

🗨️ **kip21** 11 months, 1 week ago

D

The question is talking abt MIG and you can revert Inst Template same as B. Since this is about MIG's I will choose D
upvoted 1 times

🗨️ **adoyt** 11 months, 4 weeks ago

Selected Answer: D

D. This is a question about instance groups and so modifying templates should be what we're looking for.
upvoted 1 times

🗨️ **simiramis221** 1 year ago

This a B for sure
upvoted 1 times

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

Selected Answer: B

The popped up with source code changes, hence reverting the change and deployment will solve the issue.

B. Revert the source code change, and rerun the deployment pipeline
upvoted 2 times

🗨️ **yilexar** 1 year, 2 months ago

D is incorrect:

- MIG instance group template is immutable, there is no version concept. The context never mentioned that team created multiple instance group templates.
- Software code change might not all ended up in the instance group templates, it depends on how the deployment pipeline is configured.

Regardless, B is a best practices, ensure that your infrastructure is synced with your source control system.
upvoted 1 times

🗨️ **rusli** 1 year, 3 months ago

Selected Answer: D

You don't need to touch your code, just deploy and older version and fix the code, then deploy the fixed version
upvoted 2 times

🗨️ **jalberto** 1 year, 4 months ago

Selected Answer: D

The most secure option is D
Revert a source code change could be complex (if change was made in various components)
upvoted 2 times

🗨️ **chrismar** 1 year, 6 months ago

Selected Answer: B

Because the question starting from source code
upvoted 2 times

🗨️ **oriori123123** 1 year, 6 months ago

Selected Answer: B

by bard:

The correct answer is B. Revert the source code change, and rerun the deployment pipeline.
upvoted 1 times

🗨️ **JohnWick2020** 1 year, 6 months ago

B.

The keyword here is source code not VM configuration. If it was the later then instance group templates is the answer. But in this case simply rollback your source code change and rerun to last workable version. Simples!
upvoted 2 times

🗨️ **red_panda** 1 year, 6 months ago

Selected Answer: B

B is ok for me
upvoted 1 times

Question #37

Topic 1

Your organization wants to control IAM policies for different departments independently, but centrally. Which approach should you take?

- A. Multiple Organizations with multiple Folders
- B. Multiple Organizations, one for each department
- C. A single Organization with Folders for each department
- D. A single Organization with multiple projects, each with a central owner



  **AWS56** Highly Voted 5 years ago



<https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations>


I will stick with C
upvoted 27 times



  **CamiloJrJr** 3 weeks, 5 days ago



https://cloud.google.com/architecture/identity/best-practices-for-planning#use_organizations_to_delineate_administrative_authority
upvoted 1 times



  **CamiloJrJr** 3 weeks, 5 days ago
https://cloud.google.com/architecture/identity/best-practices-for-planning#use_a_separate_staging_organization
 upvoted 1 times



  **AzureDP900** 2 years, 2 months ago
 C is recommended approach
 upvoted 2 times



  **BiddlyBdoyn** Highly Voted 2 years, 2 months ago
 The reason it isn't D is that a Dept modelled as a project puts a massive constraint on the dept that they can only have a single project, it's like a department will want many projects.
 upvoted 7 times

  **Ekramy_Elnaggar** Most Recent 1 month ago
Selected Answer: C
 1. Centralized Control: A single organization provides a central point for managing all your Google Cloud resources and IAM policies. This simplifies administration and ensures consistency across your organization.
 2. Independent Department Management: Folders allow you to group projects within your organization and delegate administrative control to different departments. Each department can manage its own IAM policies within its assigned folder, providing the necessary independence.
 3. Hierarchical Structure: Folders provide a hierarchical structure for organizing your resources. You can create sub-folders within department: further granularity and control.
 4. Efficient Resource Management: This structure makes it easier to manage resources, track costs, and enforce security policies across your organization.
 upvoted 2 times

  **Shasha1** 2 months, 1 week ago
 B
 upvoted 1 times



  **vyomkeshbakshi** 1 year, 5 months ago
Selected Answer: C
 Clearly C
 upvoted 1 times



  **red_panda** 1 year, 6 months ago
Selected Answer: C
 Is obviously C
 upvoted 1 times

  **omermahgoub** 1 year, 12 months ago
 C. A single Organization with Folders for each department

To control IAM policies for different departments independently but centrally, you should create a single organization and use folders to organize the policies for each department. This approach allows you to centralize the management of IAM policies for all departments within a single organization, while also allowing you to set up different policies for each department as needed.

Option A, multiple organizations with multiple folders, would not be an effective solution because it would create unnecessary complexity and make it more difficult to centralize the management of IAM policies. Option B, multiple organizations, one for each department, would also not be an effective solution because it would create unnecessary complexity and make it more difficult to centralize the management of IAM policies. Option D, a single organization with multiple projects, each with a central owner, would not be an effective solution because it would not allow you to set up different policies for each department as needed.
 upvoted 2 times

  **MarcoEscanor** 2 years, 2 months ago
 C. It's a best practice and I've done this with my previous and current company :)
 upvoted 3 times

