answer: A

https://cloud.google.com/service-mesh/docs/observability/alert-policy-slo

upvoted 2 times

**igor_nov1** 1 year, 4 months ago

Use the Google Cloud Console to define a Service Level Objective (SLO)
WAAAAT ?
How Console help you to define SLO?

upvoted 1 times

**AMohanty** 1 year, 4 months ago

Specific Purpose of Cloud Trace API is to get info regarding Latency.
Would go with B.

upvoted 2 times

**AzureDP900** 1 year, 5 months ago

A is right

upvoted 1 times

**sivre** 1 year, 8 months ago

Why not B....
Cloud Trace is a distributed tracing system that collects latency data from the applications and displays it in near real-time. It allows you to fol
a sample request through your distributed system, observe the network calls and profile your system end to end.
Note that Cloud Trace is disabled by default.
The Anthos Service Mesh pages provide a link to the traces in the Cloud Trace page in the Cloud Console.
https://cloud.google.com/service-mesh/docs/observability/accessing-traces
In Anthos clusters you need to install Anthos service mesh? From this link you need to install it only on GKE and on-premises platforms
https://cloud.google.com/service-mesh/docs/observability/accessing-traces

upvoted 3 times

**ryzior** 1 year, 6 months ago

I think A is about monitoring and alerting without any further investigation, while Trace is for finding the root cause/detective purposes, whe
you look into a call and track this call step by step through each endpoint, the call is going through.

upvoted 3 times

**kimharsh** 1 year, 6 months ago

Can you create an Alert when you use Cloud Trace?

upvoted 2 times

**Shawnn** 9 months, 1 week ago

yep, you can

upvoted 2 times

**[Removed]** 1 year, 10 months ago

I got same question on my exam.

upvoted 2 times

**haroldbenites** 1 year, 10 months ago

Go for A

upvoted 1 times

**technodev** 1 year, 11 months ago

Got this question in my exam, answered A

upvoted 4 times

**vincy2202** 2 years ago

Question #154 *Topic 1*

Your company has a stateless web API that performs scientific calculations. The web API runs on a single Google Kubernetes Engine (GKE) cluster. The cluster is currently deployed in us-central1. Your company has expanded to offer your API to customers in Asia. You want to reduce the latency for users in Asia.
What should you do?

A. Create a second GKE cluster in asia-southeast1, and expose both APIs using a Service of type LoadBalancer. Add the public IPs to the Cloud DNS zone.

B. Use a global HTTP(s) load balancer with Cloud CDN enabled.

C. Create a second GKE cluster in asia-southeast1, and use kubemci to create a global HTTP(s) load balancer.

D. Increase the memory and CPU allocated to the application in the cluster.

**vladik820** Highly Voted 👍 2 years, 9 months ago

C is ok .
https://cloud.google.com/blog/products/gcp/how-to-deploy-geographically-distributed-services-on-kubernetes-engine-with-kubemci

upvoted 36 times

**rishab86** 2 years, 8 months ago

After going through the link I feel its C

upvoted 3 times

**mikesp** 2 years, 7 months ago

Mee too.
CDN does not make sense

upvoted 6 times

**bandegg** 5 months, 3 weeks ago

Indeed. We don't know if the API is authenticated, reveals private data, static or not.

upvoted 1 times

**Lk9876** Highly Voted 2 years, 9 months ago

I'm not sure about C. kubemci is deprecated and is not part anymore of cloud sdk in favor of ingress for anthos. I'll go with A

upvoted 11 times

**MikeB19** 2 years, 9 months ago

I think either a or c is correct. I chose c base on the article ref in the chat. Do u have supporting article ref kubemci is deprecated? I also fo some chatter about kubemci being deprecated but couldn't find anything offical

upvoted 1 times

**Linus11** 2 years, 8 months ago

It is hee -- https://github.com/GoogleCloudPlatform/k8s-multicluster-ingress

upvoted 1 times

**Rzla** 2 years, 9 months ago

Problem with A is that a service load bancer is not l7 https. The question is outdated, the answer will have been C. Now it would be Anthos multi cluster ingress -https://cloud.google.com/kubernetes-engine/docs/concepts/multi-cluster-ingress

upvoted 14 times

**cotam** 2 years, 7 months ago

That's actually not true. Service of type: LoadBalancer, is a service from "K8s" point of view, which creates L7 HTTP(S) Load Balancer.

