





- Expert Verified, Online, **Free**.


 Custom View Settings



Topic 1 - Single Topic



Your team needs to make sure that a Compute Engine instance does not have access to the internet or to any Google APIs or services. Which two settings must remain disabled to meet these requirements? (Choose two.)



- A. Public IP
- B. IP Forwarding
- C. Private Google Access
- D. Static routes
- E. IAM Network User Role



  **KILLMAD** Highly Voted 1 year, 10 months ago
The answer is AC
upvoted 21 times



  **rafaelc** 1 year, 10 months ago
You are right
upvoted 4 times



  **Zol** Highly Voted 1 year, 10 months ago
KILLMAD
You're correct it is A C
Public IP
Private Google Access
upvoted 6 times



  **kathleen1868** Most Recent 1 week, 5 days ago
Only 5-6 questions from this dump are in the exam and all the rest are new. The EXAM VERSION gets updated without any actual update occurs on the questions here!
upvoted 3 times



  **brunobrn1** 2 weeks, 4 days ago
friends, I took the test today 12/27, if there were 5 questions here it was too much, unfortunately this dump is out of date.
upvoted 3 times



  **kathleen1868** 2 weeks, 5 days ago
Only 6 questions were from this dump. All the rest were new. I was failed :(
upvoted 4 times



  **jits1984** 4 weeks ago
I passed the exam today, only 6 questions common from this dump. All new questions.
upvoted 2 times

  **_01_** 1 month, 1 week ago
Selected Answer: AC
Public IP
Private Google Access
upvoted 1 times

  **mistryminded** 1 month, 3 weeks ago
Selected Answer: AC
Correct answer is:
upvoted 1 times

  **SuperDevops** 2 months ago
I took the test yesterday and didn't pass, NO ISSUE is from here. The questions are totally new
Whizlabs it's OK
upvoted 3 times

  **AOK08** 4 weeks, 1 day ago
I completely agree. You were right. Questions are totally new. Did not pass.
upvoted 1 times

  **SuperDevops** 2 months, 1 week ago
I took the test yesterday and didn't pass, NO ISSUE is from here. The questions are totally new
upvoted 3 times

  **gongqin1234** 2 months, 1 week ago

really? is there any other dump can share?

upvoted 2 times

  **SuperDevops** 2 months ago



Whizlabs

upvoted 1 times

  **SuperDevops** 2 months, 1 week ago

I took the test yesterday and didn't pass, NO ISSUE is from here. The questions are totally new, don't use this dump.

upvoted 4 times

  **jits1984** 2 months, 1 week ago

are these questions still relevant? Google had refreshed the topics for this certification on 15th Oct, 2021. Has anyone sat this exam after 15th Oct 2021, and passed?

upvoted 2 times



  **a_vi** 2 months, 1 week ago

Correct Answer is AC

Option A : because per GCP documentation, “Prevent internet access to instances by setting them up with only a private IP address” meaning no public IPs.



Option C: because VM instances that only have internal IP addresses (no external IP addresses) can use Private Google Access. They can reach the external IP addresses of Google APIs and services.

upvoted 2 times

  **jayk22** 2 months, 2 weeks ago

The answer is AC

upvoted 1 times

  **APATEL_12** 9 months, 3 weeks ago

Sorry A is correct

upvoted 1 times

  **APATEL_12** 9 months, 3 weeks ago

Internet access and public IP service are disabled by default

<https://cloud.google.com/vmware-engine/docs/networking/howto-setup-internet-access#:~:text=VMware%20Engine%20portal-,Select%20Network%20%3E%20Regional%20settings.,can%20disable%20public%20IP%20service.>

this is why A can not be correct

upvoted 1 times

  **bluetaurianbull** 10 months ago

For me its A and C



Google documentation is clear enough <https://cloud.google.com/vpc/docs/private-google-access>




upvoted 2 times


Which two implied firewall rules are defined on a VPC network? (Choose two.)



- A. A rule that allows all outbound connections
- B. A rule that denies all inbound connections
- C. A rule that blocks all inbound port 25 connections
- D. A rule that blocks all outbound connections
- E. A rule that allows all inbound port 80 connections



  **KILLMAD** Highly Voted  1 year, 10 months ago
I agree AB
upvoted 7 times



  **SuperDevops** 2 months, 1 week ago
I took the test yesterday and didn't pass, NO ISSUE is from here. The questions are totally new, and you?
upvoted 3 times



  **kathleen1868** Most Recent  1 week, 5 days ago
Only 5-6 questions from this dump are in the exam and all the rest are new. The EXAM VERSION gets updated without any actual update occurs on the questions here!
upvoted 1 times



  **jits1984** 4 weeks ago
only 6 questions were common in the test...all new questions. I passed, but dont follow this dump
upvoted 3 times



  **SuperDevops** 2 months, 1 week ago
I took the test yesterday and didn't pass, NO ISSUE is from here. The questions are totally new, don't use this dump.
upvoted 4 times



  **AOK08** 4 weeks, 1 day ago
Even now questions are totally new. I was suprised.
upvoted 3 times

  **DebasishLowes** 10 months, 2 weeks ago
Answer AB
upvoted 3 times

  **DebasishLowes** 10 months, 3 weeks ago
A and B
upvoted 1 times

  **[Removed]** 1 year, 2 months ago
Ans - AB
upvoted 2 times

  **saurabh1805** 1 year, 3 months ago
A and B are correct options here.
upvoted 2 times

  **ArizonaClassics** 1 year, 5 months ago
A,B is the correct answer
upvoted 4 times

Your team wants to centrally manage GCP IAM permissions from their on-premises Active Directory Service. Your team wants to manage permissions by AD group membership.
What should your team do to meet these requirements?

- A. Set up Cloud Directory Sync to sync groups, and set IAM permissions on the groups.
- B. Set up SAML 2.0 Single Sign-On (SSO), and assign IAM permissions to the groups.
- C. Use the Cloud Identity and Access Management API to create groups and IAM permissions from Active Directory.
- D. Use the Admin SDK to create groups and assign IAM permissions from Active Directory.

  **droogie** Highly Voted 1 year, 6 months ago

Answer. is A. B is just the method of authentication, all the heavy lifting is done in A
upvoted 18 times

  **johnsm** Highly Voted 10 months, 3 weeks ago

Correct Answer is A as explained here <https://www.udemy.com/course/google-security-engineer-certification/?referralCode=E90E3FF49D9DE15E2855>

"In order to be able to keep using the existing identity management system, identities need to be synchronized between AD and GCP IAM. To do so google provides a tool called Cloud Directory Sync. This tool will read all identities in AD and replicate those within GCP.

Once the identities have been replicated then it's possible to apply IAM permissions on the groups. After that you will configure SAML so google can act as a service provider and either you ADFS or other third party tools like Ping or Okta will act as the identity provider. This way you effectively delegate the authentication from Google to something that is under your control."
upvoted 8 times

  **jits1984** Most Recent 2 weeks, 1 day ago


only 6 questions came from this dump, dont follow this dump. All new questions
upvoted 2 times

  **mistryminded** 1 month, 3 weeks ago

Selected Answer: A
Correct answer is A
upvoted 1 times

  **SuperDevops** 2 months, 1 week ago

I took the test yesterday and didn't pass, NO ISSUE is from here. The questions are totally new
upvoted 2 times

  **SuperDevops** 2 months, 1 week ago

I took the test yesterday and didn't pass, NO ISSUE is from here. The questions are totally new, don't use this dump.
upvoted 2 times

  **Bhupals** 1 year ago

Reference: itself says answer is A
<https://cloud.google.com/blog/products/identity-security/using-your-existing-identity-management-system-with-google-cloud-platform>
upvoted 2 times

  **jonclem** 1 year, 2 months ago



Interestingly, the link is correct, however, the answer is wrong. I agree with the consensus of the actual answer being A.
upvoted 1 times

  **[Removed]** 1 year, 2 months ago



Ans - A
upvoted 1 times

  **saaurabh1805** 1 year, 3 months ago

A is correct option and also its best practice to use Group to manage permission
upvoted 1 times

  **aiwaai** 1 year, 4 months ago



Answer. is A
upvoted 2 times

  **bigdo** 1 year, 5 months ago

A is correct as it makes use of existing group therefore existing user and ad policy
upvoted 3 times


  **ArizonaClassics** 1 year, 5 months ago


A is the correct option
upvoted 2 times


  **xhova** 1 year, 9 months ago



B is correct
upvoted 1 times

- A. Ensure that the app does not run as PID 1.
- B. Package a single app as a container.
- C. Remove any unnecessary tools not needed by the app.
- D. Use public container images as a base image for the app.
- E. Use many container image layers to hide sensitive information.



 **jits1984** Most Recent 1 week, 5 days ago
I took the test, and only got 6 questions from this dump. The administrators won't let me comment on the main page.
upvoted 1 times



 **dopeb64075** 3 weeks, 6 days ago
I believe this guy is from Whizlabs. That platform is crap as this span. Selling Google's own free questions and lots of false questions/answers. I sent them a few corrections with references and they didn't mind to update.
upvoted 2 times



 **VenkatGCP1** 3 weeks, 6 days ago
This dude copy pasted same comment everywhere looks like someone from whizlabs trying to advertise here
upvoted 1 times

  **jits1984** 2 weeks, 1 day ago
No he is right. I appeared for the exam, earlier this month. only 6 questions from this dump. All new questions.
upvoted 1 times

 SuperDevops 2 months, 1 week ago
it is AE
upvoted 1 times

  **Jane111** 8 months, 2 weeks ago
It should be A,B
upvoted 1 times

  **WakandaF** 8 months, 3 weeks ago
So, its B C?
upvoted 1 times


  **bluetaurianbull** 10 months ago


To add to my previous comment

"A process running as PID 1 inside a container is treated specially by Linux: it ignores any signal with the default action. So, the process will not terminate on SIGINT or SIGTERM unless it is coded to do so."

Looks like this could be an issue when talking about security, a malicious coder can write a piece of code to eat all resources on the host with this one bad PID#1


What do you think guys??

 upvoted 1 times

 **lollo1234** 9 months ago

You don't usually want your container to get killed instantly - you want to see the SIGINT or SIGTERM command and respond. For example, in a webserver you may stop accepting connections, and respond to the remaining open ones, before calling `exit()`

upvoted 2 times

  **bluetaurianbull** 10 months ago
To add to my previous comment
"A process running as PID 1 inside a container is treated specially by Linux: it ignores any signal with the default action. So, the process will not terminate on SIGINT or SIGTERM unless it is coded to do so."
 upvoted 1 times



 **bluetaurianbull** 10 months ago

Really??? Wat about (A)
When the process with pid 1 die for any reason, all other processes are killed with KILL signal.

Shouldnt A be one of the biggest risk when we talk about container security???

upvoted 2 times

  **kubosuke** 10 months ago

bc of bc

upvoted 1 times

  **[Removed]** 1 year, 2 months ago

Ans - BC

upvoted 1 times

  **saurabh1805** 1 year, 3 months ago

vote for B and C

upvoted 1 times

  **MohitA** 1 year, 4 months ago

BC for sure

upvoted 1 times

  **ArizonaClassics** 1 year, 5 months ago

BC on point!

upvoted 2 times


  **KILLMAD** 1 year, 10 months ago




I agree BC

upvoted 4 times



A customer needs to launch a 3-tier internal web application on Google Cloud Platform (GCP). The customer's internal compliance requirements dictate that end- user access may only be allowed if the traffic seems to originate from a specific known good CIDR. The customer accepts the risk that their application will only have SYN flood DDoS protection. They want to use GCP's native SYN flood protection. Which product should be used to meet these requirements?



- A. Cloud Armor
- B. VPC Firewall Rules
- C. Cloud Identity and Access Management
- D. Cloud CDN



  **KILLMAD** Highly Voted  1 year, 10 months ago
Answer is A
upvoted 10 times



  **ThisisJohn** Most Recent  3 weeks, 3 days ago
Selected Answer: A
If there were at least a L4 load balancer in the picture, I'd vote for B, since then the LB would take care of "GCP's native SYN flood protection", also considering that "The customer accepts the risk that their application will only have SYN flood DDoS protection.".



With cloud armor I guess they get more protection that required on the question, but it seems to be the only entry that fulfills the requirements
upvoted 1 times



  **SuperDevops** 2 months ago
I took the test yesterday and didn't pass, NO ISSUE is from here. The questions are totally new
Whizlabs > exam
upvoted 1 times



  **DebasishLowes** 10 months, 3 weeks ago
Ans : A
upvoted 1 times

  **Bharathy** 1 year, 1 month ago
Cloud Armour supports ip range (CIDR) and also custom types can be defined using Armour Rule Language termed as CEL (Common Expression Language). Option A is correct
upvoted 1 times



  **[Removed]** 1 year, 2 months ago
Ans - A
upvoted 1 times

  **saurabh1805** 1 year, 3 months ago
A is correct answer.
upvoted 1 times

  **zee001** 1 year, 3 months ago
A is correct !
upvoted 1 times

  **Ved** 1 year, 3 months ago
Ans is A
upvoted 1 times

  **MohitA** 1 year, 4 months ago
A , you can specify allowed CIDR range of IP allowed
upvoted 1 times

  **ArizonaClassics** 1 year, 5 months ago
A is perfect!
upvoted 2 times

A company is running workloads in a dedicated server room. They must only be accessed from within the private company network. You need to connect to these workloads from Compute Engine instances within a Google Cloud Platform project.

Which two approaches can you take to meet the requirements? (Choose two.)

- A. Configure the project with Cloud VPN.
- B. Configure the project with Shared VPC.
- C. Configure the project with Cloud Interconnect.
- D. Configure the project with VPC peering.
- E. Configure all Compute Engine instances with Private Access.

🗲️ 👤 **KILLMAD** Highly Voted 👍 1 year, 10 months ago

AC makes the most sense

upvoted 20 times

🗲️ 👤 **rafaelc** 1 year, 10 months ago

Again you are correct

upvoted 1 times

🗲️ 👤 **SuperDevops** Most Recent ⌚ 2 months, 1 week ago

I took the test yesterday and didn't pass, NO ISSUE is from here. The questions are totally new, don't use this dump.

upvoted 1 times

🗲️ 👤 **DebasishLowes** 10 months, 3 weeks ago

Ans is AC

upvoted 4 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

AC

<https://cloud.google.com/solutions/secure-data-workloads-use-cases#gateway-for-hybrid>

https://cloud.google.com/solutions/secure-data-workloads-gcp-products#cloud_vpn

upvoted 3 times

🗲️ 👤 **saaurabh1805** 1 year, 3 months ago

A and C are correct answer here.

upvoted 2 times

🗲️ 👤 **Rantu** 1 year, 3 months ago

AC is the answer.

upvoted 2 times

🗲️ 👤 **zee001** 1 year, 3 months ago

I checked GCP documentation and it states that to you can use either Cloud VPN or Cloud Interconnect to securely connect your on-premises network to your VPC network

upvoted 3 times

🗲️ 👤 **MohitaA** 1 year, 4 months ago

Private Access won't help, AC is the answer

upvoted 1 times

🗲️ 👤 **aiwaai** 1 year, 4 months ago

Correct Answer: A, C

upvoted 1 times

🗲️ 👤 **bigdo** 1 year, 5 months ago

Ac A allow access to on-premise private ip address space with vpc with cloud interconnect they can access private private ip address space layer 2

upvoted 1 times

🗲️ 👤 **bigdo** 1 year, 5 months ago



CE peering is on gcp vpc only options



upvoted 2 times

🗲️ 👤 **bigdo** 1 year, 5 months ago

CD peering is on gcp vpc only options

upvoted 1 times

  **soukumar369** 1 year, 1 month ago
Again you are wrong
upvoted 2 times




  **ArizonaClassics** 1 year, 5 months ago
AC as well
upvoted 2 times




Question #7

Topic 1




A customer implements Cloud Identity-Aware Proxy for their ERP system hosted on Compute Engine. Their security team wants to add a security layer so that the ERP systems only accept traffic from Cloud Identity-Aware Proxy.
What should the customer do to meet these requirements?