  **Prashant2022** 2 years, 2 months ago
Selected Answer: C

 upvoted 1 times

- 🗳️ 👤 **holerina** 2 years, 2 months ago
C single org and multiple folders
upvoted 1 times
- 🗳️ 👤 **cmamiusa** 2 years, 8 months ago
Selected Answer: C
C is the right answer
upvoted 1 times
- 🗳️ 👤 **mygcpiourney2712** 2 years, 8 months ago
Selected Answer: C
Will go for C
upvoted 1 times
- 🗳️ 👤 **haroldbenites** 3 years ago
Go for C
upvoted 2 times
- 🗳️ 👤 **vincy2202** 3 years ago
C is the right answer
upvoted 1 times
- 🗳️ 👤 **nansi** 3 years, 2 months ago
C shall be the correct answer
upvoted 1 times
- 🗳️ 👤 **rikoko** 3 years, 4 months ago
C. Seems to be best practice (cf AWS56). And I believe that D should be excluded because it says "Project owner" - it is not best practice since it's a basic role + it's not even stated as a requisite
upvoted 1 times
- 🗳️ 👤 **victory108** 3 years, 7 months ago
C. A single Organization with Folders for each department
upvoted 3 times

Question #38

Topic 1

You deploy your custom Java application to Google App Engine. It fails to deploy and gives you the following stack trace.
What should you do?

```
java.lang.SecurityException: SHA1 digest error for
com/Altostrat/CloakedServlet.class
    at com.google.appengine.runtime.Request.process
-d36f818a24b8cf1d (Request.java)
    at
sun.security.util.ManifestEntryVerifier.verify
(ManifestEntryVerifier.java:210)
    at java.util.jar.JarVerifier.processEntry
(JarVerifier.java:218)
    at java.util.jar.JarVerifier.update
(JarVerifier.java:205)
    at
java.util.jar.JarVerifiersVerifierStream.read
(JarVerifier.java:428)
    at sun.misc.Resource.getBytes
(Resource.java:124)
    at java.net.URL.ClassLoader.defineClass
(URLClassLoader.java:273)
    at sun.reflect.GeneratedMethodAccessor5.invoke
```

```



(Unknown Source)
    at
sun.reflect.DelegatingMethodAccessorImpl.invoke
(DelegatingMethodAccessorImpl.java:43)
    at java.lang.reflect.Method.invoke
(Method.java:616)
    at java.lang.ClassLoader.loadClass
(ClassLoader.java:266)

```

- A. Upload missing JAR files and redeploy your application.
- B. Digitally sign all of your JAR files and redeploy your application
- C. Recompile the CLoakedServlet class using and MD5 hash instead of SHA1

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



Signing the JAR files grants it permissions. (<https://docs.oracle.com/javase/tutorial/deployment/jar/signindex.html>)
upvoted 23 times

  **tartar** 4 years, 4 months ago

B is ok
upvoted 9 times

  **Urban_Life** 3 years, 2 months ago

Where do you go? when we need you for other questions. Plz ans other q's if you have time
upvoted 2 times

  **nitinz** 3 years, 9 months ago

B, SHA1 Digest error in the first line in the error code. With Java errors, always focus on the first line in the error code, rest of the lines are garbage **mostly**.
upvoted 18 times

  **omermahgoub** Highly Voted 1 year, 12 months ago

The most likely cause of the error is that one of the JAR files in your application has been tampered with or is corrupt. The SHA1 digest error indicates that the JAR file's signature does not match the expected value, which could be due to tampering or corruption.

To fix the issue, you should try uploading missing JAR files and redeploying your application. If the issue persists, you may need to digitally sign all of your JAR files and redeploy your application to ensure that the signatures are valid. You should not try to recompile the Cloaked
upvoted 12 times

  **Ekramy_Elnaggar** Most Recent 1 month ago

Selected Answer: B

1. JAR signing and integrity: Digitally signing your JAR files ensures their authenticity and integrity. It adds a digital signature that verifies the origin and confirms that the file hasn't been tampered with. This is crucial for security and prevents issues like the SHA1 digest error you're encountering.

2. App Engine requirement: Google App Engine enforces JAR signing for security reasons. All deployed applications must have properly signed JAR files.

upvoted 1 times

  **chrissamharris** 1 month, 1 week ago

Selected Answer: A

A SHA1 digest error during the deployment of a Java application to Google App Engine (GAE) typically indicates an issue with the integrity of your JAR files. This error can arise due to corrupted, modified, or missing JAR files that are essential for your application to run correctly.

upvoted 1 times

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

Selected Answer: A

A missing JAR (Java ARchive) file indicates a problem with the code to be deployed.
 B Digitally signing all of your JAR files indicates a problem with the signature.
 A is better
 upvoted 3 times

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

Selected Answer: B

"JavaVerifier.Java.428" is the key here
 upvoted 1 times

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

Selected Answer: B

B is the correct answer.
 upvoted 1 times

🗨️ 👤 **JC0926** 1 year, 9 months ago

Selected Answer: A

A. Upload missing JAR files and redeploy your application.

The error message indicates that there is a problem with the SHA1 digest for the "com/altostrat/cloakedervlet.class" file. This can be caused a corrupted or incomplete JAR file. Therefore, the best course of action is to upload any missing JAR files and redeploy the application.
 upvoted 2 times

🗨️ 👤 **tocsa** 6 months, 2 weeks ago

Corrupted or incomplete. But not missing.
 upvoted 1 times

🗨️ 👤 **Racinely** 2 years, 1 month ago

B is correct
 upvoted 1 times

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

Selected Answer: B

Ok B but how is this question related to a GCP exam? I guess a google search will be faster than reading the theory around Java (unless you a developer).
 upvoted 7 times

🗨️ 👤 **zr79** 2 years, 2 months ago

have you done any Azure exams? you will thank Google
 upvoted 5 times

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

nothing to do with GCP however basic troubleshooting skills required as a DevOps or Architect, B is fine
 upvoted 3 times