upvoted 5 times

**huuthanhdlv** 3 weeks, 3 days ago

Nope, service is L4 Network/Internal load balancer

upvoted 1 times

**dija123** 1 month, 4 weeks ago

Agree with you

upvoted 1 times

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

Selected Answer: B

To reduce latency for users in Asia while maintaining high availability and scalability, the most appropriate option would be:

B. Use a global HTTP(s) load balancer with Cloud CDN enabled.

upvoted 2 times

**Diwz** 2 months, 2 weeks ago

Selected Answer: B

B is answer

upvoted 2 times

**Pime13** 4 months, 3 weeks ago

Selected Answer: C

question is old but it should be c. however currently should be multi cluster ingress
https://cloud.google.com/kubernetes-engine/docs/concepts/multi-cluster-ingress

upvoted 3 times

**AzFarid** 5 months, 3 weeks ago

really powefull
kubernetes-engine-with-kubemci

upvoted 1 times

**theBestStudent** 7 months ago

Well it should be C, but it is deprecated in favor of ingress for Anthos as can be read here https://github.com/GoogleCloudPlatform/k8s-multicluster-ingress

upvoted 2 times

**tamj123** 8 months ago

go for C

upvoted 1 times

**RaviRS** 9 months, 2 weeks ago

**Selected Answer: C**

B is funny

upvoted 2 times

**Vignesh_Krishnamurthi** 11 months, 2 weeks ago

If it is an API performing scientific calculations then its customer base is a very specific targeted group. It should not be considered as a mass market app that is used by lots of people all over the world. Considering the business purpose of the API, option B would be more than suffic to serve the need of customers anywhere in the world.

upvoted 1 times

**kapara** 11 months, 2 weeks ago

IDK if this question will be in the exam bc the answer should be C.
but kubemci has now been deprecated in favor of Ingress for Anthos.
Ingress for Anthos is the recommended way to deploy multi-cluster ingress.

upvoted 3 times

**BiddlyBdoyng** 1 year ago

The problem with B is the question very much infers we are dealing with dynamic content & not static.

upvoted 1 times

**BiddlyBdoyng** 1 year ago

It's A or C but I think A might be better.
A is a simpler solution. Cloud DNS allows you to add multiple targets and part of its decision making is the latency.
https://cloud.google.com/dns/docs/zones/zones-overview
Tough but I think A because it's only one API being exposed. Ingress comes into its own when exposing many services.

upvoted 1 times

**r1ck** 1 year, 4 months ago

kubemci - deprecated
https://github.com/GoogleCloudPlatform/k8s-multicluster-ingress

upvoted 4 times

**omermahgoub** 1 year, 5 months ago

A good option for reducing latency for users in Asia accessing the web API would be to create a second GKE cluster in asia-southeast1 and ι kubemci to create a global HTTP(s) load balancer.

Option C, "Create a second GKE cluster in asia-southeast1, and use kubemci to create a global HTTP(s) load balancer," would be the correct choice for this scenario.

By creating a second GKE cluster in asia-southeast1, you can reduce latency for users in Asia by serving the API from a closer location. You c then use kubemci, a command-line tool that simplifies the process of creating a global HTTP(s) load balancer, to expose the APIs from both clusters through a single global IP address. This allows users to access the API with low latency, regardless of their location.

upvoted 2 times

**omermahgoub** 1 year, 5 months ago

Option A, "Create a second GKE cluster in asia-southeast1, and expose both APIs using a Service of type LoadBalancer. Add the public IF to the Cloud DNS zone," would not be a good choice because it would not provide a single global IP address for users to access the API, which would increase latency and complexity.