- A. Make sure that the ERP system can validate the JWT assertion in the HTTP requests.
- B. Make sure that the ERP system can validate the identity headers in the HTTP requests.
- C. Make sure that the ERP system can validate the x-forwarded-for headers in the HTTP requests.
- D. Make sure that the ERP system can validate the user's unique identifier headers in the HTTP requests.



  **ArizonaClassics** Highly Voted  1 year, 5 months ago
A is right see : <https://cloud.google.com/iap/docs/signed-headers-howto>
upvoted 11 times



  **bolu** Highly Voted  11 months, 3 weeks ago
Use Cryptographic Verification
If there is a risk of IAP being turned off or bypassed, your app can check to make sure the identity information it receives is valid. This uses a third web request header added by IAP, called X-Goog-IAP-JWT-Assertion. The value of the header is a cryptographically signed object that also contains the user identity data. Your application can verify the digital signature and use the data provided in this object to be certain that it was provided by IAP without alteration.



So answer is A
upvoted 5 times



  **SuperDevops** Most Recent  2 months ago
I took the test yesterday and didn't pass, NO ISSUE is from here. The questions are totally new
Whizlabs it's OK
upvoted 1 times



  **sc_cloud_learn** 7 months, 3 weeks ago
Agree A makes more sense
upvoted 3 times

  **DebasishLowes** 10 months, 3 weeks ago
Ans is A
upvoted 3 times

  **[Removed]** 1 year, 2 months ago
Ans - A
upvoted 1 times

  **saurabh1805** 1 year, 3 months ago
A is correct option here.
upvoted 1 times

  **MohitA** 1 year, 4 months ago
A is the one
upvoted 1 times

  **KILLMAD** 1 year, 10 months ago
Ans is A
upvoted 4 times

A company has been running their application on Compute Engine. A bug in the application allowed a malicious user to repeatedly execute a script that results in the Compute Engine instance crashing. Although the bug has been fixed, you want to get notified in case this hack re-occurs. What should you do?

- A. Create an Alerting Policy in Stackdriver using a Process Health condition, checking that the number of executions of the script remains below the desired threshold. Enable notifications.
- B. Create an Alerting Policy in Stackdriver using the CPU usage metric. Set the threshold to 80% to be notified when the CPU usage goes above this 80%.
- C. Log every execution of the script to Stackdriver Logging. Create a User-defined metric in Stackdriver Logging on the logs, and create a Stackdriver Dashboard displaying the metric.
- D. Log every execution of the script to Stackdriver Logging. Configure BigQuery as a log sink, and create a BigQuery scheduled query to count the number of executions in a specific timeframe.

🗲️ 👤 **rafaelc** Highly Voted 👍 1 year, 10 months ago

The question asks "you want to get notified in case this hack re-occurs."

Only A has notifications in the answer so that should be the answer as having dashboards in stackdriver wont notify you of anything.
upvoted 15 times

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

I agree it should be A

upvoted 5 times

🗲️ 👤 **serg3d** Highly Voted 👍 1 year, 6 months ago

It's not necessary that running a malicious script multiple times will affect CPU usage. And, CPU usage can occur during usual normal workloads.

A

upvoted 5 times

🗲️ 👤 **SuperDevops** Most Recent ⌚ 2 months, 1 week ago

I took the test yesterday and didn't pass, NO ISSUE is from here. The questions are totally new, don't use this dump.

upvoted 1 times

🗲️ 👤 **jits1984** 1 month ago

What are you saying, where should we go for new dumps @SuperDevops?

upvoted 1 times

🗲️ 👤 **Jane111** 8 months, 2 weeks ago

The bug has been fixed, so even if somebody runs the same script, it will affect nothing. Checking against the same script, creating Process-health policy will do nothing. But if the hack reappears and the same script is run, the A will trigger

upvoted 3 times

🗲️ 👤 **Jane111** 8 months, 2 weeks ago

The bug has been fixed, so even if somebody runs the same script, it will affect nothing. Checking against the same script, creating Process-health policy will do nothing

upvoted 2 times

🗲️ 👤 **Jane111** 8 months, 2 weeks ago

There is no 'Process Health condition' but Process-health policy

A process-health policy can notify you if the number of processes that match a pattern crosses a threshold. This can be used to tell you, for example, that a process has stopped running.

This policy sends a notification to the specified notification channel when no process matching the string nginx, running as user www, has been available for more than 5 minutes:

upvoted 1 times

🗲️ 👤 **DebasishLowes** 10 months, 3 weeks ago

Ans : A

upvoted 1 times

🗲️ 👤 **soukumar369** 1 year ago

A. Correct

B. "CPU usage goes above this 80%". It's not granted that script execution will increase CPU usage.

C&D. Not providing any notification

upvoted 3 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

A
<https://cloud.google.com/monitoring/alerts/types-of-conditions#metric-threshold>
upvoted 2 times

🗨️ 👤 **saurabh1805** 1 year, 3 months ago
A seems to be closest and best option.
upvoted 2 times

🗨️ 👤 **saurabh1805** 1 year, 2 months ago
<https://cloud.google.com/monitoring/alerts/ui-conditions-ga#process-health>
upvoted 1 times

🗨️ 👤 **zee001** 1 year, 3 months ago
I think the answer is B based on the article I found on Medium, which states that Metrics are used to represent the state or health of your system over time, and In Stackdriver specifically, metrics are the only kind of data that can be used to create alerts via alerting policies. The question is also asking about monitoring the health of system.
<https://medium.com/google-cloud/can-you-alert-on-logs-in-stackdriver-7dfb07f495c0>
upvoted 1 times

🗨️ 👤 **SA1** 1 year, 3 months ago
Looks B to me. Not sure what is "Process Health condition".
upvoted 1 times

🗨️ 👤 **Mohita** 1 year, 4 months ago
The suggested answer is wrong, ask is for alerting, A is the best match
upvoted 3 times

🗨️ 👤 **aiwaai** 1 year, 4 months ago
Answer. is A
upvoted 3 times


🗨️ 👤 **gcp_learner** 1 year, 6 months ago
I agree that the answer should be B because the question asks for alerts. I'd choose to to receive alerts when CPU exceed a threshold
upvoted 3 times


🗨️ 👤 **mozammil89** 1 year, 10 months ago
I think the answer should be, B.
upvoted 3 times

Your team needs to obtain a unified log view of all development cloud projects in your SIEM. The development projects are under the NONPROD organization folder with the test and pre-production projects. The development projects share the ABC-BILLING billing account with the rest of the organization.


Which logging export strategy should you use to meet the requirements?


- A. 1. Export logs to a Cloud Pub/Sub topic with folders/NONPROD parent and includeChildren property set to True in a dedicated SIEM project. 2. Subscribe SIEM to the topic.
- B. 1. Create a Cloud Storage sink with billingAccounts/ABC-BILLING parent and includeChildren property set to False in a dedicated SIEM project. 2. Process Cloud Storage objects in SIEM.
- C. 1. Export logs in each dev project to a Cloud Pub/Sub topic in a dedicated SIEM project. 2. Subscribe SIEM to the topic.
- D. 1. Create a Cloud Storage sink with a publicly shared Cloud Storage bucket in each project. 2. Process Cloud Storage objects in SIEM.


🗲️  **xhova** Highly Voted 👍 1 year, 9 months ago
Answer is A. https://cloud.google.com/logging/docs/export/aggregated_sinks
upvoted 20 times

🗲️  **TNT87** Highly Voted 👍 10 months, 4 weeks ago
To use the aggregated sink feature, create a sink in a Google Cloud organization or folder and set the sink's includeChildren parameter to True. That sink can then export log entries from the organization or folder, plus (recursively) from any contained folders, billing accounts, or projects. You can use the sink's filter to specify log entries from projects, resource types, or named logs.
https://cloud.google.com/logging/docs/export/aggregated_sinks


so the Ans is A
upvoted 6 times

🗲️  **Lancyqusa** Most Recent 🕒 3 weeks, 3 days ago
"Your team needs to obtain a unified log view of all development cloud projects in your SIEM" - This means we are ONLY interested in development projects.
"The development projects are under the NONPROD organization folder with the test and pre-production projects" - We will need to filter out development from others i.e test and pre-prod.
"The development projects share the ABC-BILLING billing account with the rest of the organization." - This is unnecessary information.
The only option that filters the log is C - so the answer must be C.
upvoted 1 times

🗲️  **SuperDevops** 2 months, 1 week ago
I took the test yesterday and didn't pass, NO ISSUE is from here. The questions are totally new, don't use this dump.
upvoted 2 times


🗲️  **KyubiBlaze** 4 months ago
Guys, C is the answer.
A - NO, This will bring in test and pre-prod as well, this does not solve our problem
B - NO, This has nothing to do with the question,
C - YES- Specifically take development projects, and centralises the logs
D - Once the work public comes in answer, it is wrong.


Request the admins to set answer to C
This is seriously a simple question
upvoted 1 times

🗲️  **[Removed]** 10 months ago
A is the answer.
To use the aggregated sink feature, create a sink in a Google Cloud organization or folder and set the sink's includeChildren parameter to True. That sink can then export log entries from the organization or folder, plus (recursively) from any contained folders, billing accounts, or projects. You can use the sink's filter to specify log entries from projects, resource types, or named logs.



Please note that sinks filters can be used to get exact logs required and the given requirement from the question will be fulfilled.



https://cloud.google.com/logging/docs/export/aggregated_sinks
upvoted 3 times



🗲️  **[Removed]** 1 year, 2 months ago
Ans may be A or C.
A- not very cost effective and need filtering
C - Tedious to create for all dev projects
upvoted 3 times



🗲️  **saurabh1805** 1 year, 3 months ago
I will vote for option C.

upvoted 2 times

  **MohitA** 1 year, 4 months ago
A because it's more selective and adds only projects below NONPROD folder
upvoted 2 times

  **aiwaai** 1 year, 4 months ago
Correct Answer: A
upvoted 1 times



  **bigdo** 1 year, 5 months ago
c is the ans A export log with recursive option c is selective
upvoted 1 times



  **Sheeda** 1 year, 5 months ago
Atleast B is false. See this link.



https://cloud.google.com/logging/docs/export/aggregated_sinks



Without the aggregated sink feature, sinks are limited to exporting log entries from the exact resource in which the sink was created: a Google Cloud project, organization, folder, or billing account.



To use the aggregated sink feature, create a sink in a Google Cloud organization or folder and set the sink's includeChildren parameter to True. That sink can then export log entries from the organization or folder, plus (recursively) from any contained folders, billing accounts, or projects. You can use the sink's query to specify log entries from projects, resource types, or named logs.
upvoted 1 times



  **dg63** 1 year, 5 months ago
I think the only feasible answer is C. State goal is to provide a unified log view of ALL development cloud projects.
A Approach A won't work as this will send logs for test as well as pre-prod projects also to the SIEM.
B Approach B won't work as this will send logs for all projects (billing code is shared with rest of the organization) to the SIEM.
C This is only feasible approach. I will prefer to filter logs based on a tag or some other property.
D Approach D will send data for every project to SIEM. We only want dev projects.
upvoted 1 times

  **Sheeda** 1 year, 5 months ago
I second you. A, B and D for sure are wrong.
upvoted 1 times

  **ArizonaClassics** 1 year, 5 months ago
I would go with option B
upvoted 1 times

  **rafaelc** 1 year, 10 months ago
I think it is A
upvoted 3 times

  **jonclem** 1 year, 9 months ago
Why is it you think the answer is A?
upvoted 1 times

  **KILLMAD** 1 year, 10 months ago
ans is B
upvoted 2 times

A customer needs to prevent attackers from hijacking their domain/IP and redirecting users to a malicious site through a man-in-the-middle attack.

Which solution should this customer use?

- A. VPC Flow Logs
- B. Cloud Armor
- C. DNS Security Extensions
- D. Cloud Identity-Aware Proxy

🗲️ 👤 **ESP_SAP** Highly Voted 👍 1 year, 1 month ago

Correct Answer is (C):

DNSSEC — use a DNS registrar that supports DNSSEC, and enable it. DNSSEC digitally signs DNS communication, making it more difficult (but not impossible) for hackers to intercept and spoof.

Domain Name System Security Extensions (DNSSEC) adds security to the Domain Name System (DNS) protocol by enabling DNS responses to be validated. Having a trustworthy Domain Name System (DNS) that translates a domain name like www.example.com into its associated IP address is an increasingly important building block of today's web-based applications. Attackers can hijack this process of domain/IP lookup and redirect users to a malicious site through DNS hijacking and man-in-the-middle attacks. DNSSEC helps mitigate the risk of such attacks by cryptographically signing DNS records. As a result, it prevents attackers from issuing fake DNS responses that may misdirect browsers to nefarious websites.

<https://cloud.google.com/blog/products/gcp/dnssec-now-available-in-cloud-dns>

upvoted 8 times

🗲️ 👤 **shreenine** Most Recent 🕒 3 months, 2 weeks ago

C is the correct answer indeed.

upvoted 2 times

🗲️ 👤 **Kameswara** 7 months, 2 weeks ago

C. Attackers can hijack this process of domain/IP lookup and redirect users to a malicious site through DNS hijacking and man-in-the-middle attacks. DNSSEC helps mitigate the risk of such attacks by cryptographically signing DNS records. As a result, it prevents attackers from issuing fake DNS responses that may misdirect browsers to nefarious websites.

upvoted 4 times

🗲️ 👤 **sc_cloud_learn** 7 months, 3 weeks ago

C. DNSSEC is the ans

upvoted 2 times

🗲️ 👤 **ASG** 11 months ago

Its man in the middle attack protection. The traffic first needs to reach cloud armour before you can make use of cloud armour related protection. DNS can be hijacked if you dont use DNSSEC. Its your DNS that needs to resolve the initial request before traffic is directed to cloud armour. Option C is most appropriate measure. (think of sequencing of how traffic will flow)

upvoted 3 times

🗲️ 👤 **bolu** 11 months, 3 weeks ago

The answers from rest of the folks are complete unreliable. The right answer is Cloud Armor based on my Hands-On labs in Qwiklabs. Reason: Creating a policy in Cloud Armor sends 403 forbidden message for man-in-the middle-attack. Reference: <https://cloud.google.com/blog/products/identity-security/identifying-and-protecting-against-the-largest-ddos-attacks> Some more: <https://cloud.google.com/armor> Refer this lab: https://www.qwiklabs.com/focuses/1232?catalog_rank=%7B%22rank%22%3A1%2C%22num_filters%22%3A0%2C%22has_search%22%3Atrue%7D&parent=catalog&search_id=8696512

upvoted 2 times

🗲️ 👤 **KyubiBlaze** 4 months ago

No, C is the correct answer.

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - C

upvoted 2 times

🗲️ 👤 **saurabh1805** 1 year, 3 months ago


DNSEC is the thing, Option C

upvoted 2 times


🗲️ 👤 **Mohita** 1 year, 4 months ago

C, Yes for sure DNSSEC


upvoted 2 times

-  **bigdo** 1 year, 5 months ago

C DNSSEC

upvoted 2 times
-  **ArizonaClassics** 1 year, 5 months ago

Option C is Perfect. DNSSECURITY!

upvoted 2 times
-  **KILLMAD** 1 year, 10 months ago

I agree it's C


upvoted 1 times


Question #11

Topic 1

A customer deploys an application to App Engine and needs to check for Open Web Application Security Project (OWASP) vulnerabilities. Which service should be used to accomplish this?