🗨️ 👤 **[Removed]** 1 year, 11 months ago

I see your point, but for basic troubleshooting of apps, i will usually have access to google (aka stackoverflow homepage). This could have been a cloud developer question that they repurposed.
 upvoted 1 times

🗨️ 👤 **holerina** 2 years, 2 months ago

B is the right answer
 upvoted 1 times

🗨️ 👤 **avinashvidyarthi** 2 years, 7 months ago

Selected Answer: B

B is Correct!
 upvoted 1 times

- 🗲️ 👤 **Munna19** 2 years, 7 months ago
B is the right answer
upvoted 1 times
- 🗲️ 👤 **vincy2202** 2 years, 11 months ago
B is the correct answer
upvoted 2 times
- 🗲️ 👤 **duocnh** 3 years ago
Selected Answer: B
vote B
upvoted 1 times
- 🗲️ 👤 **TheCloudBoy77** 3 years, 1 month ago
Selected Answer: B
B is correct answer
upvoted 1 times
- 🗲️ 👤 **bala786** 3 years, 5 months ago
Option B. Digitally sign all of your JAR files and redeploy your application
upvoted 1 times

Question #39



Topic 1

You are designing a mobile chat application. You want to ensure people cannot spoof chat messages, by providing a message were sent by a specific user.

What should you do?

- A. Tag messages client side with the originating user identifier and the destination user.
- B. Encrypt the message client side using block-based encryption with a shared key.
- C. Use public key infrastructure (PKI) to encrypt the message client side using the originating user's private key.
- D. Use a trusted certificate authority to enable SSL connectivity between the client application and the server.

- 🗲️ 👤 **KouShikyou** **Highly Voted** 👍 5 years, 1 month ago
I am not sure about this one. D works if SSL client authentication is enabled.
C works as well if client encrypts message with private key and server decrypt with public key.
I prefer C.
upvoted 37 times
- 🗲️ 👤 **JoeShmoe** 5 years, 1 month ago
Agree with C
upvoted 5 times

  **asfar** 4 years, 11 months ago

I agree with C on this one.



upvoted 5 times

  **Tobbe** Highly Voted 3 years, 10 months ago

Encrypting each block and tagging each message at the client side is an overhead on the application. Best method which has been adopted since years is contacting SSL provider and use public certificate to encrypt the traffic between client and server.

D is correct

upvoted 13 times

  **Meyucho** 2 years, 11 months ago

If you use server public key you aren't meeting the goal. Don't miss the "for specific user" in the statement



upvoted 1 times

  **Alekshar** 3 years, 9 months ago

If you use the server's public certificate to encrypt your data you only ensure the right server is the only one to read you.

But anyone can use the same encryption key as you did and pretend to be you. Hence it does not solve our authentication problematic

upvoted 6 times

  **Tobbe** 3 years, 9 months ago

thanks for your insight! C is correct.

upvoted 2 times

  **stefanop** 1 year ago

Can you explain why you think this?

upvoted 1 times

  **lynx256** 3 years, 8 months ago

I cannot agree with you. Before one be able to pretend to be someone else, he should know his (someone's) password on the Chat Server...

upvoted 1 times

  **PeppaPig** 3 years, 4 months ago

SSL doesn't use server's public key to encrypt data. This is definitely wrong. Please read SSL specs. SSL uses a separate session key message encryption. This session key is temporary and will be rotated for every single session.

upvoted 4 times

  **Ekramy_Elnaggar** Most Recent 1 month ago



Selected Answer: C

1. Digital Signatures and Non-Repudiation: PKI provides the foundation for digital signatures. When a user sends a message, it's encrypted with their private key. The recipient can then use the sender's public key to decrypt it. This ensures:

- Authenticity: The message truly originated from the claimed sender.
- Non-repudiation: The sender cannot deny sending the message.
- Integrity: The message hasn't been tampered with in transit.

2. How it prevents spoofing: Since only the sender has access to their private key, no one else can create a message that would decrypt correctly with their public key. This effectively prevents spoofing.

upvoted 2 times

  **Chojrak** 6 months, 2 weeks ago

The "C" answer is either messed up on purpose, or somebody dumped it wrong.

When you use PKI (Public Key Infrastructure), you encrypt using a public key of the recipient, and the recipient decrypts using their private key. Sample reference that this is correct: <https://www.keyfactor.com/education-center/what-is-pki/>

On the contrary, when a message is digitally signed, the originator is using their private key to sign the message, and the recipient is verifying it using public key of the originator.

I still don't know which answer would I choose on the actual exam.

upvoted 3 times

🗨️ **yas_cloud** 10 months, 3 weeks ago

Option A is not secure because anyone who intercepts the message could modify the user identifiers. Option B does not provide a way to verify the sender's identity. Option D is important for securing the connection between the client and server, but it does not prevent message spoofing by itself.

Hence C.

upvoted 1 times

🗨️ **02fc23a** 1 year ago

Selected Answer: C

I was considering D, but nope, C:

<https://support.google.com/messages/answer/10262381#:~:text=your%20device%20and%20the%20device%20you%20message>

upvoted 1 times

🗨️ **_kartik_raj** 1 year, 1 month ago

Answer : D

Let me clarify, what PKI is saying I think first the answer is D, reason, Just understand what it says, i.e. option c - Using PKI to encrypt messages using the originating user's private key, now couple people are saying that it is good and then the server will decrypt the msg using public key, but can't you see anyone in the whole world will be able to see the messages as public key is available publicly. Ideally what should have been the solution, Using the public key of receiver the messages should have been encrypted then the receiver would have decrypted using his private key, which absolutely makes sense, Talking about ssl I think it's one of the widely used secure tech for communication between client and server

upvoted 1 times

🗨️ **ArtistS** 1 year, 1 month ago

Thanks for your explanation, so I choose C.....