Option B, "Use a global HTTP(s) load balancer with Cloud CDN enabled," would not be a good choice because it would not allow you to s the API from a closer location for users in Asia.

Option D, "Increase the memory and CPU allocated to the application in the cluster," would not be a good choice because it would not address the issue of latency for users in Asia accessing the API.

upvoted 2 times

**ale_brd_111** 1 year, 6 months ago

**Selected Answer: C**

Answer is C but kubemci is deprecated, now you have to go with:

mp

Question #155 *Topic 1*

You are migrating third-party applications from optimized on-premises virtual machines to Google Cloud. You are unsure about the optimum CPU and memory options. The applications have a consistent usage pattern across multiple weeks. You want to optimize resource usage for the lowest cost. What should you do?

A. Create an instance template with the smallest available machine type, and use an image of the third-party application taken from a current on-premises virtual machine. Create a managed instance group that uses average CPU utilization to autoscale the number of instances in the group. Modify the average CPU utilization threshold to optimize the number of instances running.

B. Create an App Engine flexible environment, and deploy the third-party application using a Dockerfile and a custom runtime. Set CPU and memory options similar to your application's current on-premises virtual machine in the app.yaml file.

C. Create multiple Compute Engine instances with varying CPU and memory options. Install the Cloud Monitoring agent, and deploy the third-party application on each of them. Run a load test with high traffic levels on the application, and use the results to determine the optimal settings.

D. Create a Compute Engine instance with CPU and memory options similar to your application's current on-premises virtual machine. Install the Cloud Monitoring agent, and deploy the third-party application. Run a load test with normal traffic levels on the application, and follow the Rightsizing Recommendations in the Cloud Console.

**pr2web** Highly Voted 2 years, 9 months ago

Answer is D.

https://cloud.google.com/migrate/compute-engine/docs/4.9/concepts/planning-a-migration/cloud-instance-rightsizing?hl=en

"Rightsizing provides two types of recommendations:

1. Performance-based recommendations: Recommends Compute Engine instances based on the CPU and RAM currently allocated to the on premises VM. This recommendation is the default.

2. Cost-based recommendations: Recommends Compute Engine instances based on:
- The current CPU and RAM configuration of the on-premises VM.
- The average usage of this VM during a given period. To use this option, you must activate rightsizing monitoring with vSphere for this group VMs and allow time for Migrate for Compute Engine to analyze usage.

upvoted 55 times

**melono** 1 year, 8 months ago

The point:
2. Cost-based recommendations: Recommends Compute Engine instances based on:
The current CPU and RAM configuration of the on-premises VM.

upvoted 1 times

**cloudmon** Highly Voted 2 years, 2 months ago

**Selected Answer: D**

It's definitely D. See the reference at the following link that says "The recommendation algorithm is suited to workloads that follow weekly patterns", which matches the part of the questions that says "consistent usage pattern over multiple weeks":
https://cloud.google.com/compute/docs/instances/apply-machine-type-recommendations-for-instances

Option A also has two problems;
1. It only focuses on CPU, but the question says "CPU and memory"
2. The question does not mention anything about horizontal scalability

upvoted 9 times

**cloudmon** 2 years, 2 months ago

Another (less obvious) reason for choosing D: I've noticed a pattern in these exams that the cloud provider wants to advertise and promote anything that they consider to be a cool feature of their platform. In this case, they are promoting their recommendation engine. If there's e an option that sounds like it's advertising a relevant managed service from the cloud provider, then that's usually one to consider.

upvoted 4 times

**cloudmon** 2 years, 2 months ago

I also find the following wording in option A to be a bit iffy: "an image of the third-party application taken from a current on-premises vir machine". That seems a bit vague in terms of what the image format would be.

upvoted 1 times

**e5019c6** Most Recent 5 months, 3 weeks ago

**Selected Answer: D**

I choose A at first, because I thought that the Rightsizing Recommendations took various days to offer the estimate stats. But according to th article:
https://cloud.google.com/migrate/compute-engine/docs/4.11/concepts/planning-a-migration/cloud-instance-rightsizing
While it needs a week to give a proper estimate, it can give an estimate with less time too (But the accuracy decreases)
"For better recommendations, Migrate for Compute Engine recommends monitoring the migrated workloads for at least seven consecutive da (or one typical business week). Migrate for Compute Engine warns you when the monitoring period is insufficient for an adequate recommendation.