- A. Cloud Armor
- B. Google Cloud Audit Logs
- C. Cloud Security Scanner
- D. Forseti Security


-  **desertlotus1211**

Highly Voted 

 9 months ago


The answer is C, BUT it's now called Web Security Scanner....

upvoted 11 times
-  **DebasishLowes**


Most Recent 

 10 months, 3 weeks ago


Ans is C

upvoted 3 times
-  **[Removed]** 1 year, 2 months ago


Ans - C

upvoted 2 times
-  **saurabh1805** 1 year, 3 months ago

C is correct answer

upvoted 2 times
-  **KILLMAD** 1 year, 10 months ago

Ans is C

upvoted 4 times
-  **MohitA** 1 year, 4 months ago

Agree C is the answer

upvoted 2 times

A customer's data science group wants to use Google Cloud Platform (GCP) for their analytics workloads. Company policy dictates that all data must be company-owned and all user authentications must go through their own Security Assertion Markup Language (SAML) 2.0 Identity Provider (IdP). The Infrastructure Operations Systems Engineer was trying to set up Cloud Identity for the customer and realized that their domain was already being used by G Suite. How should you best advise the Systems Engineer to proceed with the least disruption?

- A. Contact Google Support and initiate the Domain Contestation Process to use the domain name in your new Cloud Identity domain.
- B. Register a new domain name, and use that for the new Cloud Identity domain.
- C. Ask Google to provision the data science manager's account as a Super Administrator in the existing domain.
- D. Ask customer's management to discover any other uses of Google managed services, and work with the existing Super Administrator.

  **TNT87** Highly Voted 1 year, 2 months ago

The answer is A

"This domain is already in use"

If you receive this message when trying to sign up for a Google service, it might be because:

You recently removed this domain from another managed Google account. It can take 24 hours (or 7 days if you purchased your account from a reseller) before you can use the domain with a new account.

You or someone in your organization already created a managed Google account with your domain. Try resetting the administrator password and we'll send an email to the secondary email you provided when you signed up, telling you how to access the account.

You're using the domain with another managed Google account that you own. If so, remove the domain from the other account.

Contact us

If none of these applies, the previous owner of your domain might have signed up for a Google service. Fill out this form and the Support team will get back to you within 48 hours.

upvoted 8 times

  **lollo1234** 9 months ago

Answer is D - there is no evidence that the account is lost, or similar. In a large corp it is very possible that someone (the IT org) has registered with google, and the Data science Department simply haven't been given access to it yet.

upvoted 9 times

  **syllox** Highly Voted 8 months, 2 weeks ago

Ans :D

upvoted 7 times

  **SuperDevops** Most Recent 2 months, 1 week ago

I took the test yesterday and didn't pass, NO ISSUE is from here. The questions are totally new, don't use this dump.

upvoted 1 times

  **idtroo** 9 months, 3 weeks ago

Answer is D.

<https://support.google.com/cloudidentity/answer/7389973>

If you're an existing Google Workspace customer

Follow these steps to sign up for Cloud Identity Premium:

Using your administrator account, sign in to the Google Admin console at admin.google.com.

From the Admin console Home page, at the top left, click Menu "" and then Billing and then Get more services.

Click Cloud Identity.

Next to Cloud Identity Premium, click Start Free Trial.

Follow the guided instructions.

upvoted 5 times

  **TNT87** 10 months, 4 weeks ago

Sorry Ans is D

upvoted 5 times

  **CloudTrip** 11 months ago

A, B are definitely not the answer for this. Most of you are aligned with D but can somebody explain what is wrong with C ? Their domain is already used by the G-Suite. It will be least disruptive also.

upvoted 1 times

  **lollo1234** 9 months ago

Principle of least privilege - should the 'data science manager' be a superadmin?? Probably not. Hence D, work with the existing admin - we assume that they were chosen sensibly.

upvoted 1 times

🗨️ 👤 **ronron89** 1 year, 1 month ago

I think its D.

@SomabrataPani: did you pass this exam yet?

upvoted 2 times

🗨️ 👤 **[Removed]** 1 year, 2 months ago

Ans - D

upvoted 2 times

🗨️ 👤 **saurabh1805** 1 year, 3 months ago

D is best answer here.

upvoted 2 times

🗨️ 👤 **aiwaai** 1 year, 4 months ago

Answer. is D

upvoted 2 times

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

I am considering B or D but still needs some narrowing down to choose the right answer

upvoted 1 times

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

If SAML is already used and configured, then Google support won't be able to add a new account since it doesn't manage the user directory.

Answer is D

upvoted 2 times

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

if domain already in use then you cant release that, you need to request google to assign admin rights after verification steps as you owner of that domain,

upvoted 2 times

🗨️ 👤 **xhova** 1 year, 9 months ago

B is wrong. The question statea least disruptive

upvoted 1 times

🗨️ 👤 **rafaelc** 1 year, 10 months ago

I don't think google can go around changing IAM permission in accounts they don't own so it cannot be C.

upvoted 2 times

🗨️ 👤 **rafaelc** 1 year, 10 months ago

I would say B or D. B being the easiest

upvoted 1 times

🗨️ 👤 **rafaelc** 1 year, 10 months ago

Actually D since you have to use the existing SAML

upvoted 4 times

A business unit at a multinational corporation signs up for GCP and starts moving workloads into GCP. The business unit creates a Cloud Identity domain with an organizational resource that has hundreds of projects.

Your team becomes aware of this and wants to take over managing permissions and auditing the domain resources.

Which type of access should your team grant to meet this requirement?

- A. Organization Administrator
- B. Security Reviewer
- C. Organization Role Administrator
- D. Organization Policy Administrator

🗲️ 👤 **ffdd1234** Highly Voted 👍 11 months, 4 weeks ago

Answer A > Its the only one that allow you to manage permissions on the projects
answer B > dont have any iam set permission so is not correct
C > organizationRoleAdmin let you only create custom roles, you cant assign it to anyone (so with thisone you cant manage permissions just create roles)
D> org policyes are for manage the ORG policies constrains , that is not about project permissions,
for me the correct is A
upvoted 8 times

🗲️ 👤 **zanhsieh** Highly Voted 👍 1 year ago

C. After carefully review this link:
<https://cloud.google.com/iam/docs/understanding-roles>
my opinion is based on 'the least privilege' practice, that future domain shall not get granted automatically:
A - Too broad permissions. The question asked "The business unit creates a Cloud Identity domain..." does not imply your team should be granted for ALL future domain(s) (domain = folder) permission management.
B - Security Reviewer does not have "set*" permission. All this role could do is just looking, not management.
C - The best answer so far. Only the domain current created and underneath iam role assignment as well as change.
D - Too broad permissions on the organization level. In other words, this role could make policy but future domains admin could hijack the role names / policies to do not desired operations.
upvoted 8 times

🗲️ 👤 **Lancyqusa** Most Recent 🕒 3 weeks, 3 days ago

The answer must be A - check out the example that allows the CTO to setup permissions for the security team:
https://cloud.google.com/iam/docs/job-functions/auditing#scenario_operational_monitoring
upvoted 1 times

🗲️ 👤 **OSNG** 4 months, 2 weeks ago

Its A.
They are looking for Domain Resources Management i.e. Projects, Folders, Permissions. and only Organization Administrator is the only option allows it. Moreover, Organization Administrator is the only option that falls under "Used IN: Resource Manager"
roles/resourcemanager.organizationAdmin
upvoted 1 times

🗲️ 👤 **[Removed]** 9 months, 4 weeks ago

C is the answer.
Here are the permissions available to organizationRoleAdmin

```
iam.roles.create
iam.roles.delete
iam.roles undelete
iam.roles.get
iam.roles.list
iam.roles.update
resourcemanager.projects.get
resourcemanager.projects.getIamPolicy
resourcemanager.projects.list
resourcemanager.organizations.get
resourcemanager.organizations.getIamPolicy
```

There are sufficient as per least privilege policy. You can do user management as well as auditing.
upvoted 2 times

🗲️ 👤 **[Removed]** 9 months, 4 weeks ago
link - <https://cloud.google.com/iam/docs/understanding-custom-roles>
upvoted 1 times

🗲️ 👤 **DebasishLowes** 10 months ago

Ans : D. As it's related to Resources, so definitely policy comes into picture.
upvoted 1 times

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

Correct is D

<https://cloud.google.com/resource-manager/docs/organization-policy/overview>

upvoted 2 times

🗨️ 👤 **Bhupals** 1 year ago

Role Permissions

roles/iam.organizationRoleAdmin iam.roles.create

iam.roles.delete

iam.roles undelete

iam.roles.get

iam.roles.list

iam.roles.update

resourcemanager.projects.get

resourcemanager.projects.getIamPolicy

resourcemanager.projects.list

resourcemanager.organizations.get

resourcemanager.organizations.getIamPolicy

upvoted 1 times

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

The confusion here, in my opinion, is that the question is asking for the ability to manage roles & audit _DOMAIN_ resources.

Domain resources in the GCP hierarchy are folders & projects, because those are the only things that can be directly under an Organization (aka Domain).

The Organization Role Admin is the option that gives you the ability to manage custom roles & list folders & projects.

upvoted 4 times

🗨️ 👤 **jonclem** 1 year, 2 months ago

Organization Policy Administrator has 2 assigned permissions: orgpolicy.policy.get

orgpolicy.policy.set

Organization Role Administrator has 11 assigned permissions: iam.roles.create, iam.roles.delete, iam.roles.get, iam.roles.list, iam.roles undelete,

iam.roles.update, resourcemanager.organizations.get, resourcemanager.organizations.getIamPolicy, resourcemanager.projects.get,

resourcemanager.projects.getIamPolicy, resourcemanager.projects.list,

While Security Review has over 700 permissions assigned to it.

With the question focusing on managing permissions and auditing I'd be inclined to go with option B: Security Reviewer.

upvoted 2 times

🗨️ 👤 **saaurabh1805** 1 year, 2 months ago

D is correct answer here.

<https://cloud.google.com/resource-manager/docs/organization-policy/overview>

upvoted 1 times

🗨️ 👤 **genesis3k** 1 year, 2 months ago

Correct answer is D as the question is referring to 'what' (i.e. resources), not 'who' (i.e. role of a user/service account). Here is an excerpt from "Differences from Identity and Access Management" section:

"Identity and Access Management focuses on who, and lets the administrator authorize who can take action on specific resources based on permissions.

Organization Policy focuses on what, and lets the administrator set restrictions on specific resources to determine how they can be configured."

at

<https://cloud.google.com/resource-manager/docs/organization-policy/overview>

upvoted 1 times

🗨️ 👤 **[Removed]** 1 year, 2 months ago

Ans - C

https://cloud.google.com/iam/docs/understanding-custom-roles#organization_role_administrator_role

upvoted 2 times

🗨️ 👤 **HectorLeon2099** 1 year, 3 months ago

Answer is A. Is the only one that lets you auditing resources.

upvoted 1 times

🗨️ 👤 **CHECK666** 1 year, 3 months ago

C is correct

upvoted 1 times

🗨️ 👤 **mlyu** 1 year, 4 months ago

Answer is not C, should be D

The problem should be "who" has or not the right to use GCP service, but not what service is restricted.

Caption from Google, "Organization Policy focuses on what, and lets the administrator set restrictions on specific resources to determine how they can be configured."

https://cloud.google.com/resource-manager/docs/organization-policy/overview#differences_from_iam

upvoted 2 times

🗨️ 👤 **Mohita** 1 year, 4 months ago

My best answer would be C, it serves the purpose. since there is no mention of constraints.

upvoted 1 times

An application running on a Compute Engine instance needs to read data from a Cloud Storage bucket. Your team does not allow Cloud Storage buckets to be globally readable and wants to ensure the principle of least privilege.

Which option meets the requirement of your team?

- A. Create a Cloud Storage ACL that allows read-only access from the Compute Engine instance's IP address and allows the application to read from the bucket without credentials.
- B. Use a service account with read-only access to the Cloud Storage bucket, and store the credentials to the service account in the config of the application on the Compute Engine instance.
- C. Use a service account with read-only access to the Cloud Storage bucket to retrieve the credentials from the instance metadata.
- D. Encrypt the data in the Cloud Storage bucket using Cloud KMS, and allow the application to decrypt the data with the KMS key.

🗨️ 👤 **ESP_SAP** Highly Voted 👍 1 year, 1 month ago

Correct Answer is (B):

If your application runs inside a Google Cloud environment that has a default service account, your application can retrieve the service account credentials to call Google Cloud APIs. Such environments include Compute Engine, Google Kubernetes Engine, App Engine, Cloud Run, and Cloud Functions. We recommend using this strategy because it is more convenient and secure than manually passing credentials.

Additionally, we recommend you use Google Cloud Client Libraries for your application. Google Cloud Client Libraries use a library called Application Default Credentials (ADC) to automatically find your service account credentials. ADC looks for service account credentials in the following order:

<https://cloud.google.com/docs/authentication/production#automatically>

upvoted 5 times

🗨️ 👤 **ChewB666** 1 year, 1 month ago

Hello guys!

Does anyone have the rest of the questions to share? :(
I can't see the rest of the issues because of the subscription.

upvoted 1 times

🗨️ 👤 **jj_618** Most Recent 🕒 3 months, 3 weeks ago

So is it B or C?

upvoted 1 times

🗨️ 👤 **bolu** 11 months, 2 weeks ago

Answer can be either B or C due to the relevance to servicing account. But storing password in app is a worst practice and we read it several times everywhere online hence it results in C as a best answer to handle service account through metadata

upvoted 3 times

🗨️ 👤 **[Removed]** 1 year, 2 months ago

Ans - C

upvoted 1 times

🗨️ 👤 **HectorLeon2099** 1 year, 3 months ago

I'll go with B.

A - ACL's are not able to allow access based on IP

C - If you store the credentials in the metadata those will be public accessible by everyone with project access.

D - Too complex

upvoted 4 times

🗨️ 👤 **saurabh1805** 1 year, 3 months ago

Yes B is best possible option. This is something google also recommnd.

<https://cloud.google.com/storage/docs/authentication#libauth>

upvoted 2 times

🗨️ 👤 **CHECK666** 1 year, 3 months ago

c is correct

upvoted 1 times

🗨️ 👤 **Moe666** 1 year, 3 months ago

C is the answer

upvoted 1 times

🗨️ 👤 **mlyu** 1 year, 4 months ago

Hi guys, How do we handle the requirement "does not allow Cloud Storage buckets to be globally readable"? seems none of the answers mention about it

upvoted 1 times

  **rakeshvardan** 1 year, 4 months ago

You most likely want to use ACLs if you need to customize access to individual objects within a bucket, since IAM permissions apply to all objects within a bucket. However, you should still use IAM for any access that is common to all objects in a bucket, because this reduces the amount of micro-managing you have to do.

A - as per the above documentation ACLs are needed for specific objects inside bucket.

B - credentials for the service account shouldn't be stored in the app

D - there is no requirement to encrypt the storage data

Hence C seems to be the correct one

upvoted 2 times

  **ArizonaClassics** 1 year, 5 months ago

I agree with C

upvoted 2 times

  **MohitA** 1 year, 4 months ago

Yup C is the right one

upvoted 1 times

An organization's typical network and security review consists of analyzing application transit routes, request handling, and firewall rules. They want to enable their developer teams to deploy new applications without the overhead of this full review. How should you advise this organization?

- A. Use Forseti with Firewall filters to catch any unwanted configurations in production.
- B. Mandate use of infrastructure as code and provide static analysis in the CI/CD pipelines to enforce policies.
- C. Route all VPC traffic through customer-managed routers to detect malicious patterns in production.
- D. All production applications will run on-premises. Allow developers free rein in GCP as their dev and QA platforms.

🗨️  **bluetaurianbull** Highly Voted 👍 9 months, 3 weeks ago

@TNT87 and others, if you say (B) or even (C) or (A) can you provide proof and URLs to support your claims. Simply saying if you have done Cloud Architect you will know Everything under the sun is not the proper response, this is a discussion and a community here trying to learn. Not everyone will be in same standard or level.
Be helpful for others please....
upvoted 11 times

🗨️  **xhova** Highly Voted 👍 1 year, 9 months ago

Answer is A

<https://cloud.google.com/solutions/partners/forseti-firewall-rules-anomalies>

upvoted 6 times

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

It doesn't cover routes and request handling checks, as mentionned in the question. So correct answer should be B.
upvoted 5 times

🗨️  **ThisisJohn** Most Recent 🕒 1 month ago

Selected Answer: B

My vote goes to B by discard.