upvoted 1 times

🗨️ **stefanop** 1 year ago

Why? Can you explain that?

upvoted 1 times

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

Selected Answer: C

Option C - Use public key infrastructure (PKI) to encrypt the message client-side using the originating user's private key: Using PKI to encrypt messages using the originating user's private key provides end-to-end encryption, which means only the intended recipient can decrypt the message. This option also ensures that the message's authenticity is protected. If a malicious user changes the sender's name, the recipient will not be able to decrypt the message since it was not encrypted using the correct private key. This option is a strong method for securing chat messages.

upvoted 4 times

🗨️ **patricklin1105** 1 year, 5 months ago

C is wrong because private can only be used for signing, not encrypting. Public key is used for encrypting, private key is used for decrypting.

upvoted 3 times

🗨️ **stefanop** 1 year ago

But still, spoofing is not about reading data in clear but impersonating someone else.

Using D you can sign the message by confirming your identity.

upvoted 1 times

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

Selected Answer: C

As question is about ensuring a specific user sent a message, answer could not be D, which would ensure secure message transmission, but message origin (which can only be done by using asymmetric key)

upvoted 3 times

🗨️ **stefanop** 1 year ago

So the sender is signing the message while encrypting it with the private key?

upvoted 1 times

🗨️ **oriori123123** 1 year, 6 months ago

bard say D.

and ChatGPT say C..

upvoted 1 times

  **ionescuandrei** 1 year, 8 months ago

Selected Answer: C

I noticed this question in other tests and the suggested answer was C.
upvoted 1 times

  **JC0926** 1 year, 9 months ago

Selected Answer: C

To prevent message spoofing, it is important to ensure that messages cannot be altered or forged by anyone other than the originating user. C way to accomplish this is by using public key infrastructure (PKI) to encrypt messages using the originating user's private key.
upvoted 4 times

  **omermahgoub** 1 year, 12 months ago

To ensure that chat messages cannot be spoofed and that the messages are truly sent by a specific user, the best option would be to use public key infrastructure (PKI) to encrypt the message client side using the originating user's private key. This would allow the recipient to verify the authenticity of the message by using the originating user's public key to decrypt the message.

Option A, tagging the message with the originating user identifier and the destination user, would not ensure the authenticity of the message, could potentially be forged by an attacker.

upvoted 2 times

  **omermahgoub** 1 year, 12 months ago

Option B, encrypting the message using block-based encryption with a shared key, would also not ensure the authenticity of the message. the shared key could potentially be compromised by an attacker.

Option D, using a trusted certificate authority to enable SSL connectivity between the client application and the server, would help to secure the communication channel between the client and the server, but it would not necessarily ensure the authenticity of the chat messages themselves.

Overall, using PKI and the originating user's private key to encrypt the message would be the most effective way to ensure the authenticity of the chat messages in your mobile chat application.

upvoted 1 times

  **FateSpringfield** 2 years ago

C is the answer, The requirement is the integrity of messages sent in CIA security (Confidentiality, Integrity, and Availability). For Confidentiality using PublicKey of receiver, for Integrity, using PrivateKey of sender. D works in case of SSL client authentication.

upvoted 3 times

  **megumin** 2 years, 1 month ago

Selected Answer: C

C is ok
upvoted 1 times

  **AjayPandit** 2 years, 1 month ago

Selected Answer: C

PKI uses X.509 certificates and Public Keys, where the key is used for end-to-end encrypted communication, so that both parties can trust each other and test their authenticity. PKI is mostly used in TLS/SSL to secure connections between the user and the server, while the user tests the server's authenticity to make sure it's not spoofed

upvoted 1 times

Question #40

Topic 1

As part of implementing their disaster recovery plan, your company is trying to replicate their production MySQL database from their private data center to their

GCP project using a Google Cloud VPN connection. They are experiencing latency issues and a small amount of packet loss that is disrupting the replication.

What should they do?

- A. Configure their replication to use UDP.
- B. Configure a Google Cloud Dedicated Interconnect.
- C. Restore their database daily using Google Cloud SQL.
- D. Add additional VPN connections and load balance them.
- E. Send the replicated transaction to Google Cloud Pub/Sub.

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

It's latency issues. That won't be solved by adding another VPN tunnel. If it was just a throughput issue then VPN would do, however to improve latency you need to go layer 2. Answer is B

upvoted 35 times

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

I think B is correct. I think it is more reliable.

upvoted 30 times

  **desertlotus1211** Most Recent 2 weeks ago

Selected Answer: B

Adding VPN connections may improve bandwidth but does not resolve latency or packet loss issues caused by public internet routing... though not mentioned, we must 'think' beyond the scope of the question and ask 'what is causing the latency'...

Answer B.

upvoted 1 times

  **Ekramy_Elnaggar** 1 month ago

Selected Answer: B

1. Dedicated Interconnect for high performance: Dedicated Interconnect provides a direct physical connection between your on-premises network and Google Cloud. This offers significantly lower latency, higher bandwidth, and greater reliability compared to a VPN. It's ideal for demanding workloads like database replication.

2. Reduced latency and packet loss: By bypassing the public internet, Dedicated Interconnect minimizes latency and packet loss, ensuring consistent and efficient data transfer for your MySQL replication.

3. Enhanced reliability: Dedicated Interconnect provides a more stable and predictable connection compared to a VPN, which can be affected by internet traffic fluctuations.