Even if the monitoring period is insufficient, Migrate for Compute Engine still offers a cost-optimized recommendation based on the data available."

upvoted 2 times

**e5019c6** 5 months, 3 weeks ago

Also note that Migrate to Virtual Machines v4.11 (Which the info is from) is no longer the latest version. V5 is already out and, strangely, lac any article about rightsizing recommendations...

upvoted 2 times

**tamj123** 8 months ago

D make sense.

upvoted 1 times

**RaviRS** 9 months, 2 weeks ago

**Selected Answer: D**

D is correct

upvoted 1 times

**WinSxS** 1 year, 3 months ago

**Selected Answer: D**

Option D would be the best option to optimize resource usage for the lowest cost when migrating third-party applications from optimized on-premises virtual machines to Google Cloud.

upvoted 2 times

**AugustoKras011111** 1 year, 3 months ago

Selected Answer: D

Answer is D. Similar than third-party convince me...

upvoted 1 times

**beehive** 1 year, 5 months ago

why most of the answers selected by host is INCORRECT? Is it intentional to misguide the folks?

upvoted 7 times

**thamaster** 1 year, 5 months ago

Selected Answer: D

i choose D as it's best practice create an instance with similar configuration as on premise and check metrics

upvoted 1 times

**shefalia** 1 year, 6 months ago

Selected Answer: D

D is the right one because of Rightsizing option from GCP

upvoted 1 times

**surajkrishnamurthy** 1 year, 6 months ago

Selected Answer: D

D is the correct answer

upvoted 1 times

**megumin** 1 year, 7 months ago

Selected Answer: D

D is ok

upvoted 1 times

**Mahmoud_E** 1 year, 8 months ago

Selected Answer: D

I agree with D is the most accurate

upvoted 1 times

**AzureDP900** 1 year, 8 months ago

D is correct

upvoted 1 times

**SerGCP** 1 year, 8 months ago

Selected Answer: D

A, application may not support horizontal scaling and may not run in instances whith small cpu
B, dockerize third-party applications is not a requirement....Complex and costly
C, too expensive
D, simple and works

upvoted 3 times

**shekarcfc** 1 year, 9 months ago

Selected Answer: A

A, the benefit of moving to cloud is scaling based on load, start with min infra and scale-up based on usage.

upvoted 4 times

**amxexam** 2 years ago

Selected Answer: D

A - you cannot expect application to behavior similar in 2 different envior met without a test.
B - App Engine is costly
C- Varing cpu and memory cannot be doone.
D- correa.

upvoted 3 times

Question #156 *Topic 1*

Your company has a Google Cloud project that uses BigQuery for data warehousing. They have a VPN tunnel between the on-premises environment and Google
Cloud that is configured with Cloud VPN. The security team wants to avoid data exfiltration by malicious insiders, compromised code, and accidental oversharing.
What should they do?

A. Configure Private Google Access for on-premises only.

B. Perform the following tasks: 1. Create a service account. 2. Give the BigQuery JobUser role and Storage Reader role to the service account. 3. Remove all other IAM access from the project.

C. Configure VPC Service Controls and configure Private Google Access.

D. Configure Private Google Access.

**Craigenator** Highly Voted 2 years, 6 months ago
Without the discussion this site would be useless, many thanks to all that participate. Majority of answers are wrong...
upvoted 71 times

**VarunGo** 1 year ago
you can used chatGPT now
upvoted 3 times

**Murtuza** 8 months, 2 weeks ago
Then you are definitely bound to fail :-)
upvoted 11 times

**diaga2** Highly Voted 2 years, 9 months ago
C is the recommended one https://cloud.google.com/vpc-service-controls/docs/overview
upvoted 31 times