A) only mentions firewall rules, but nothing about network routes, and nothing on Forseti website either <https://forsetisecurity.org/about/>
C) Talks about malicious patterns, not about network routes, requests handling and patterns, like the question says
D) Running on-prem doesn't guarantee a higher level of control

Thus, the only answer that makes sense for me is B
upvoted 1 times

🗨️  **OSNG** 4 months, 2 weeks ago

Its B.

Reasons:

1. They are asking for advise for Developers. (IaC is the suitable as they don't have to worry about managing infrastructure manually).
Moreover "An organization's typical network and security review consists of analyzing application transit routes, request handling, and firewall rules." statement is defining the process, they are not asking about the option to review the rules. Using Forseti is not reducing the overhead for Developers.
upvoted 5 times

🗨️  **TNT87** 10 months, 4 weeks ago

if you done Cloud Rchitect,you will understand why the answer is B
upvoted 4 times

🗨️  **bluetaurianbull** 8 months, 1 week ago

its like saying if you have gone to space you experiance weighlessness .. be professional man... give proof for your claims, dont just expect world to be in same level as you. thats about COMMUNITY LEARNING ...
upvoted 6 times

🗨️  **[Removed]** 1 year, 2 months ago

Ans - C

upvoted 2 times

🗨️  **[Removed]** 1 year, 2 months ago

Sry(Typo) .. It's B

upvoted 2 times



🗨️  **saaurabh1805** 1 year, 3 months ago

I will also go with option A

upvoted 1 times



🗨️  **CHECK666** 1 year, 3 months ago

B is the answer
upvoted 1 times



  **ownez** 1 year, 4 months ago

Answer is B and not A because in A, the answer provided tells us the environment is in production where the question is about to enable their developer teams to deploy new applications without the overhead of the full review. Implementation of IAC is suitable for this.



Answer is B.
upvoted 3 times

  **MohitA** 1 year, 4 months ago

Yes B serves the purpose.
upvoted 2 times

  **aiwaai** 1 year, 4 months ago

Answer is A
upvoted 1 times

  **bigdo** 1 year, 5 months ago

b is correct <https://cloud.google.com/blog/products/containers-kubernetes/guard-against-security-vulnerabilities-with-container-registry-vulnerability-scanning>
upvoted 2 times

  **ArizonaClassics** 1 year, 5 months ago

Foreseti makes sense == A
upvoted 2 times

  **ArizonaClassics** 1 year, 4 months ago

The Core FORSETI modules includes the Following; (1.) INVENTORY (2.) SCANNING (3.) ENFORCEMENT (4.) EXPLAIN
Hence the question already gave a clue on what they are looking for (INVENTORY/VISIBILITY/ANALYSIS) of all transit routes, firewall rules etc
upvoted 1 times

  **SilentSec** 1 year, 6 months ago

B is right. With ci/cd pipeline you can use template for deployment and limit scan effort
upvoted 3 times

An employer wants to track how bonus compensations have changed over time to identify employee outliers and correct earning disparities. This task must be performed without exposing the sensitive compensation data for any individual and must be reversible to identify the outlier. Which Cloud Data Loss Prevention API technique should you use to accomplish this?

- A. Generalization
- B. Redaction
- C. CryptoHashConfig
- D. CryptoReplaceFfxFpeConfig

🗲️ 👤 **xhova** Highly Voted 👍 1 year, 9 months ago
Answer is D

<https://cloud.google.com/dlp/docs/pseudonymization>
upvoted 10 times

🗲️ 👤 **SilentSec** 1 year, 6 months ago
Also the same usecase in the url that you post. D is right.
upvoted 1 times

🗲️ 👤 **smart123** 1 year, 7 months ago
Option D is correct because it is reversible whereas option B is not.
upvoted 2 times

🗲️ 👤 **gcp_learner** Highly Voted 👍 1 year, 6 months ago
The answer is A.
By bucketing or generalizing, we achieve a reversible pseudonymised data that can still yield the required analysis.
<https://cloud.google.com/dlp/docs/concepts-bucketing>
upvoted 5 times

🗲️ 👤 **Sheeda** 1 year, 5 months ago
Completely wrong

The answer is D for sure. The example was even in google docs but replaced for some reasons.

http://price2meet.com/gcp/docs/dlp_docs_pseudonymization.pdf
upvoted 2 times

🗲️ 👤 **Bwitch** Most Recent 🕒 1 month, 2 weeks ago
I think B is correct.

<https://cloud.google.com/dlp/docs/transformations-reference#redaction>
upvoted 1 times

🗲️ 👤 **OSNG** 4 months, 2 weeks ago
Answer is D.
<https://cloud.google.com/dlp/docs/transformations-reference>
upvoted 1 times

🗲️ 👤 **rand0mb0t** 5 months, 1 week ago
The correct answer is A . As it will let you de-identify the data and also generalise it with bucketing so that outliers can be found during analysis.
I would go with A
upvoted 1 times

🗲️ 👤 **Zuy01** 5 months, 1 week ago
The answer are closest is between C and D, if you read on this link : https://cloud.google.com/dlp/docs/transformations-reference#transformation_methods
"CryptoHashConfig" it can't be reverse, but "CryptoReplaceFfxFpeConfig" it can be reversed. so the answer is D.
upvoted 1 times

🗲️ 👤 **ASG** 11 months ago
Ans - D - <https://cloud.google.com/dlp/docs/transformations-reference> (pls do read the details in this link for clarification - it will only take you a min or two)
upvoted 1 times

🗲️ 👤 **ESP_SAP** 1 year, 1 month ago
Correct Answer is (D):

De-identifying sensitive data

Cloud Data Loss Prevention (DLP) can de-identify sensitive data in text content, including text stored in container structures such as tables. De-identification is the process of removing identifying information from data. The API detects sensitive data such as personally identifiable information (PII), and then uses a de-identification transformation to mask, delete, or otherwise obscure the data. For example, de-identification techniques can include any of the following:

Masking sensitive data by partially or fully replacing characters with a symbol, such as an asterisk (*) or hash (#).

Replacing each instance of sensitive data with a token, or surrogate, string.

Encrypting and replacing sensitive data using a randomly generated or pre-determined key.

When you de-identify data using the `CryptoReplaceFfxFpeConfig` or `CryptoDeterministicConfig` infoType transformations, you can re-identify that data, as long as you have the `CryptoKey` used to originally de-identify the data.

<https://cloud.google.com/dlp/docs/deidentify-sensitive-data>

upvoted 3 times

🗲️ 👤 **jonclem** 1 year, 2 months ago

My conclusion is answer B since watching the DLP vide from Linuxacademy. It mentions the process and even describes identifying the outliers.

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - D

<https://cloud.google.com/dlp/docs/deidentify-sensitive-data>

upvoted 1 times

🗲️ 👤 **saaurabh1805** 1 year, 3 months ago

D is correct option as question is asking information to be re-identified hence D is best possible options

upvoted 1 times

🗲️ 👤 **CHECK666** 1 year, 3 months ago

D is the Answer

upvoted 1 times

🗲️ 👤 **MohitA** 1 year, 4 months ago

D. `CryptoReplaceFfxFpeConfig` is the answer for sure, it allows you to recover the original data.

upvoted 2 times

🗲️ 👤 **soukumar369** 1 year, 1 month ago

<https://youtu.be/JLDpbXbT6wo>

upvoted 1 times

🗲️ 👤 **aiwaai** 1 year, 4 months ago

Answer is A

upvoted 1 times

An organization adopts Google Cloud Platform (GCP) for application hosting services and needs guidance on setting up password requirements for their Cloud Identity account. The organization has a password policy requirement that corporate employee passwords must have a minimum number of characters.

Which Cloud Identity password guidelines can the organization use to inform their new requirements?

- A. Set the minimum length for passwords to be 8 characters.
- B. Set the minimum length for passwords to be 10 characters.
- C. Set the minimum length for passwords to be 12 characters.
- D. Set the minimum length for passwords to be 6 characters.

🗲️ 👤 **KILLMAD** Highly Voted 👍 1 year, 10 months ago

Ans is A

upvoted 9 times

🗲️ 👤 **rafaelc** 1 year, 10 months ago

Default password length is 8 characters.

<https://support.google.com/cloudidentity/answer/33319?hl=en>

upvoted 6 times

🗲️ 👤 **bolu** Highly Voted 👍 11 months, 2 weeks ago

The situation changes year on year on GCP. Right now the right answer is C based on minimum requirement of 12 char in GCP as on Jan 2021.

<https://support.google.com/accounts/answer/32040?hl=en#zippy=%2Cmake-your-password-longer-more-memorable>

upvoted 8 times

🗲️ 👤 **desertlotus1211** 10 months ago

It asked for Cloud Identity password requirements... Minimum is 8 Maximum is 100

upvoted 2 times

🗲️ 👤 **umashankar_a** Most Recent ⌚ 6 months, 1 week ago

Answer A

For Cloud Identity password requirements still is - Minimum 8 Maximum is 100

[https://support.google.com/cloudidentity/answer/139399?](https://support.google.com/cloudidentity/answer/139399?hl=en#:~:text=It%20can%20be%20between%208,decide%20to%20change%20their%20password.)

[hl=en#:~:text=It%20can%20be%20between%208,decide%20to%20change%20their%20password.](https://support.google.com/cloudidentity/answer/139399?hl=en#:~:text=It%20can%20be%20between%208,decide%20to%20change%20their%20password.)

upvoted 2 times

🗲️ 👤 **soukumar369** 1 year ago

Answer is C : <https://support.google.com/accounts/answer/32040?hl=en#zippy=%2Cmake-your-password-longer-more-memorable>

Long passwords are stronger, so make your password at least 12 characters long. These tips can help you create longer passwords that are easier to remember. Try to use:

upvoted 2 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - A

upvoted 2 times

🗲️ 👤 **CHECK666** 1 year, 3 months ago

A is the answer.

upvoted 1 times

🗲️ 👤 **MohitA** 1 year, 4 months ago

Is it really an exam Question? it depends on what's your company policy is for password length

upvoted 4 times

🗲️ 👤 **Zol** 1 year, 10 months ago

Rafaec


You're correct A is the answer

upvoted 1 times



You need to follow Google-recommended practices to leverage envelope encryption and encrypt data at the application layer.



What should you do?



- A. Generate a data encryption key (DEK) locally to encrypt the data, and generate a new key encryption key (KEK) in Cloud KMS to encrypt the DEK. Store both the encrypted data and the encrypted DEK.
- B. Generate a data encryption key (DEK) locally to encrypt the data, and generate a new key encryption key (KEK) in Cloud KMS to encrypt the DEK. Store both the encrypted data and the KEK.
- C. Generate a new data encryption key (DEK) in Cloud KMS to encrypt the data, and generate a key encryption key (KEK) locally to encrypt the key. Store both the encrypted data and the encrypted DEK.
- D. Generate a new data encryption key (DEK) in Cloud KMS to encrypt the data, and generate a key encryption key (KEK) locally to encrypt the key. Store both the encrypted data and the KEK.



  **Sheeda** Highly Voted 1 year, 5 months ago
Yes, A is correct



The process of encrypting data is to generate a DEK locally, encrypt data with the DEK, use a KEK to wrap the DEK, and then store the encrypted data and the wrapped DEK. The KEK never leaves Cloud KMS.
upvoted 12 times



  **MohitA** 1 year, 4 months ago
Agree on A, spot on "KEK never leaves Cloud KMS"
upvoted 3 times



  **Bill831231** Most Recent 1 month ago
A sounds like the correct answer:
https://cloud.google.com/kms/docs/envelope-encryption#how_to_encrypt_data_using_envelope_encryption
upvoted 1 times

  **umashankar_a** 6 months, 1 week ago
Answer A
Envelope Encryption: <https://cloud.google.com/kms/docs/envelope-encryption>
Here are best practices for managing DEKs:
-Generate DEKs locally.
-When stored, always ensure DEKs are encrypted at rest.
- For easy access, store the DEK near the data that it encrypts.
The DEK is encrypted (also known as wrapped) by a key encryption key (KEK). The process of encrypting a key with another key is known as envelope encryption.
Here are best practices for managing KEKs:
-Store KEKs centrally. (KMS)
-Set the granularity of the DEKs they encrypt based on their use case. For example, consider a workload that requires multiple DEKs to encrypt the workload's data chunks. You could use a single KEK to wrap all DEKs that are responsible for that workload's encryption.
-Rotate keys regularly, and also after a suspected incident.
upvoted 2 times


  **desertlotus1211** 9 months ago
I'm no sure what the answers is, but the answers to this question has changed.... be prepared
upvoted 1 times

  **dtmtor** 9 months, 4 weeks ago
Answer is A
upvoted 1 times

  **DebasishLowes** 10 months ago
Ans : A
upvoted 1 times

  **CloudTrip** 10 months, 4 weeks ago
Correction I change it to A after reading the question once again.
upvoted 1 times

  **CloudTrip** 11 months ago
Answer is B as after DEK encryption it's KEK (not encrypted DEK) which never leaves KMS
upvoted 1 times

  **Bharathy** 1 year, 1 month ago
A - Envelope Encryption (DEK - to encrypt the data, KEK - encrypt the DEK , KEK resides in KMS and only the encrypted data and wrapped DEK will be stored back)

upvoted 2 times

  **[Removed]** 1 year, 2 months ago

Ans - A


https://cloud.google.com/kms/docs/envelope-encryption#how_to_encrypt_data_using_envelope_encryption

upvoted 1 times

  **CHECK666** 1 year, 3 months ago

The answer is A

upvoted 1 times

  **aiwaai** 1 year, 4 months ago

The Answer is A

upvoted 2 times

  **ArizonaClassics** 1 year, 5 months ago

C is the correct option. See BEST Practices for managing DEKS



<https://cloud.google.com/kms/docs/envelope-encryption>

upvoted 1 times

  **ArizonaClassics** 1 year, 4 months ago

A is the correct one. Made a mistake earlier

upvoted 2 times

  **kumar999** 1 year, 5 months ago

It is A. See How to encrypt data using envelope encryption

upvoted 2 times

  **ArizonaClassics** 1 year, 4 months ago

Thank you Kumar. it is A. I made a mistake.

upvoted 1 times

How should a customer reliably deliver Stackdriver logs from GCP to their on-premises SIEM system?

- A. Send all logs to the SIEM system via an existing protocol such as syslog.
- B. Configure every project to export all their logs to a common BigQuery DataSet, which will be queried by the SIEM system.
- C. Configure Organizational Log Sinks to export logs to a Cloud Pub/Sub Topic, which will be sent to the SIEM via Dataflow.
- D. Build a connector for the SIEM to query for all logs in real time from the GCP RESTful JSON APIs.

🗲️ 👤 **ESP_SAP** Highly Voted 👍 1 year, 1 month ago

Correct answer is (C):

Scenarios for exporting Cloud Logging data: Splunk

This scenario shows how to export selected logs from Cloud Logging to Pub/Sub for ingestion into Splunk. Splunk is a security information and event management (SIEM) solution that supports several ways of ingesting data, such as receiving streaming data out of Google Cloud through Splunk HTTP Event Collector (HEC) or by fetching data from Google Cloud APIs through Splunk Add-on for Google Cloud.

Using the Pub/Sub to Splunk Dataflow template, you can natively forward logs and events from a Pub/Sub topic into Splunk HEC. If Splunk HEC is not available in your Splunk deployment, you can use the Add-on to collect the logs and events from the Pub/Sub topic.