Why D is not correct: Add additional VPN connections and load balance them: This might improve bandwidth slightly but won't address the fundamental latency and packet loss issues inherent with VPNs over the public internet.

upvoted 1 times

  **19040e5** 7 months ago

Selected Answer: B

It's B, Interconnect.

D is wrong in this case: While this might help distribute traffic, it won't solve the underlying issue of latency and packet loss caused by the inherent limitations of VPNs.

upvoted 2 times

  **AWS_Sam** 11 months, 2 weeks ago

Dedicated interconnect is the answer. A second VPN will give you an HA solution, not going to resolve the latency.

upvoted 2 times

  **[Removed]** 11 months, 2 weeks ago

Selected Answer: E

Have you mind the budget you'll need to improve network infrastructure - whether it's dedicated interconnect or duplicating VPN connection? Mega IT corps may can afford, but I won't approve the work just for disaster recovery plan, if I were the authority. It's definitely overkill.

Main problem here is a latency issue and/or packet loss, yet the reason hasn't clearly configured. Whether it's occasional, or repetitive, and/or by DB engine or by network, mostly unknown. But you don't have to solve the problem if there's better bypass. Simply retry and test it. There also can be a solution (which likely being placed already), but it doesn't have significant feature for logging a transaction success/fail. If you to advance Pub/Sub, you can track each transaction processes. Ordering, can adding another issue, but it worth a try - cost effectively.

upvoted 2 times

🗨️ 👤 **Roro_Brother** 1 year ago

Selected Answer: B

Correct answer is B as its a latency issue.
upvoted 2 times

🗨️ 👤 **stefanop** 1 year ago

Selected Answer: B

I go for B.
Latency won't be solved by adding new VPN tunnels.
upvoted 2 times

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

Selected Answer: D

We have something called as HAVPN which uses 2 VPN Connections at a time. As this Question is old. we dont have this Option called use HAVPN. Now its Updated so the answer will be D. As its just a replication for disaster recovery and they are facing very minimal challenges
upvoted 6 times

🗨️ 👤 **SandipGhosal** 1 year, 9 months ago

I think the best option is E, using PubSub. In question the main issue is " a small amount of packet loss". As per google PubSub documentati data replication among databases is one of the common use case of PubSub. The asynchronously communication of PubSub can overcome small latency issues. Setting up dedicated interconnect would be very costly and required many pre-requisites.
upvoted 3 times

🗨️ 👤 **Shawnn** 1 year, 9 months ago

You could technically use your private key to encrypt a message, but it would not be secure because anyone who has your public key could decrypt the message. The recommended practice is to use your private key only for decryption and to use the recipient's public key for encryption.

I vote for D
upvoted 1 times

🗨️ 👤 **SirajShan** 1 year, 9 months ago

Configuring a Google Cloud Dedicated Interconnect requirement for company is a proximity to colocation facility and meeting condition to ha dedicated interconnect. Had this was possible why did they used Cloud VPN in the first place ? I think answer should be D.
upvoted 1 times

🗨️ 👤 **n_nana** 1 year, 11 months ago

If i face this issue, I will give a try with additional VPN, decision using VPN, maybe because they need encryption as well. With switching to dedicated interconnect, you have to implement your own VPN solution or application encryption. so it need more anyalsis to just skip VPN an use dedicated interconnect solution.
upvoted 2 times

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

The company should consider configuring a Google Cloud Dedicated Interconnect. A Google Cloud Dedicated Interconnect provides a private connection between the company's on-premises data center and GCP, which can help to reduce latency and improve the reliability of the connection. This can be particularly useful for replicating large amounts of data or for applications that require low-latency connectivity.

Option A, configuring the replication to use UDP, would not necessarily improve the reliability of the connection, as UDP is a connectionless protocol that does not guarantee delivery of packets.

Option C, restoring the database daily using Google Cloud SQL, would not address the underlying issues with the replication process.

upvoted 2 times

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

Option D, adding additional VPN connections and load balancing them, may help to improve the reliability of the connection by providing redundancy, but it may not necessarily address latency issues.

Option E, sending the replicated transaction to Google Cloud Pub/Sub, could potentially help to improve the reliability of the replication process by allowing the company to handle failures and retries in a more structured way, but it would not necessarily address latency issues.

Overall, configuring a Google Cloud Dedicated Interconnect is likely to be the most effective solution for addressing latency issues and packet loss in the replication process.

upvoted 1 times

🗨️ 👤 **VSMu** 1 year, 10 months ago

Why focus on latency when the solution is for disaster recovery? The main issue is packet loss. While this can be solved with Dedicated Interconnect or Cloud Pub/Sub, PubSub seems like a cheaper alternative that prevents data loss and achieves reliability. I wouldn't care about latency as the backup is only for DR.. so how does it matter if it goes slowly?

upvoted 3 times

🗨️ 👤 **jris1991** 1 year, 2 months ago

Because latency and packet loss are probably coming from traffic going over public internet. This is the Cloud VPN definition from the public documentation:

"Cloud VPN securely extends your peer network to Google's network through an IPsec VPN tunnel. Traffic is encrypted and travels between the two networks over the public internet. Cloud VPN is useful for low-volume data connections."

There are documents showing what happens when public internet is used, but basically there's no way to prevent information from going through multiple hops over the internet, which is why Dedicated Interconnect should work. Plus, VPN is recommended for low volume data connections, and I highly doubt that replicating a database is considered a low-volume operation.