**squishy_fishy** Most Recent 6 months, 1 week ago
Correct answer is C.
Security benefits of VPC Service Controls
Access from unauthorized networks using stolen credentials
Data exfiltration by malicious insiders or compromised code
https://cloud.google.com/vpc-service-controls/docs/overview#benefits
upvoted 1 times

**thewalker** 7 months, 1 week ago

Selected Answer: C

VPC Service Controls is required to stop data exfiltration. Hence C

upvoted 2 times

**tamj123** 8 months ago

C, VPC Service controls is need for the solution

upvoted 1 times

**Mrinalini19** 1 year, 3 months ago

Selected Answer: C

C is correct

upvoted 1 times

**examch** 1 year, 5 months ago

Selected Answer: C

C is the correct answer,

To secure data from exfiltration by malicious insiders, compromised code or accidental oversharing, we use VPC Service controls

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

For private access options, connect to services in VPC networks we use private service endpoints or VPC network peering.

https://cloud.google.com/vpc/docs/private-access-options#connect-services

upvoted 2 times

**surajkrishnamurthy** 1 year, 6 months ago

Selected Answer: C

C is the correct answer

upvoted 2 times

**megumin** 1 year, 7 months ago

Selected Answer: C

C is ok

upvoted 2 times

**Mahmoud_E** 1 year, 8 months ago

Selected Answer: C

C is the right answer

upvoted 1 times

**AzureDP900** 1 year, 8 months ago

I will go with C

upvoted 1 times

**nkit** 2 years, 1 month ago

Selected Answer: C

Going by definition- VPC Service Controls improves your ability to mitigate the risk of data exfiltration from Google Cloud services such as Cl
Storage and BigQuery.

hence C is correct

upvoted 7 times

**dangcpped** 2 years, 2 months ago

Selected Answer: C

C is the recommended
https://cloud.google.com/vpc-service-controls/docs/overview

upvoted 2 times

**kimharsh** 2 years, 3 months ago

I don't get it , C is correct because of the "VPC service Control", But Privet Google access is not for on On-premises, A is for On-premises = https://cloud.google.com/vpc/docs/private-access-options

upvoted 2 times

**OrangeTiger** 2 years, 5 months ago

Selected Answer: C

I agree C.
The link that wroted in Reveral Solution means C.

upvoted 1 times

**vincy2202** 2 years, 6 months ago

Selected Answer: C

C is the correct answer
https://cloud.google.com/vpc-service-controls/docs/overview

upvoted 2 times

**sapsant** 2 years, 6 months ago

Selected Answer: C

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

upvoted 2 times

Question #157 *Topic 1*

You are working at an institution that processes medical data. You are migrating several workloads onto Google Cloud. Company policies require all workloads to run on physically separated hardware, and workloads from different clients must also be separated. You created a sole-tenant node group and added a node for each client. You need to deploy the workloads on these dedicated hosts. What should you do?

A. Add the node group name as a network tag when creating Compute Engine instances in order to host each workload on the correct node group.

B. Add the node name as a network tag when creating Compute Engine instances in order to host each workload on the correct node.

C. Use node affinity labels based on the node group name when creating Compute Engine instances in order to host each workload on the correct node group.

D. Use node affinity labels based on the node name when creating Compute Engine instances in order to host each workload on the correct node.

**pr2web** Highly Voted 3 years, 3 months ago

Answer is D.

Y'all not reading the fine details. The question is about aligning EACH client to their dedicated nodes (D), not to a node group (C).

https://cloud.google.com/compute/docs/nodes/sole-tenant-nodes#default_affinity_labels

The above reference clearly articulates the default affinity label for node group and node name. Unless we're thinking about growing each clie
to their own dedicated node groups (not in the current requirement), then the answer is not C, rather D.

Compute Engine assigns two default affinity labels to each node:

A label for the node group name:
Key: compute.googleapis.com/node-group-name
Value: Name of the node group.
A label for the node name:
Key: compute.googleapis.com/node-name
Value: Name of the individual node.