<https://cloud.google.com/solutions/exporting-stackdriver-logging-for-splunk>

upvoted 9 times

🗲️ 👤 **DebasishLowes** Most Recent ⌚ 10 months ago

Ans : C

upvoted 2 times

🗲️ 👤 **BlahBaller** 1 year ago

As I was the Logging Service Manager when we set this up with GCP. I can verify that C is how we have it setup, based on the Google's recommendations.

upvoted 2 times

🗲️ 👤 **Moss2011** 1 year, 2 months ago

I think the correct one its D because C mention "Dataflow" and it cannot be connected to any sink out of GCP.

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - C

<https://cloud.google.com/solutions/exporting-stackdriver-logging-for-splunk>

upvoted 1 times

🗲️ 👤 **devisrk** 1 year, 2 months ago

C looks correct..

<https://cloud.google.com/solutions/exporting-stackdriver-logging-for-splunk>

Splunk is on premises SIEM solution in above example.

upvoted 2 times

🗲️ 👤 **saaurabh1805** 1 year, 3 months ago

I will go with Option B.

Read this email for more reason. C is not workable solution so that is first one not to consider.

upvoted 1 times

🗲️ 👤 **CHECK666** 1 year, 3 months ago

C is the answer.

upvoted 1 times

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

I will go with C

upvoted 2 times

🗲️ 👤 **xhova** 1 year, 9 months ago

C is correct

upvoted 4 times

In order to meet PCI DSS requirements, a customer wants to ensure that all outbound traffic is authorized.

Which two cloud offerings meet this requirement without additional compensating controls? (Choose two.)

- A. App Engine
- B. Cloud Functions
- C. Compute Engine
- D. Google Kubernetes Engine
- E. Cloud Storage

🗲️ 👤 **KILLMAD** Highly Voted 👍 1 year, 10 months ago
Answer is CD

because the doc mentions the following: "App Engine ingress firewall rules are available, but egress rules are not currently available:" and "Compute Engine and GKE are the preferred alternatives."
upvoted 14 times

🗲️ 👤 **rafaelc** 1 year, 10 months ago
It is CD.

App Engine ingress firewall rules are available, but egress rules are not currently available. Per requirements 1.2.1 and 1.3.4, you must ensure that all outbound traffic is authorized. SAQ A-EP and SAQ D-type merchants must provide compensating controls or use a different Google Cloud product. Compute Engine and GKE are the preferred alternatives.

<https://cloud.google.com/solutions/pci-dss-compliance-in-gcp>
upvoted 5 times

🗲️ 👤 **DebasishLowes** Most Recent 🕒 10 months ago
Ans : CD
upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago
Ans - CD
https://cloud.google.com/solutions/pci-dss-compliance-in-gcp#app_engine
upvoted 1 times

🗲️ 👤 **saurabh1805** 1 year, 3 months ago
C & D is correct answer here.

<https://cloud.google.com/solutions/pci-dss-compliance-in-gcp>
upvoted 1 times

🗲️ 👤 **CHECK666** 1 year, 3 months ago
CD is the answer.
upvoted 1 times

🗲️ 👤 **MohitA** 1 year, 4 months ago
CD serves the purpose for sure
upvoted 1 times

🗲️ 👤 **ArizonaClassics** 1 year, 5 months ago
CD best option
upvoted 2 times

🗲️ 👤 **xhova** 1 year, 9 months ago
CD is right
upvoted 2 times

When working with agents in a support center via online chat, an organization's customers often share pictures of their documents with personally identifiable information (PII). The organization that owns the support center is concerned that the PII is being stored in their databases as part of the regular chat logs they retain for review by internal or external analysts for customer service trend analysis.

Which Google Cloud solution should the organization use to help resolve this concern for the customer while still maintaining data utility?

- A. Use Cloud Key Management Service (KMS) to encrypt the PII data shared by customers before storing it for analysis.
- B. Use Object Lifecycle Management to make sure that all chat records with PII in them are discarded and not saved for analysis.
- C. Use the image inspection and redaction actions of the DLP API to redact PII from the images before storing them for analysis.
- D. Use the generalization and bucketing actions of the DLP API solution to redact PII from the texts before storing them for analysis.

🗲️ 👤 **rafaelc** Highly Voted 👍 1 year, 10 months ago

Answer is actually C

C. Use the image inspection and redaction actions of the DLP API to redact PII from the images before storing them for analysis.

<https://cloud.google.com/dlp/docs/concepts-image-redaction>

upvoted 16 times

🗲️ 👤 **jonclem** 1 year, 9 months ago

I think you'll find D is correct. Check out Generalisation and Bucketing in the videos on LA.

upvoted 1 times

🗲️ 👤 **xhova** Highly Voted 👍 1 year, 9 months ago

D only talks about texts however the question is asking...."an organization's customers often share pictures of their documents" keyword there is pictures. So C is the answer

upvoted 9 times

🗲️ 👤 **sc_cloud_learn** Most Recent ⌚ 6 months, 3 weeks ago

answer looks like C

upvoted 1 times

🗲️ 👤 **Jane111** 8 months, 2 weeks ago

"Generalization is the process of taking a distinguishing value and abstracting it into a more general, less distinguishing value. Generalization attempts to preserve data utility while also reducing the identifiability of the data.

One common generalization technique that Cloud DLP supports is bucketing. With bucketing, you group records into smaller buckets in an attempt to minimize the risk of an attacker associating sensitive information with identifying information. Doing so can retain meaning and utility, but it will also obscure the individual values that have too few participants."

upvoted 1 times

🗲️ 👤 **DebasishLowes** 9 months, 4 weeks ago

Ans : C

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - C

<https://cloud.google.com/dlp/docs/redacting-sensitive-data-images>

upvoted 1 times

🗲️ 👤 **saurabh1805** 1 year, 3 months ago

I will also vote for C.

upvoted 1 times

🗲️ 👤 **CHECK666** 1 year, 3 months ago

C is the answer.

upvoted 1 times

🗲️ 👤 **MohitA** 1 year, 4 months ago

C is the Answer, as it talks about image

upvoted 1 times

🗲️ 👤 **aiwaai** 1 year, 4 months ago



Answer is C

upvoted 1 times

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

I go with option C

upvoted 1 times

  **gcp_learner** 1 year, 6 months ago

The answer is C. Question requests redacting PII I'm uploaded pics. DLP API does this.

upvoted 1 times

Your team needs to configure their Google Cloud Platform (GCP) environment so they can centralize the control over networking resources like firewall rules, subnets, and routes. They also have an on-premises environment where resources need access back to the GCP resources through a private VPN connection.

The networking resources will need to be controlled by the network security team.

Which type of networking design should your team use to meet these requirements?

- A. Shared VPC Network with a host project and service projects
- B. Grant Compute Admin role to the networking team for each engineering project
- C. VPC peering between all engineering projects using a hub and spoke model
- D. Cloud VPN Gateway between all engineering projects using a hub and spoke model

  **ArizonaClassics** Highly Voted 1 year, 5 months ago

I agree with A
Centralize network control:

Use Shared VPC to connect to a common VPC network. Resources in those projects can communicate with each other securely and efficiently across project boundaries using internal IPs. You can manage shared network resources, such as subnets, routes, and firewalls, from a central host project, enabling you to apply and enforce consistent network policies across the projects.

upvoted 11 times

  **ArizonaClassics** 1 year, 5 months ago

WATCH: <https://www.youtube.com/watch?v=WotV3D01tJA>

READ:
https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations#centralize_network_control

upvoted 3 times

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


Sheeda En mi caso te confirmo que desde la share VPC se establecen las VPNs y allí ingresa el tráfico desde los sitios locales. Definitivamente, la respuesta es la A

upvoted 1 times

  **DebasishLowes** 10 months ago

Ans : A. It will be shared VPC as it is asking for centralized network control.

upvoted 1 times

  **jonclem** 1 year, 2 months ago

Option D is incorrect and a violation of Google's Service Specific terms as per : <https://cloud.google.com/network-connectivity/docs/vpn/concepts/overview>

I'd go with option A myself.

upvoted 1 times

  **[Removed]** 1 year, 2 months ago

Ans - A

upvoted 1 times

  **saaurabh1805** 1 year, 3 months ago

A, this is exact reason to use shared VPC

upvoted 1 times

  **CHECK666** 1 year, 3 months ago



A is the answer.

upvoted 1 times

  **Akku1614** 1 year, 4 months ago

A is correct as Shared VPC provides us with Centralized control however VPC Peering is a decentralized option.

upvoted 1 times

  **aiwaai** 1 year, 4 months ago

Correct Answer: A

upvoted 1 times

  **Sheeda** 1 year, 5 months ago

Connect your enterprise network

Many enterprises need to connect existing on-premises infrastructure with their Google Cloud resources. Evaluate your bandwidth, latency, and

SLA requirements to choose the best connection option:

If you need low-latency, highly available, enterprise-grade connections that enable you to reliably transfer data between your on-premises and VPC networks without traversing the internet connections to Google Cloud, use Cloud Interconnect:

Dedicated Interconnect provides a direct physical connection between your on-premises network and Google's network. Partner Interconnect provides connectivity between your on-premises and Google Cloud VPC networks through a supported service provider. If you don't require the low latency and high availability of Cloud Interconnect, or you are just starting on your cloud journey, use Cloud VPN to set up encrypted IPsec VPN tunnels between your on-premises network and VPC. Compared to a direct, private connection, an IPsec VPN tunnel has lower overhead and costs.

upvoted 1 times

  **ESP_SAP** 1 year, 1 month ago

you Should go back to the GCP Cloud Architect concepts or GCP Networking!

upvoted 2 times

  **ArizonaClassics** 1 year, 4 months ago

Sheeda you need to read and understand the the question.


upvoted 1 times

  **ArizonaClassics** 1 year, 4 months ago

They are asking how you can centralize the control over networking resources like firewall rules, subnets, and routes. watch this: <https://www.youtube.com/watch?v=WotV3D01tJA>

you will see that you can also manage vpn connections as well

upvoted 1 times

  **Sheeda** 1 year, 5 months ago

I believe the answer is D. How can shared VPC give access to your on premise environment ? A seems wrong to me.

upvoted 1 times

Question #23

Topic 1

A customer's company has multiple business units. Each business unit operates independently, and each has their own engineering group. Your team wants visibility into all projects created within the company and wants to organize their Google Cloud Platform (GCP) projects based on different business units. Each business unit also requires separate sets of IAM permissions.

Which strategy should you use to meet these needs?

- A. Create an organization node, and assign folders for each business unit.
- B. Establish standalone projects for each business unit, using gmail.com accounts.
- C. Assign GCP resources in a project, with a label identifying which business unit owns the resource.
- D. Assign GCP resources in a VPC for each business unit to separate network access.

  **ArizonaClassics** Highly Voted  1 year, 5 months ago

I will go with A

Refer to: <https://cloud.google.com/resource-manager/docs/listing-all-resources>

Also: <https://wideops.com/mapping-your-organization-with-the-google-cloud-platform-resource-hierarchy/>

upvoted 8 times

  **DebasishLowes** Most Recent  11 months ago



Ans - A

upvoted 3 times

  **[Removed]** 1 year, 2 months ago

Ans - A

upvoted 1 times

  **aiwaai** 1 year, 4 months ago

Correct Answer: A

upvoted 1 times

A company has redundant mail servers in different Google Cloud Platform regions and wants to route customers to the nearest mail server based on location.

How should the company accomplish this?

- A. Configure TCP Proxy Load Balancing as a global load balancing service listening on port 995.
- B. Create a Network Load Balancer to listen on TCP port 995 with a forwarding rule to forward traffic based on location.
- C. Use Cross-Region Load Balancing with an HTTP(S) load balancer to route traffic to the nearest region.
- D. Use Cloud CDN to route the mail traffic to the closest origin mail server based on client IP address.

🗲️ 👤 **ESP_SAP** Highly Voted 👍 1 year, 1 month ago
Correct Answer is (A):

TCP Proxy Load Balancing is implemented on GFEs that are distributed globally. If you choose the Premium Tier of Network Service Tiers, a TCP proxy load balancer is global. In Premium Tier, you can deploy backends in multiple regions, and the load balancer automatically directs user traffic to the closest region that has capacity. If you choose the Standard Tier, a TCP proxy load balancer can only direct traffic among backends in a single region.

<https://cloud.google.com/load-balancing/docs/load-balancing-overview#tcp-proxy-load-balancing>
upvoted 12 times

🗲️ 👤 **AWSE** Most Recent 🕒 11 months, 1 week ago
Ans should be A. TCP Proxy Load Balancing is intended for TCP traffic on specific well-known ports, such as port 25 for Simple Mail Transfer Protocol (SMTP).
upvoted 3 times

🗲️ 👤 **jonclem** 1 year, 2 months ago
I'd agree with option A as it covers location based traffic plus the mail port 993.
upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago
Ans - A
upvoted 1 times

🗲️ 👤 **passtest100** 1 year, 3 months ago
should be C.
the port 995 has nothing to do with email service . HTTP LB can work on TCP traffic while CDN does NOT support email
so the better answer is C
upvoted 2 times

🗲️ 👤 **CHECK666** 1 year, 3 months ago
A is the answer.
upvoted 1 times

🗲️ 👤 **ArizonaClassics** 1 year, 5 months ago
A: <https://cloud.google.com/load-balancing/docs/tcp>
upvoted 1 times

🗲️ 👤 **Warren2020** 1 year, 6 months ago
A is the correct answer. D is not correct. CDN works with HTTP(s) traffic and requires caching, which is not a valid feature used for mail server
upvoted 4 times

🗲️ 👤 **Zol** 1 year, 9 months ago
Answer A is correct
upvoted 1 times

🗲️ 👤 **mozammil89** 1 year, 10 months ago
Answer should be, A

<https://cloud.google.com/load-balancing/docs/tcp>
upvoted 4 times

Your team sets up a Shared VPC Network where project co-vpc-prod is the host project. Your team has configured the firewall rules, subnets, and VPN gateway on the host project. They need to enable Engineering Group A to attach a Compute Engine instance to only the 10.1.1.0/24 subnet. What should your team grant to Engineering Group A to meet this requirement?

- A. Compute Network User Role at the host project level.
- B. Compute Network User Role at the subnet level.
- C. Compute Shared VPC Admin Role at the host project level.
- D. Compute Shared VPC Admin Role at the service project level.

🗲️ 👤 **mozammil89** Highly Voted 👍 1 year, 10 months ago

The correct answer is B.

https://cloud.google.com/vpc/docs/shared-vpc#svc_proj_admins

upvoted 11 times

🗲️ 👤 **droppler** Most Recent 🕒 6 months, 1 week ago

The right one is b on my thinking, but i need to enable the other team to do the jobs, falls into D

upvoted 1 times

🗲️ 👤 **DebasishLowes** 9 months, 4 weeks ago

Ans : B

upvoted 2 times

🗲️ 👤 **saurabh1805** 1 year, 2 months ago

B is correct answer

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - B

upvoted 1 times

🗲️ 👤 **CHECK666** 1 year, 3 months ago

B is the answer.

upvoted 1 times

🗲️ 👤 **Mohita** 1 year, 4 months ago

B is right

upvoted 1 times

🗲️ 👤 **ArizonaClassics** 1 year, 4 months ago

B is correct

upvoted 1 times

🗲️ 👤 **Zol** 1 year, 9 months ago

Correct B

upvoted 1 times

A company migrated their entire data/center to Google Cloud Platform. It is running thousands of instances across multiple projects managed by different departments. You want to have a historical record of what was running in Google Cloud Platform at any point in time. What should you do?

- A. Use Resource Manager on the organization level.
- B. Use Forseti Security to automate inventory snapshots.
- C. Use Stackdriver to create a dashboard across all projects.
- D. Use Security Command Center to view all assets across the organization.