I'm going with B: using Cloud Dedicated Interconnect.

upvoted 2 times

🗨️ 👤 **ashrafh** 2 years, 1 month ago

so just to solve this issue we are going over a Dedicated Interconnect imagine saying this to a your project head.

upvoted 3 times

🗨️ 👤 **megumin** 2 years, 1 month ago

Selected Answer: B

ok for B

upvoted 2 times

Question #41

Topic 1


Your customer support tool logs all email and chat conversations to Cloud Bigtable for retention and analysis. What is the recommended approach for sanitizing this data of personally identifiable information or payment card information before initial storage?

A. Hash all data using SHA256


- B. Encrypt all data using elliptic curve cryptography
- C. De-identify the data with the Cloud Data Loss Prevention API
- D. Use regular expressions to find and redact phone numbers, email addresses, and credit card numbers

 **AWS56** Highly Voted 4 years, 11 months ago

C is the answer
upvoted 23 times

 **nitinz** 3 years, 9 months ago

C, data sanitization = DLP
upvoted 8 times

 **tartar** 4 years, 4 months ago

C is ok
upvoted 8 times

 **omermahgoub** Highly Voted 1 year, 12 months ago

The recommended approach for sanitizing data of personally identifiable information or payment card information before storing it in Cloud Bigtable is option C: De-identify the data with the Cloud Data Loss Prevention API.

The Cloud Data Loss Prevention (DLP) API is a powerful tool that allows you to automatically discover, classify, and redact sensitive data in your organization. It uses advanced machine learning techniques to accurately identify and protect a wide range of sensitive data types, including personal information such as names, addresses, phone numbers, and payment card information.

Using the DLP API to de-identify your data before storing it in Cloud Bigtable is the most effective way to ensure that sensitive information is protected and not accessible to unauthorized users.

upvoted 12 times


 **omermahgoub** 1 year, 12 months ago

Option A: Hashing data using SHA256 is not sufficient for protecting sensitive information, as hashes can be reversed using various techniques.

Option B: Encrypting data using elliptic curve cryptography is a good option for protecting data, but it requires that you have a secure way to store and manage the encryption keys. If the keys are lost or compromised, the data will be inaccessible.

Option D: Using regular expressions to find and redact phone numbers, email addresses, and credit card numbers can be effective in some cases, but it requires that you have a complete and up-to-date list of all the data patterns that you want to protect. It is also prone to errors and may not be able to detect all instances of sensitive data.

upvoted 3 times

 **Kiroo** 1 year, 7 months ago

About D, usually is recommended that you don't reinvent the wheel specially when talking about security .
upvoted 1 times

 **Ekramy_Elnaggar** Most Recent 1 month ago

Selected Answer: C

1. Accurate and comprehensive: The Cloud DLP API is specifically designed to identify and redact sensitive information like PII (personally identifiable information) and payment card data. It uses advanced techniques like machine learning to accurately detect sensitive data, even in complex and unstructured text.

2. Context-aware: DLP understands the context of the data. It can differentiate between a credit card number and a similar-looking sequence of numbers that's not a credit card. This reduces false positives and ensures accurate sanitization.

3. Flexible and customizable: You can configure DLP to detect specific types of sensitive data, define your own detection rules, and choose how to de-identify the data (e.g., redaction, masking, tokenization).

4. Scalable and efficient: DLP can handle large volumes of data and integrates seamlessly with other GCP services like Cloud Storage and BigQuery.

upvoted 1 times

🗲️ 👤 **sim7243** 1 month, 1 week ago

Selected Answer: C

C option

upvoted 1 times

🗲️ 👤 **Palan** 1 year, 3 months ago

Without any doubt C is the right answer as the DLP API is a flexible and robust tool that helps identify sensitive data like credit card numbers, social security numbers, names and other forms of personally identifiable information (PII).

upvoted 1 times

🗲️ 👤 **shutupbot** 1 year, 8 months ago

Cloud Data Loss Prevention API provides obfuscation and de-identification methods like masking and tokenization. Especially for credit card transactions, the card numbers are supposed to be tokenized. Therefore, this API is helpful.

upvoted 1 times

🗲️ 👤 **mbrochard** 2 years ago

Selected Answer: C

C for sure !

upvoted 1 times

🗲️ 👤 **AniketD** 2 years, 1 month ago

Selected Answer: C

C is correct, DLP is the solution

upvoted 1 times

🗲️ 👤 **megumin** 2 years, 1 month ago

Selected Answer: C

ok for C

upvoted 1 times

🗲️ 👤 **vincy2202** 2 years, 11 months ago

Selected Answer: C

C is the correct answer

upvoted 2 times

🗲️ 👤 **haroldbenites** 3 years ago

Go for C

upvoted 3 times

🗲️ 👤 **haroldbenites** 3 years ago

<https://cloud.google.com/dlp>

upvoted 1 times

🗲️ 👤 **MamthaSJ** 3 years, 5 months ago

Answer is C

upvoted 1 times

🗲️ 👤 **victory108** 3 years, 7 months ago

C. De-identify the data with the Cloud Data Loss Prevention API

upvoted 3 times

🗲️ 👤 **un** 3 years, 7 months ago

C is correct

upvoted 1 times

🗲️ 👤 **sidhappy** 3 years, 8 months ago

Effectively reduce data risk with de-identification methods like masking and tokenization

<https://cloud.google.com/dlp>

upvoted 3 times

🗲️ 👤 **Ausias18** 3 years, 8 months ago

Answer is C

upvoted 1 times

lynx256 3 years, 8 months ago
C is ok
upvoted 1 times

Question #42

Topic 1

You are using Cloud Shell and need to install a custom utility for use in a few weeks. Where can you store the file so it is in the default execution path and persists across sessions?

- A. ~/bin
- B. Cloud Storage
- C. /google/scripts
- D. /usr/local/bin

ffk Highly Voted 5 years, 1 month ago

A is correct

<https://cloud.google.com/shell/docs/how-cloud-shell-works>

Cloud Shell provisions 5 GB of free persistent disk storage mounted as your \$HOME directory on the virtual machine instance. This storage is a per-user basis and is available across projects. Unlike the instance itself, this storage does not time out on inactivity. All files you store in your home directory, including installed software, scripts and user configuration files like .bashrc and .vimrc, persist between sessions. Your \$HOME directory is private to you and cannot be accessed by other users.

upvoted 73 times

Jambalaja 3 years, 8 months ago

Maybe also to mention is that ~/bin is located in the \$HOME directory

upvoted 17 times

zanfo 3 years, 3 months ago

cd ~/ is equal at cd \$HOME

~/bin is equal a cd \$HOME/bin

the persistent disk in cloud shell is for \$HOME

upvoted 9 times

AzureDP900 2 years, 2 months ago

Agree. A is right

upvoted 1 times

akoti 4 years, 1 month ago

\$HOME is not ~/bin. So 'C' is the answer.

upvoted 1 times

zanfo 3 years, 3 months ago

cd ~/ is equal at cd \$HOME

~/bin is equal a cd \$HOME/bin

the persistent disk in cloud shell is for \$HOME

upvoted 10 times

🗨️ 👤 **Shabje** 4 years, 7 months ago

Won't the persistent disk be auto-delete enabled by default, whereby the work maybe lost. Would that not be sufficient reason to consider Cloud storage instead. Thanks

upvoted 2 times

🗨️ 👤 **kaush** 4 years, 6 months ago

The virtual machine instance that backs your Cloud Shell session is not permanently allocated to a Cloud Shell session and terminates the session is inactive for an hour. After the instance is terminated, any modifications that you made to it outside your \$HOME are lost.

upvoted 3 times

🗨️ 👤 **zanfo** 3 years, 3 months ago

Cloud Shell provisions 5 GB of free persistent disk storage mounted as your \$HOME

upvoted 1 times

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

Well, I just double checked and if they were referring to the PATH variable then /usr/local/bin is also a correct answer.....

upvoted 21 times

🗨️ 👤 **RobertArnaud** Most Recent 🕒 6 days, 18 hours ago

Selected Answer: A

If "few weeks" means less than 120 days

upvoted 1 times

🗨️ 👤 **Ekramy_Elnaggar** 1 month ago

Selected Answer: A

1. Cloud Shell's home directory: ~/bin is a subdirectory within your Cloud Shell home directory. Files placed in this directory are automatically added to your PATH environment variable, making them accessible from anywhere in your Cloud Shell session.

2. Persistence: Your Cloud Shell home directory is persistent across sessions. This means any files you store there, including those in ~/bin, w remain available even if you close and reopen Cloud Shell.

3. Convenience: This option is the most straightforward. It doesn't require any extra configuration or interaction with other services.

Why D i snot correct? because /usr/local/bin: is a common directory for system-wide binaries, but in Cloud Shell, your home directory's

upvoted 2 times

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

Selected Answer: D

/usr/local/bin is the place where the files will persist across sessions.

Hence, D.

upvoted 2 times

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

A is correct!

upvoted 1 times

🗨️ 👤 **mootaa** 1 year, 10 months ago

I tested this. Although ~/bin is not in the default \$PATH, choice D is definitely not persisting across sessions.

upvoted 2 times

🗨️ 👤 **Flight1976** 1 year, 6 months ago

1. When logging in to cloud shell for the first time, the ~/bin directory does not exist

2. mkdir ~/bin

3. After re-login to the cloud shell, \$PATH will automatically add ~/bin

So A is the correct answer

upvoted 4 times

🗨️ 👤 **F122** 1 year, 11 months ago

At this moment default directory cant be set as Cloud storage bucket, so no C.

A will be correct as zonal PD with preinstalled tools 5gb available that does not timeout!

upvoted 2 times

  **omermahgoub** 1 year, 12 months ago

The recommended location for storing a custom utility file that you want to use in Cloud Shell and that should be in the default execution path and persist across sessions is option A: ~/bin.

The ~/bin directory is a personal directory that is in the default execution path for all users in Cloud Shell. Any executable files that you place in this directory will be available to you whenever you log in to Cloud Shell, and they will persist across sessions.

upvoted 3 times

  **omermahgoub** 1 year, 12 months ago

Option B: Cloud Storage is not a suitable location for storing a custom utility file that you want to use in Cloud Shell, as it is not in the default execution path and would require additional steps to make it accessible.

Option C: The /google/scripts directory is not a suitable location for storing a custom utility file, as it is not in the default execution path and is intended for use by Google Cloud system processes.

Option D: The /usr/local/bin directory is a system directory that is in the default execution path for all users, but it is not a suitable location for storing a custom utility file, as any files that you place in this directory may be deleted or overwritten during system updates.

upvoted 3 times

  **Jailbreaker** 2 years, 1 month ago

Selected Answer: A

For sure correct answer is A

upvoted 1 times

  **megumin** 2 years, 1 month ago

Selected Answer: A

ok for A

upvoted 1 times

  **minmin2020** 2 years, 2 months ago

Selected Answer: A

A. ~/bin

upvoted 1 times

  **vpatiltech** 2 years, 10 months ago

Selected Answer: A

Cloud Shell provisions 5 GB of persistent disk storage mounted as your \$HOME directory on the Cloud Shell instance. All files you store in your home directory, including scripts and user configuration files like .bashrc and .vimrc, persist between sessions.