🗲️ 👤 **smart123** Highly Voted 👍 1 year, 7 months ago

'B is the correct answer. Only Forseti security can have both 'past' and 'present' (i.e. historical) records of the resources.
<https://forsetisecurity.org/about/>
upvoted 8 times

🗲️ 👤 **mitow95526** Most Recent ⌚ 7 months, 2 weeks ago
<https://cloud.google.com/security-command-center>

Discover and view your assets in near-real time across App Engine, BigQuery, Cloud SQL, Cloud Storage, Compute Engine, Cloud Identity and Access Management, Google Kubernetes Engine, and more. Review historical discovery scans to identify new, modified, or deleted assets.

Why not D?
upvoted 3 times

🗲️ 👤 **ThisisJohn** 1 month ago

I guess the reason to discard D is that it says "all assets", while according to the documentation, "Security Command Center supports a large subset of Google Cloud assets.", so it supports a large number but not all assets.

Ref: <https://cloud.google.com/security-command-center/docs/concepts-security-command-center-overview#inventory>
upvoted 1 times

🗲️ 👤 **pfilourenco** 8 months ago
And about D?
upvoted 2 times

🗲️ 👤 **dtmtor** 9 months, 4 weeks ago
Answer is B
upvoted 2 times

🗲️ 👤 **pythonrocks** 6 months, 1 week ago
<https://forsetisecurity.org/about/> inventory
upvoted 1 times

🗲️ 👤 **DebasishLowes** 10 months ago
Ans : B. You need to keep the records for long time so it's Inventory.
upvoted 2 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago
Ans - B
upvoted 2 times

🗲️ 👤 **Mohita** 1 year, 4 months ago
B is the right answer, Forseti has a track of inventory snapshots
upvoted 1 times



🗲️ 👤 **aiwaai** 1 year, 4 months ago
Correct answer is B
upvoted 1 times



🗲️ 👤 **ArizonaClassics** 1 year, 5 months ago
I will go with B
question says " historical inventory" and that makes B the right choice
upvoted 4 times

🗲️ 👤 **MarkDillon1075** 1 year, 6 months ago
B is correct
upvoted 1 times



🗲️ 👤 **xhova** 1 year, 9 months ago



A is correct
upvoted 1 times

  **ArizonaClassics** 1 year, 4 months ago
B IS CORRECT SEE: <https://forsetisecurity.org/about/>
upvoted 2 times

  **mozammil89** 1 year, 10 months ago
The correct answer is A.

Feature of Resource Manager - <https://cloud.google.com/asset-inventory>
upvoted 3 times

  **FatCharlie** 1 year, 1 month ago
Resource Manager / Cloud Asset Inventory only keeps data for 6 weeks, so doesn't meet the requirements in the question
upvoted 1 times

  **ArizonaClassics** 1 year, 4 months ago
SEE THE SUB-HEADING 'INVENTORY' ON THIS LINK: <https://forsetisecurity.org/about/>
upvoted 1 times

  **gcp_learner** 1 year, 6 months ago
The answer is not A because Cloud Asset Inventory is not one of the choices. The correct answer is B.
upvoted 5 times

An organization is starting to move its infrastructure from its on-premises environment to Google Cloud Platform (GCP). The first step the organization wants to take is to migrate its current data backup and disaster recovery solutions to GCP for later analysis. The organization's production environment will remain on- premises for an indefinite time. The organization wants a scalable and cost-efficient solution. Which GCP solution should the organization use?

- A. BigQuery using a data pipeline job with continuous updates
- B. Cloud Storage using a scheduled task and gsutil
- C. Compute Engine Virtual Machines using Persistent Disk
- D. Cloud Datastore using regularly scheduled batch upload jobs

🗲️ 👤 **xhova** Highly Voted 👍 1 year, 9 months ago

Ans is B. A cost efficient disaster recovery solution is needed not a data warehouse.
upvoted 13 times

🗲️ 👤 **DebasishLowes** Most Recent 🕒 10 months ago

Ans : B. Cloud storage is cost efficient one.
upvoted 3 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - B
upvoted 1 times

🗲️ 👤 **CHECK666** 1 year, 3 months ago

B is the answer.
upvoted 1 times

🗲️ 👤 **paxjoshi** 1 year, 4 months ago

B is the correct answer. They need the data for later analysis and they are looking for cost-effective service.
upvoted 2 times

🗲️ 👤 **aiwaai** 1 year, 4 months ago

Correct Answer: A
upvoted 1 times

🗲️ 👤 **aiwaai** 1 year, 4 months ago

I make corrections, B is Correct Answer.
upvoted 1 times

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

Answer B works for me as the type of workload to be stored is not stated or defined
upvoted 1 times

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

B confirmed: <https://cloud.google.com/solutions/dr-scenarios-planning-guide#use-cloud-storage-as-part-of-your-daily-backup-routine>
upvoted 3 times

You are creating an internal App Engine application that needs to access a user's Google Drive on the user's behalf. Your company does not want to rely on the current user's credentials. It also wants to follow Google-recommended practices.

What should you do?

- A. Create a new Service account, and give all application users the role of Service Account User.
- B. Create a new Service account, and add all application users to a Google Group. Give this group the role of Service Account User.
- C. Use a dedicated G Suite Admin account, and authenticate the application's operations with these G Suite credentials.
- D. Create a new service account, and grant it G Suite domain-wide delegation. Have the application use it to impersonate the user.

🗲️ 👤 **mozammil89** Highly Voted 👍 1 year, 10 months ago

I think the correct answer is D

<https://developers.google.com/admin-sdk/directory/v1/guides/delegation>

upvoted 13 times

🗲️ 👤 **Rhehehe** Most Recent 🕒 3 weeks, 3 days ago

They are asking for google recommended practice. Does D says that?

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - D

upvoted 2 times

🗲️ 👤 **CHECK666** 1 year, 3 months ago

D is the answer.

upvoted 1 times

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

D is the best choice

upvoted 1 times

🗲️ 👤 **MarkDillon1075** 1 year, 6 months ago

I agree D

upvoted 1 times

A customer wants to move their sensitive workloads to a Compute Engine-based cluster using Managed Instance Groups (MIGs). The jobs are bursty and must be completed quickly. They have a requirement to be able to manage and rotate the encryption keys. Which boot disk encryption solution should you use on the cluster to meet this customer's requirements?

- A. Customer-supplied encryption keys (CSEK)
- B. Customer-managed encryption keys (CMEK) using Cloud Key Management Service (KMS)
- C. Encryption by default
- D. Pre-encrypting files before transferring to Google Cloud Platform (GCP) for analysis

🗲️ 👤 **ArizonaClassics** Highly Voted 👍 1 year, 5 months ago

B is correct. Customer managed
upvoted 10 times

🗲️ 👤 **Rhehehe** Most Recent ⌚ 3 weeks, 3 days ago

Compute Engine does not store encryption keys with instance templates, so you need to store your own keys in KMS to encrypt disks in a managed instance group.
upvoted 1 times

🗲️ 👤 **Bill831231** 1 month ago

not sure, A sounds better
<https://cloud.google.com/compute/docs/disks/customer-supplied-encryption>
upvoted 1 times

🗲️ 👤 **DebasishLowes** 11 months ago

Ans - B
upvoted 3 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - B
upvoted 2 times

🗲️ 👤 **CHECK666** 1 year, 3 months ago

B is the answer.
upvoted 2 times

You are a member of the security team at an organization. Your team has a single GCP project with credit card payment processing systems alongside web applications and data processing systems. You want to reduce the scope of systems subject to PCI audit standards. What should you do?

- A. Use multi-factor authentication for admin access to the web application.
- B. Use only applications certified compliant with PA-DSS.
- C. Move the cardholder data environment into a separate GCP project.
- D. Use VPN for all connections between your office and cloud environments.

🗲️ 👤 **jonclem** Highly Voted 👍 1 year, 9 months ago
I'd go for answer C myself.

<https://cloud.google.com/solutions/best-practices-vpc-design>
upvoted 17 times

🗲️ 👤 **[Removed]** Most Recent 🕒 1 year, 2 months ago
Ans - C
https://cloud.google.com/solutions/pci-dss-compliance-in-gcp#setting_up_your_payment-processing_environment
upvoted 4 times

🗲️ 👤 **CHECK666** 1 year, 3 months ago
C is the answer.
upvoted 1 times

🗲️ 👤 **smart123** 1 year, 7 months ago
The Answer is C. Check "Setting up your payment-processing environment" section in <https://cloud.google.com/solutions/pci-dss-compliance-in-gcp>.
In the question, it is mentioned that it is the same environment for card processing as the Web App and Data processing and that is not recommended.
upvoted 2 times

🗲️ 👤 **xhova** 1 year, 9 months ago
Definitely C
upvoted 1 times

A retail customer allows users to upload comments and product reviews. The customer needs to make sure the text does not include sensitive data before the comments or reviews are published.

Which Google Cloud Service should be used to achieve this?

- A. Cloud Key Management Service
- B. Cloud Data Loss Prevention API
- C. BigQuery
- D. Cloud Security Scanner

🗲️ 👤 **rafaelc** Highly Voted 👍 1 year, 10 months ago
It's definitely B. It was on the practice test on google site.
B. Cloud Data Loss Prevention API
upvoted 18 times

🗲️ 👤 **Bwitch** Most Recent ⌚ 1 month, 2 weeks ago
Selected Answer: B
DLP provides the service of redaction.
upvoted 2 times

🗲️ 👤 **DebasishLowes** 10 months, 1 week ago
Its B.
upvoted 2 times

🗲️ 👤 **saurabh1805** 1 year, 2 months ago
B is correct answer here.
upvoted 2 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago
Ans - B
upvoted 2 times

🗲️ 👤 **CHECK666** 1 year, 3 months ago
B is the answer.
upvoted 2 times

🗲️ 👤 **aiwaai** 1 year, 4 months ago
Correct Answer: B
upvoted 1 times

🗲️ 👤 **paxjoshi** 1 year, 4 months ago
Yes, the correct answer is B.
upvoted 1 times

🗲️ 👤 **aiwaai** 1 year, 4 months ago
Correct Answer: B
upvoted 1 times

🗲️ 👤 **bigdo** 1 year, 5 months ago
B D is for vulnerability scanning
upvoted 1 times

🗲️ 👤 **smart123** 1 year, 6 months ago
The Answer is B
upvoted 1 times

🗲️ 👤 **xhova** 1 year, 9 months ago
Definitely B
upvoted 2 times

🗲️ 👤 **meraexam** 1 year, 10 months ago
How it is D. should have been B
upvoted 4 times

A customer has 300 engineers. The company wants to grant different levels of access and efficiently manage IAM permissions between users in the development and production environment projects.

Which two steps should the company take to meet these requirements? (Choose two.)

- A. Create a project with multiple VPC networks for each environment.
- B. Create a folder for each development and production environment.
- C. Create a Google Group for the Engineering team, and assign permissions at the folder level.
- D. Create an Organizational Policy constraint for each folder environment.
- E. Create projects for each environment, and grant IAM rights to each engineering user.

🗲️ 👤 **mozammil89** Highly Voted 👍 1 year, 10 months ago

B and C should be correct...

upvoted 13 times

🗲️ 👤 **Jane111** Most Recent ⌚ 9 months ago

A - no VPC required

B - yes - pre req

C - Yes

D - likely but C is first

E - not scalable/feasible/advisable

upvoted 1 times

🗲️ 👤 **DebasishLowes** 10 months ago

Ans : BC

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - BC

upvoted 1 times

🗲️ 👤 **CHECK666** 1 year, 3 months ago

B,C is the answer.

Create a folder for each env and assign IAM policies to the group.

upvoted 2 times

🗲️ 👤 **Mohita** 1 year, 4 months ago

BC is the right answer, create folder for each env and assign IAM policies to group

upvoted 1 times

🗲️ 👤 **aiwaai** 1 year, 4 months ago

Correct Answer: CE

upvoted 1 times

🗲️ 👤 **aiwaai** 1 year, 4 months ago

made correction CE -> BC

upvoted 2 times

🗲️ 👤 **xhova** 1 year, 9 months ago

B&C

D does not help efficiently manage IAM. Effective IAM implies using groups.

upvoted 2 times

🗲️ 👤 **smart123** 1 year, 7 months ago

Organization policy is used on resources and not the users. Hence option 'D' cannot be right.

upvoted 2 times

🗲️ 👤 **jonclem** 1 year, 9 months ago

I'd say B and D are correct

upvoted 1 times

You want to evaluate GCP for PCI compliance. You need to identify Google's inherent controls. Which document should you review to find the information?

- A. Google Cloud Platform: Customer Responsibility Matrix
- B. PCI DSS Requirements and Security Assessment Procedures
- C. PCI SSC Cloud Computing Guidelines
- D. Product documentation for Compute Engine

🗲️ 👤 **rafaelc** Highly Voted 👍 1 year, 10 months ago

It's A.

https://cloud.google.com/files/PCI_DSS_Shared_Responsibility_GCP_v32.pdf

upvoted 9 times

🗲️ 👤 **Jane111** Most Recent ⌚ 9 months ago

identify Google's inherent controls.

A- Customer Responsibility Matrix A Qualified Security Assessor has assessed and validated these specific requirements and found GCP to be compliant with PCI-DSS v3.2.1

B and C - are guidelines for industry I assume

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - A

upvoted 1 times

🗲️ 👤 **Rantu** 1 year, 3 months ago

A is correct. https://services.google.com/fh/files/misc/gcp_crm_2018.pdf

upvoted 1 times

🗲️ 👤 **aiwaai** 1 year, 4 months ago

Correct Answer: A

upvoted 1 times

🗲️ 👤 **jonclm** 1 year, 9 months ago

I agree, it should be A. C is how to impliment PCI DSS and goes beyond PCI SSC..

upvoted 2 times

A DevOps team will create a new container to run on Google Kubernetes Engine. As the application will be internet-facing, they want to minimize the attack surface of the container.

What should they do?

- A. Use Cloud Build to build the container images.
- B. Build small containers using small base images.
- C. Delete non-used versions from Container Registry.
- D. Use a Continuous Delivery tool to deploy the application.

🗲️ 👤 **xhova** Highly Voted 👍 1 year, 9 months ago
Ans is B

Small containers usually have a smaller attack surface as compared to containers that use large base images.

<https://cloud.google.com/blog/products/gcp/kubernetes-best-practices-how-and-why-to-build-small-container-images>
upvoted 17 times

🗲️ 👤 **smart123** 1 year, 6 months ago
I agree
upvoted 1 times

🗲️ 👤 **lxs** Most Recent 🕒 1 month, 1 week ago
Selected Answer: C

A. Use Cloud Build to build the container images.

If you build a container using Cloud Build or not the surface is the same

B. Build small containers using small base images.

It is indeed best practice, but I doubt if small base images can reduce the surface. It is still the same app version with the same vulnerabilities etc.

C. Delete non-used versions from Container Registry.

Unused, historical versions are additional attack surface. attacker can exploit old, unpatched image which indeed the surface extension.

D. Use a Continuous Delivery tool to deploy the application.

This is just a method of image delivery. The app is the same.

upvoted 1 times

🗲️ 👤 **DebasishLowes** 10 months ago
Ans : B. Small the base image there is less vulnerability and less chance of attack.
upvoted 2 times

🗲️ 👤 **soukumar369** 1 year, 1 month ago
Answer is B : at the cost of more space and a slightly higher surface area for attacks.
upvoted 3 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago
should be A, because cloud build has a feature for vulnerability scan
upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago
Ans - B
upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago
Ans - B
upvoted 1 times

🗲️ 👤 **CHECK666** 1 year, 3 months ago
B is the answer, small containers have smaller attack surface.
upvoted 1 times

🗲️ 👤 **ArizonaClassics** 1 year, 4 months ago
The Correct answer is B
upvoted 1 times

Your company is using GSuite and has developed an application meant for internal usage on Google App Engine. You need to make sure that an external user cannot gain access to the application even when an employee's password has been compromised. What should you do?