Reference- https://cloud.google.com/shell/?utm_source=google&utm_medium=cpc&utm_campaign=japac-IN-all-en-dr-bkwsrmkt-all-all-trial-dr-1009882&utm_content=text-ad-none-none-DEV_c-CRE_442449534611-ADGP_Hybrid%20%7C%20BKWS%20-%20EXA%20%7C%20Txt%20~%20Management%20Tools%20~%20Cloud%20Shell_cloud%20shell-general%20-%20Products-KWID_43700054972141701-kwd-837034669893&userloc_9302140-network_g&utm_term=KW_gcp%20cloud%20shell&gclid=ds&gclid=ds

upvoted 4 times

  **OrangeTiger** 2 years, 11 months ago

I think D is correct. ummm

upvoted 2 times

  **vincy2202** 2 years, 11 months ago

A is the correct answer

upvoted 1 times

  **exam_war** 3 years, 1 month ago

A is for sure. ~ stands for user's home

upvoted 1 times

  **MamthaSJ** 3 years, 5 months ago

Answer is A

upvoted 1 times

Question #43



Topic 1

You want to create a private connection between your instances on Compute Engine and your on-premises data center. You require a connection of at least 20 Gbps. You want to follow Google-recommended practices. How should you set up the connection?



- A. Create a VPC and connect it to your on-premises data center using Dedicated Interconnect.
- B. Create a VPC and connect it to your on-premises data center using a single Cloud VPN.
- C. Create a Cloud Content Delivery Network (Cloud CDN) and connect it to your on-premises data center using Dedicated Interconnect.
- D. Create a Cloud Content Delivery Network (Cloud CDN) and connect it to your on-premises datacenter using a single Cloud VPN.

  **AWS56** Highly Voted 4 years, 11 months ago



Cloud VPN supports upto 3 Gbps where as Interconnect can support upto 100 gbps... I'll go with A
upvoted 45 times

  **tartar** 4 years, 4 months ago

A is ok
upvoted 7 times

  **fraloca** 3 years, 11 months ago



<https://cloud.google.com/network-connectivity/docs/vpn/concepts/overview#network-bandwidth>
upvoted 3 times

  **nitinz** 3 years, 9 months ago

A, 20Gbps dedicated interconnect is the way.
upvoted 2 times

  **AzureDP900** 2 years, 2 months ago

A is required for consistent speed and VPN not supports that speed
upvoted 2 times

  **omermahgoub** Highly Voted 1 year, 12 months ago

Answer is A: Dedicated Interconnect is a service that allows you to create a dedicated, high-bandwidth network connection between your on-premises data center and Google Cloud. It is the recommended solution for creating a private connection between your on-premises data center and Google Cloud when you require a connection of at least 20 Gbps.

Option B: Using a single Cloud VPN to connect your VPC to your on-premises data center is not suitable for a connection of at least 20 Gbps. Cloud VPN has a maximum capacity of 30 Gbps.

Option C: The Cloud Content Delivery Network (Cloud CDN) is a globally distributed network of caching servers that speeds up the delivery of static and dynamic web content. It is not suitable for creating a private connection between your instances on Compute Engine and your on-premises data center.

Option D: Connecting your Cloud CDN to your on-premises data center using a single Cloud VPN is not suitable for a connection of at least 20 Gbps, as Cloud VPN has a maximum capacity of 30 Gbps.

upvoted 13 times

  **MJCLOUD** 1 year, 9 months ago

Very nice answer, I think you meant 3 Gbps for Cloud VPN.
upvoted 4 times

  **Ekramy_Elnaggar** Most Recent 1 month ago

Selected Answer: A

1. Dedicated Interconnect for high bandwidth: Dedicated Interconnect is designed for high-bandwidth, private connections between your on-premises network and Google Virtual Private Cloud (VPC). It offers speeds of 10 Gbps up to 100 Gbps, meeting your requirement of at least 2 Gbps.

2. Private and secure connection: Dedicated Interconnect provides a direct physical connection, bypassing the public internet. This ensures a secure and private connection for your sensitive data.

3. Google-recommended practice: For demanding workloads that require high bandwidth and low latency, Google recommends Dedicated Interconnect over VPN.

upvoted 1 times

  **heretolearnazure** 1 year, 3 months ago

high bandwidth means A

upvoted 1 times

  **greyhats13** 2 years ago

Selected Answer: A

the question mention 20gbps for the least, it should be Dedicated Interconnect. The answer is A

upvoted 1 times

  **megumin** 2 years, 1 month ago

Selected Answer: A

ok for A

upvoted 1 times

  **Jay_Krish** 2 years, 3 months ago

Selected Answer: A

Any connection between On-Prem and GCP and requires high speed I'd choose dedicated interconnect

upvoted 1 times

  **avinashvidyarthi** 2 years, 7 months ago

A is correct

upvoted 1 times

  **vincy2202** 2 years, 11 months ago



A is the correct answer

upvoted 2 times

  **haroldbenites** 3 years ago

Go for A

upvoted 2 times

  **joe2211** 3 years ago

Selected Answer: A

vote A


upvoted 2 times

  **duocnh** 3 years ago

Selected Answer: A

vote A

upvoted 3 times

  **unnikrisb** 3 years, 2 months ago

A is good option (easily eliminate C & D) and B with connection speed.

10Gbps per link for Dedicated Interconnect and Direct Peering

1.5-3Gbps per tunnel for Cloud VPN

50Mbps to 10Gbps per connection - Partner Interconnect

noSLA - Carrier Peering

upvoted 1 times