- A. Enforce 2-factor authentication in GSuite for all users.
- B. Configure Cloud Identity-Aware Proxy for the App Engine Application.
- C. Provision user passwords using GSuite Password Sync.
- D. Configure Cloud VPN between your private network and GCP.

🗲️ 👤 **rafaelc** Highly Voted 👍 1 year, 10 months ago

A. Enforce 2-factor authentication in GSuite for all users.
upvoted 14 times

🗲️ 👤 **johnsm** Most Recent ⌚ 5 months, 2 weeks ago

Correct answer is A. Well explained here: https://docs.google.com/document/d/11o3e14tyhnT7w45Q8-r9ZmTAfj2WUNUpJPZImrxm_F4/edit?usp=sharing found some other answers for other questions in this site as well.
upvoted 4 times

🗲️ 👤 **Jane111** 9 months ago

Shouldn't it be
B. Configure Cloud Identity-Aware Proxy for the App Engine Application.
identity based app access
upvoted 1 times

🗲️ 👤 **desertlotus1211** 10 months ago

The key is external user. Best practice is to have internal users/datacenter connect via VPN for security purpose, correct? External users will try to connect via Internet - they still cannot reach the app engine even if they have a users' password because a VPN connection is need to reach the resource. MA will work IF the external user has VPN access... But I think D is what they're looking for based on the question....
upvoted 2 times

🗲️ 👤 **DebasishLowes** 10 months ago

Ans : A. When passwords is compromised, enforcing 2 factor authentication is the best way to prevent non authorized users.
upvoted 1 times

🗲️ 👤 **soukumar369** 1 year, 1 month ago

Enforcing 2-factor authentication can save an employee's password has been compromised
upvoted 1 times

🗲️ 👤 **soukumar369** 1 year, 1 month ago

Enforce 2-factor authentication safe employee, when an employee's password has been compromised.
upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - A
upvoted 1 times

🗲️ 👤 **subhala** 1 year, 2 months ago

If you limit your GCP VPC to only private access (no resources having external IP), and have VPN. then inspite of having any creds, external folks cannot access the resources.
upvoted 2 times

🗲️ 👤 **soukumar369** 1 year, 1 month ago

I'm also thinking the same.
upvoted 2 times

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

They can if they login from inside Org - So A is the only correct asnwer
upvoted 1 times

🗲️ 👤 **passtest100** 1 year, 3 months ago

should be B
upvoted 1 times

🗲️ 👤 **CHECK666** 1 year, 3 months ago

A is the answer. User MFA
upvoted 1 times

🗨️ 👤 **xhova** 1 year, 9 months ago
A is the answer. VPN does not help if credentials are compromised.
upvoted 2 times

🗨️ 👤 **smart123** 1 year, 6 months ago
I agree option 'A' is the right answer.
upvoted 1 times

Question #36

Topic 1

A large financial institution is moving its Big Data analytics to Google Cloud Platform. They want to have maximum control over the encryption process of data stored at rest in BigQuery.

What technique should the institution use?

- A. Use Cloud Storage as a federated Data Source.
- B. Use a Cloud Hardware Security Module (Cloud HSM).
- C. Customer-managed encryption keys (CMEK).
- D. Customer-supplied encryption keys (CSEK).

🗨️ 👤 **ownez** Highly Voted 👍 1 year, 4 months ago
Agree with C.
"If you want to control encryption yourself, you can use customer-managed encryption keys (CMEK) for BigQuery"

<https://cloud.google.com/bigquery/docs/customer-managed-encryption>
upvoted 8 times

🗨️ 👤 **dtmtor** Highly Voted 👍 9 months, 4 weeks ago
Answer is C. CSEK not in BigQuery
upvoted 5 times

🗨️ 👤 **DebasishLowes** Most Recent 🕒 10 months ago
Ans : C. CSEK supports only compute engine and Cloud storage. So CMEK is the best option.
upvoted 3 times

🗨️ 👤 **chetz12** 1 year ago
A : as the requirement state max control. you can use CSEK for GCS then federate GCS storage in BQ for analysis
upvoted 1 times

🗨️ 👤 **[Removed]** 1 year, 2 months ago
Ans - C
upvoted 2 times

🗨️ 👤 **CHECK666** 1 year, 3 months ago
C is the answer. Use customer-managed encryption key.
upvoted 2 times

🗨️ 👤 **CHECK666** 1 year, 3 months ago
A is the answer. Use MFA
upvoted 1 times

🗨️ 👤 **mlyu** 1 year, 4 months ago
I think should be D, as the requirement is max. control over the key
<https://cloud.google.com/security/encryption-at-rest>
upvoted 1 times

🗨️ 👤 **MohitA** 1 year, 4 months ago
CSEC is not available for bigquery as of now, so C is the best match
upvoted 2 times

🗨️ 👤 **Sheeda** 1 year, 4 months ago
It is not even supported for big data. See your link.
<https://cloud.google.com/security/encryption-at-rest>
upvoted 1 times

A company is deploying their application on Google Cloud Platform. Company policy requires long-term data to be stored using a solution that can automatically replicate data over at least two geographic places.

Which Storage solution are they allowed to use?

- A. Cloud Bigtable
- B. Cloud BigQuery
- C. Compute Engine SSD Disk
- D. Compute Engine Persistent Disk

🗲️ 👤 **ronron89** Highly Voted 👍 1 year, 1 month ago

<https://cloud.google.com/bigquery#:~:text=BigQuery%20transparently%20and%20automatically%20provides,charge%20and%20no%20additional%20setup.&text=BigQuery%20also%20provides%20ODBC%20and,interact%20with%20its%20powerful%20engine.>

Answer is B.

BigQuery transparently and automatically provides highly durable, replicated storage in multiple locations and high availability with no extra charge and no additional setup.

@xhova: <https://cloud.google.com/bigquery-transfer/docs/locations>

What it mentions here is once you create a replication. YOU cannot change a location. Here the question is about high availability. synchronous replication.

upvoted 10 times

🗲️ 👤 **Arad** 1 month, 3 weeks ago

Correct answer is A.

B is not correct because: "BigQuery does not automatically provide a backup or replica of your data in another geographic region."

<https://cloud.google.com/bigquery/docs/availability>

upvoted 3 times

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

Correct answer is B.

BQ: <https://cloud.google.com/bigquery-transfer/docs/locations#multi-regional-locations> and https://cloud.google.com/bigquery-transfer/docs/locations#colocation_required

Bigtable: <https://cloud.google.com/bigtable/docs/locations>

PS: To people that are only commenting an answer, please provide a valid source to back your answers. This is a community driven forum and just spamming with wrong answers affects all of us.

upvoted 1 times

🗲️ 👤 **Lancyqusa** Most Recent 🕒 2 weeks, 3 days ago

The key here is to set up the resource that will "automatically replicate over two regions". In case of BigQuery, when you set up the resource, you can specify a "location" e.g us or eu, and the data will be replicate over multiple regions. On the other hand, you have to configure the replication and for that reason, is not automatic.

upvoted 1 times

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

Forgot to add - B is the answer :)

upvoted 1 times

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

It is A Bigtable

See : <https://cloud.google.com/bigtable/docs/replication-overview>

upvoted 1 times

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

Selected Answer: B

Correct answer is B.

BQ: <https://cloud.google.com/bigquery-transfer/docs/locations#multi-regional-locations> and https://cloud.google.com/bigquery-transfer/docs/locations#colocation_required

Bigtable: <https://cloud.google.com/bigtable/docs/locations>

PS: To people that are only commenting an answer, please provide a valid source to back your answers. This is a community driven forum and just spamming with wrong answers affects all of us.

upvoted 1 times

🗳️ 👤 **Alex0303** 5 months, 3 weeks ago

A - correct answer. IN BigTable you can create one cluster in region-1, other cluster in region-2

upvoted 1 times

🗳️ 👤 **umashankar_a** 6 months, 1 week ago

Answer A

Automatic Replication of Data in different regions is not supported by Big Query.

<https://cloud.google.com/bigquery/docs/availability>

It states - "In a single region, data is stored only in the region. There is no Google Cloud–provided backup or replication to another region. If you want to use a single region for your datasets but consider the lack of backup or replication too risky, you can create cross-region dataset copies to enhance your disaster recovery guarantees."

So this question specifically asked for "Automatic Data Replication" and it's only possible with Big Table. So Answer is A.

upvoted 2 times

🗳️ 👤 **tzKhalil** 8 months, 1 week ago

Answer is B. Pick BigQuery with multi-region

A multi-region is a large geographic area, such as the United States (US) or Europe (EU), that contains two or more geographic places. In a multi-region, data is stored in a single region but is backed up in a geographically-separated region to provide resilience to a regional disaster. The recovery and failover process is managed by BigQuery.

https://cloud.google.com/bigquery/docs/availability#multi_regions

upvoted 2 times

🗳️ 👤 **talktolanka** 9 months, 1 week ago

Answer is B. the term automatic is matching to BigQuery. Also refer to <https://cloud.google.com/bigquery>

upvoted 1 times

🗳️ 👤 **talktolanka** 8 months, 1 week ago

Very Complicated. automatic replication done by BigTable as well. Also data should be stored for long time. I will go with A

upvoted 1 times

🗳️ 👤 **desertlotus1211** 10 months ago

Answer D: You're forgetting the keywords 'storage solution'

<https://cloud.google.com/persistent-disk>

'For maximum flexibility and minimal effort, snapshots are geo-replicated and available for restore in all regions by default'

upvoted 3 times

🗳️ 👤 **DebasishLowes** 10 months ago

Ans : A

upvoted 1 times

🗳️ 👤 **[Removed]** 1 year, 2 months ago

Ans - A

upvoted 1 times

🗳️ 👤 **Rantu** 1 year, 3 months ago

I was looking for GCS buckets for this, but since we don't have this options, I suspect the answer would be C. Because we have regional pd which can span across geographical places. Bigtable can do the job, but its expensive compared to pd.

<https://cloud.google.com/compute/docs/disks#repds>

upvoted 2 times

🗳️ 👤 **ThisisJohn** 1 month ago

Agree with you.

The question talks about "long-term data to be stored" and persistent disk documentation says the following "regional persistent disks provide durable storage and replication of data between two zones in the same region." <https://cloud.google.com/compute/docs/disks#repds>

On the other side, long-term storage is not mentioned as one use case of BigTable automatic replication

<https://cloud.google.com/bigtable/docs/replication-overview#use-cases>

upvoted 1 times

🗳️ 👤 **CHECK666** 1 year, 3 months ago

A is the answer. Bigtable support automatic replication.

upvoted 1 times

🗳️ 👤 **aiwaai** 1 year, 4 months ago

Correct Answer: A

upvoted 1 times

🗳️ 👤 **ArizonaClassics** 1 year, 5 months ago

A SUPPORTS DATA REPLICATION

<https://cloud.google.com/bigtable/docs/replication-overview>

upvoted 1 times



🗳️ 👤 **ranjeetpatil** 1 year, 7 months ago

I think the Ans is A. The key word is Replication, Big Table does auto replication across regions and Big query can only do backups (make copies of dataset)

<https://cloud.google.com/bigquery/docs/availability>

<https://cloud.google.com/bigtable/docs/replication-overview>

upvoted 2 times

  **xhova** 1 year, 9 months ago

Answer is A.


The question asks about AUTOMATIC REPLICATION. Biq Query cannot automatically replicate data set it must be done manually

<https://cloud.google.com/bigquery-transfer/docs/locations>

Bigtable does automatic replication

<https://cloud.google.com/bigtable/docs/replication-overview>

upvoted 4 times

  **smart123** 1 year, 6 months ago

I agree. The answer is 'A'.

upvoted 1 times

  **Ganshank** 1 year, 7 months ago

I'd go with A.

upvoted 1 times

Question #38

Topic 1

A large e-retailer is moving to Google Cloud Platform with its ecommerce website. The company wants to ensure payment information is encrypted between the customer's browser and GCP when the customers checkout online.

What should they do?

- A. Configure an SSL Certificate on an L7 Load Balancer and require encryption.
- B. Configure an SSL Certificate on a Network TCP Load Balancer and require encryption.
- C. Configure the firewall to allow inbound traffic on port 443, and block all other inbound traffic.
- D. Configure the firewall to allow outbound traffic on port 443, and block all other outbound traffic.

  **ESP_SAP** 1 year, 1 month ago

Correct Answer is (A):

he type of traffic that you need your load balancer to handle is another factor in determining which load balancer to use:

For HTTP and HTTPS traffic, use:

External HTTP(S) Load Balancing

https://cloud.google.com/load-balancing/docs/load-balancing-overview#external_versus_internal_load_balancing

upvoted 4 times

  **[Removed]** 1 year, 2 months ago

Ans - A

upvoted 1 times

  **CHECK666** 1 year, 3 months ago

A is the answer, SSL certificate on L7 layer LoadBlanacer

upvoted 2 times

  **ArizonaClassics** 1 year, 5 months ago


A is the correct one. the question is to see if you understand difference between Layer 7 vs Layer 4 protocols.

upvoted 1 times

  **smart123** 1 year, 6 months ago

Option 'A' is the correct answer.

upvoted 1 times

  **srinidutt** 1 year, 7 months ago

A is right

upvoted 1 times

Applications often require access to "secrets" - small pieces of sensitive data at build or run time. The administrator managing these secrets on GCP wants to keep a track of "who did what, where, and when?" within their GCP projects.

Which two log streams would provide the information that the administrator is looking for? (Choose two.)

- A. Admin Activity logs
- B. System Event logs
- C. Data Access logs
- D. VPC Flow logs
- E. Agent logs

🗲️ 👤 **Ganshank** Highly Voted 👍 1 year, 7 months ago
Agreed AC.
<https://cloud.google.com/secret-manager/docs/audit-logging>
upvoted 7 times

🗲️ 👤 **DebasishLowes** Most Recent ⌚ 10 months, 1 week ago
Ans AC
upvoted 3 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago
Ans - AC
upvoted 2 times

🗲️ 👤 **CHECK666** 1 year, 3 months ago
AC is the answer.
Admin Access Logs and Data Access Logs
upvoted 3 times

🗲️ 👤 **smart123** 1 year, 6 months ago
Yes 'A & C' are the right answers.
upvoted 2 times

You are in charge of migrating a legacy application from your company datacenters to GCP before the current maintenance contract expires. You do not know what ports the application is using and no documentation is available for you to check. You want to complete the migration without putting your environment at risk.

What should you do?

- A. Migrate the application into an isolated project using a "Lift & Shift" approach. Enable all internal TCP traffic using VPC Firewall rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.
- B. Migrate the application into an isolated project using a "Lift & Shift" approach in a custom network. Disable all traffic within the VPC and look at the Firewall logs to determine what traffic should be allowed for the application to work properly.
- C. Refactor the application into a micro-services architecture in a GKE cluster. Disable all traffic from outside the cluster using Firewall Rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.
- D. Refactor the application into a micro-services architecture hosted in Cloud Functions in an isolated project. Disable all traffic from outside your project using Firewall Rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.

🗲️ 👤 **rafaelc** Highly Voted 👍 1 year, 10 months ago

A or B. Leaning towards A

You have a deadline you cannot develop a new app so you have to lift and shift.

upvoted 10 times

🗲️ 👤 **xhova** 1 year, 9 months ago

Answer is A.. You need VPC Flow Logs not "Firewall logs" stated in B

upvoted 5 times

🗲️ 👤 **smart123** 1 year, 6 months ago

I agree.

upvoted 1 times

🗲️ 👤 **GPK** Most Recent 🕒 4 weeks ago

These questions are no more relevant as google has changed exam and made it really challenging now.

upvoted 1 times

🗲️ 👤 **vicky_cyber** 3 weeks, 1 day ago

Could you please help us with recent dumps or guide which dump to be referred

upvoted 1 times

🗲️ 👤 **rr4444** 1 month ago

Selected Answer: B

B - VPC Flow Logs

Firewall logging only covers TCP and UDP, you explicitly don't know what the app does. That limitation is also important to the fact that implied deny all ingress and deny all egress rules are not covered by Firewall Logging. Plus you have to enable Firewall Logging per rule, so you'd have to have a rule for everything in advance - chicken and egg.... you don't know what is going on, so how could you!?

upvoted 1 times

🗲️ 👤 **rr4444** 1 month ago

VPC FLOW logs is A!

I meant A!

upvoted 1 times

🗲️ 👤 **keresh** 8 months, 1 week ago

Answer A matches "without putting your environment at risk" best, all the other answers are higher in risk

upvoted 3 times

🗲️ 👤 **DebasishLowes** 9 months, 4 weeks ago

Ans : A

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - A

upvoted 1 times

🗲️ 👤 **CHECK666** 1 year, 3 months ago

A is the answer. You need to take a look at the VPC Flow Logs to know what kind of traffic going in.

upvoted 2 times

🗑️ 👤 **MohitA** 1 year, 4 months ago
A is the correct Answer
upvoted 1 times

🗑️ 👤 **aiwaai** 1 year, 4 months ago
Correct Answer: B
upvoted 1 times

🗑️ 👤 **aiwaai** 1 year, 4 months ago
made correction B -> A
upvoted 1 times

🗑️ 👤 **srinidutt** 1 year, 7 months ago
A is relevent
upvoted 1 times

Question #41

Topic 1

Your company has deployed an application on Compute Engine. The application is accessible by clients on port 587. You need to balance the load between the different instances running the application. The connection should be secured using TLS, and terminated by the Load Balancer. What type of Load Balancing should you use?

- A. Network Load Balancing
- B. HTTP(S) Load Balancing
- C. TCP Proxy Load Balancing
- D. SSL Proxy Load Balancing

🗑️ 👤 **smart123** Highly Voted 👍 1 year, 6 months ago
Although both TCP Proxy LB and SSL Proxy LB support port 587 but only SSL Proxy LB support TLS. Hence 'D' is the right answer.
upvoted 10 times

🗑️ 👤 **umashankar_a** Most Recent ⌚ 6 months, 1 week ago
Answer D
<https://cloud.google.com/load-balancing/docs/ssl>
- SSL Proxy Load Balancing is a reverse proxy load balancer that distributes SSL traffic coming from the internet to virtual machine (VM) instances in your Google Cloud VPC network.

When using SSL Proxy Load Balancing for your SSL traffic, user SSL (TLS) connections are terminated at the load balancing layer, and then proxied to the closest available backend instances by using either SSL (recommended) or TCP.
upvoted 4 times

🗑️ 👤 **dtmtor** 9 months, 4 weeks ago
Answer: D
upvoted 1 times

🗑️ 👤 **DebasishLowes** 10 months, 3 weeks ago
Ans : D
upvoted 1 times

🗑️ 👤 **[Removed]** 1 year, 2 months ago
Ans - D
upvoted 1 times

🗑️ 👤 **CHECK666** 1 year, 3 months ago
D is the answer. SSL Proxy LoadBalancer supports TLS.
upvoted 2 times

🗑️ 👤 **mlyu** 1 year, 4 months ago
Agreed with smart123. Ans is D
https://cloud.google.com/load-balancing/docs/choosing-load-balancer#flow_chart
upvoted 2 times

You want to limit the images that can be used as the source for boot disks. These images will be stored in a dedicated project. What should you do?

- A. Use the Organization Policy Service to create a `compute.trustedimageProjects` constraint on the organization level. List the trusted project as the whitelist in an allow operation.
- B. Use the Organization Policy Service to create a `compute.trustedimageProjects` constraint on the organization level. List the trusted projects as the exceptions in a deny operation.
- C. In Resource Manager, edit the project permissions for the trusted project. Add the organization as member with the role: Compute Image User.
- D. In Resource Manager, edit the organization permissions. Add the project ID as member with the role: Compute Image User.

🗲️ 👤 **DebasishLowes** Highly Voted 👍 9 months, 4 weeks ago

Ans : A

upvoted 6 times

🗲️ 👤 **[Removed]** Highly Voted 👍 1 year, 2 months ago

Ans - A

https://cloud.google.com/compute/docs/images/restricting-image-access#trusted_images

upvoted 5 times

🗲️ 👤 **CHECK666** Most Recent 🕒 1 year, 3 months ago

A is the answer. you need to allow operations.

upvoted 1 times

🗲️ 👤 **ownez** 1 year, 4 months ago

I agree with B.

"<https://cloud.google.com/compute/docs/images/restricting-image-access>"

upvoted 2 times

🗲️ 👤 **ownez** 1 year, 4 months ago

Answer is A.

"Use the Trusted image feature to define an organization policy that allows your project members to create persistent disks only from images in specific projects."

"After sharing your images with other users, you can control where those users employ those resources within your organization. Set the `constraints/compute.storageResourceUseRestrictions` constraint to define the projects where users are permitted to use your storage resources."

upvoted 2 times

🗲️ 👤 **Sheeda** 1 year, 4 months ago

Yes, A made sense to me too.

upvoted 1 times

Your team needs to prevent users from creating projects in the organization. Only the DevOps team should be allowed to create projects on behalf of the requester.

Which two tasks should your team perform to handle this request? (Choose two.)

- A. Remove all users from the Project Creator role at the organizational level.
- B. Create an Organization Policy constraint, and apply it at the organizational level.
- C. Grant the Project Editor role at the organizational level to a designated group of users.
- D. Add a designated group of users to the Project Creator role at the organizational level.
- E. Grant the billing account creator role to the designated DevOps team.

🗲️ 👤 **mlyu** Highly Voted 👍 1 year, 4 months ago

I think Ans is AD

Because we need to stop the users can create project first (A), and allow devops team to create project (D)

upvoted 12 times

🗲️ 👤 **syllox** Most Recent ⌚ 8 months, 2 weeks ago

Ans AC also

upvoted 1 times

🗲️ 👤 **syllox** 8 months, 2 weeks ago

AD , C is a mistake it's project Editor and not creator

upvoted 3 times

🗲️ 👤 **[Removed]** 9 months, 3 weeks ago

AD is the answer.

If constraint is added , no project creation will be allowed, hence B is wrong

upvoted 3 times

🗲️ 👤 **DebasishLowes** 10 months, 3 weeks ago

Ans : AD

upvoted 3 times

🗲️ 👤 **Aniyadu** 1 year ago

A & D is the right answer.

upvoted 4 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - AD

upvoted 3 times

🗲️ 👤 **genesis3k** 1 year, 2 months ago

I think AC. Because, a role is granted to user/group, rather user/group is added to a role.

upvoted 1 times

🗲️ 👤 **syllox** 8 months, 2 weeks ago

C is a mistake it's project Editor and not creator

upvoted 1 times

🗲️ 👤 **CHECK666** 1 year, 3 months ago

AD is the answer. There's nothing related to project creation in organization policy constraints.

upvoted 4 times

A customer deployed an application on Compute Engine that takes advantage of the elastic nature of cloud computing.

How can you work with Infrastructure Operations Engineers to best ensure that Windows Compute Engine VMs are up to date with all the latest OS patches?

- A. Build new base images when patches are available, and use a CI/CD pipeline to rebuild VMs, deploying incrementally.
- B. Federate a Domain Controller into Compute Engine, and roll out weekly patches via Group Policy Object.
- C. Use Deployment Manager to provision updated VMs into new serving Instance Groups (IGs).
- D. Reboot all VMs during the weekly maintenance window and allow the StartUp Script to download the latest patches from the internet.

🗲️ 👤 **genesis3k** Highly Voted 👍 1 year, 2 months ago

Answer is A.

Compute Engine doesn't automatically update the OS or the software on your deployed instances. You will need to patch or update your deployed Compute Engine instances when necessary. However, in the cloud it is not recommended that you patch or update individual running instances. Instead it is best to patch the image that was used to launch the instance and then replace each affected instance with a new copy.

upvoted 16 times

🗲️ 👤 **VenkatGCP1** Most Recent 🕒 2 weeks, 1 day ago

The answer is A, we are using this in practice as a solution from Google in one of the top 5 banks for managing windows image patching.

upvoted 1 times

🗲️ 👤 **lxs** 1 month, 1 week ago

Selected Answer: A

Definitely it will be A. The solution must take the advantage of elasticity of compute engine, so you create a template with patched OS base and redeploy images.

upvoted 1 times

🗲️ 👤 **sc_cloud_learn** 6 months, 2 weeks ago

Answer should be A,

C talks about MIG which may not be always needed

upvoted 1 times

🗲️ 👤 **DebasishLowes** 9 months, 4 weeks ago

Ans : A

upvoted 1 times

🗲️ 👤 **gu9singg** 9 months, 3 weeks ago

this questions still valid for exam?

upvoted 1 times

🗲️ 👤 **umashankar_a** 6 months, 1 week ago

yeah....even i'm thinking the same, as we got OS Patch Management Service now in GCP for Patching Compute machines as per requirement.

<https://cloud.google.com/compute/docs/os-patch-management>.

Not really sure on the answer.

upvoted 1 times

🗲️ 👤 **DuncanTu** 6 months, 1 week ago

Hi

May I know why C is incorrect?

upvoted 1 times

🗲️ 👤 **HateMicrosoft** 10 months, 1 week ago

The correct anwser is C.

<https://cloud.google.com/deployment-manager/docs/reference/latest/deployments/patch>

upvoted 1 times

🗲️ 👤 **CloudTrip** 11 months ago

Given the options here Answer D seems practical


upvoted 1 times

🗲️ 👤 **singhjoga** 1 year ago

B seems the only possible answer. Windows patches are configured using Group Policies on the Windows Domain Controller. All other windows machines should be part of the same domain.

upvoted 1 times

🗲️

 **FatCharlie** 1 year, 1 month ago

The answer is A. This is referring to VMs in an instance group which has built in roll out deployment of new images that can easily be integrated into a CI/CD pipeline.

The people mentioning the patch management tool are considering these to be long running VMs, but that makes little sense in an instance group.

upvoted 3 times

  **[Removed]** 1 year, 2 months ago



Ans - A

upvoted 3 times

  **Wooky** 1 year, 3 months ago

I think best ans is C

upvoted 4 times

  **mlyu** 1 year, 4 months ago

None of the answer makes sense.

GCP has provide os patch management tool to patch Windows OS

<https://cloud.google.com/compute/docs/os-patch-management>

upvoted 2 times

  **Sheeda** 1 year, 4 months ago

Next best is D ?

upvoted 1 times

Your team needs to make sure that their backend database can only be accessed by the frontend application and no other instances on the network.

How should your team design this network?

- A. Create an ingress firewall rule to allow access only from the application to the database using firewall tags.
- B. Create a different subnet for the frontend application and database to ensure network isolation.
- C. Create two VPC networks, and connect the two networks using Cloud VPN gateways to ensure network isolation.
- D. Create two VPC networks, and connect the two networks using VPC peering to ensure network isolation.

🗲️ 👤 **zqwiklabs** 9 months, 2 weeks ago

A is definitely incorrect

upvoted 3 times

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

This one is confusing but cannot be A because it says 'Firewall tags'. There is no such thing as firewall tags, only 'Network tags'.

upvoted 1 times

🗲️ 👤 **desertlotus1211** 10 months ago

Answer is D: you'd want the DB in a separate VPC. Allow vpc peering and connect the Front End's backend to the DB. Don't get confused by the question saying 'front end' Front end only means public facing...

upvoted 1 times

🗲️ 👤 **Jane111** 9 months ago

you need to read basic concepts again

upvoted 6 times

🗲️ 👤 **DebasishLowes** 10 months, 3 weeks ago

Ans : A

upvoted 3 times

🗲️ 👤 **singhjoga** 1 year ago

Although A is correct, but B would be more secure when combined with firewall rules to restrict traffic based on subnets.

Ideal solution would be to use Service Account based firewall rules instead of tag based. See the below paragraph from

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

"However, even though it is possible to uses tags for target filtering in this manner, we recommend that you use service accounts where possible. Target tags are not access-controlled and can be changed by someone with the instanceAdmin role while VMs are in service. Service accounts are access-controlled, meaning that a specific user must be explicitly authorized to use a service account. There can only be one service account per instance, whereas there can be multiple tags. Also, service accounts assigned to a VM can only be changed when the VM is stopped"

upvoted 4 times

🗲️ 👤 **ThisisJohn** 1 month ago

You may be right but B doesn't mention anything about firewall rules, thus we need to assume there will be communication between both subnets

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - A

upvoted 2 times

🗲️ 👤 **CHECK666** 1 year, 3 months ago

A is the answer, use network tags.

upvoted 4 times

🗲️ 👤 **mlyu** 1 year, 4 months ago



Agree with A



upvoted 2 times



An organization receives an increasing number of phishing emails.
Which method should be used to protect employee credentials in this situation?

- A. Multifactor Authentication
- B. A strict password policy
- C. Captcha on login pages
- D. Encrypted emails



  **DebasishLowes** Highly Voted 10 months, 3 weeks ago
A is the answer.
upvoted 5 times



  **lxs** Most Recent 1 month, 1 week ago
Selected Answer: D
This question has been taken from the GCP book.
upvoted 1 times



  **mondigo** 1 year, 1 month ago
A
<https://cloud.google.com/blog/products/g-suite/7-ways-admins-can-help-secure-accounts-against-phishing-g-suite>
upvoted 3 times



  **ronron89** 1 year, 1 month ago
<https://www.duocircle.com/content/email-security-services/email-security-in-cryptography#:~:text=Customer%20Login-,Email%20Security%20In%20Cryptography%20Is%20One%20Of%20The%20Most,Measures%20To%20Prevent%20Phishing%20Attempts&text=Cybercriminals%20love%20emails%20the%20most,networks%20all%20over%20the%20world.>

The answer should be D.
upvoted 1 times

  **shk2011** 1 year, 2 months ago
Logically if i think even if i have not read about cloud answer is A
upvoted 3 times

  **[Removed]** 1 year, 2 months ago
Ans - A
upvoted 2 times

  **CHECK666** 1 year, 3 months ago
The answer is A.
<https://cloud.google.com/blog/products/identity-security/protect-users-in-your-apps-with-multi-factor-authentication>
upvoted 3 times

  **Sheeda** 1 year, 4 months ago
Should be A
upvoted 3 times

A customer is collaborating with another company to build an application on Compute Engine. The customer is building the application tier in their GCP

Organization, and the other company is building the storage tier in a different GCP Organization. This is a 3-tier web application. Communication between portions of the application must not traverse the public internet by any means.

Which connectivity option should be implemented?

- A. VPC peering
- B. Cloud VPN
- C. Cloud Interconnect
- D. Shared VPC

🗲️ 👤 **sc_cloud_learn** Highly Voted 👍 6 months, 2 weeks ago
both are GCP, should be VPC peering- Option A
upvoted 7 times

🗲️ 👤 **DP_GCP** Most Recent ⌚ 8 months, 2 weeks ago
B is not correct because if Cloud VPN is used data travels over internet and question mentions it doesnt want the data to travel through internet.
<https://cloud.google.com/network-connectivity/docs/vpn/concepts/overview> Cloud VPN securely connects your peer network to your Virtual Private Cloud (VPC) network through an IPsec VPN connection. Traffic traveling between the two networks is encrypted by one VPN gateway and then decrypted by the other VPN gateway. This action protects your data as it travels over the internet
upvoted 1 times

🗲️ 👤 **dtmtor** 10 months ago
A, different orgs
upvoted 3 times

🗲️ 👤 **DebasishLowes** 10 months, 3 weeks ago
A is the answer.
upvoted 2 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago
Ans - A
upvoted 3 times

🗲️ 👤 **CHECK666** 1 year, 3 months ago
A is the ansswer. use VCP Peering.
upvoted 3 times

🗲️ 👤 **Akku1614** 1 year, 4 months ago
Yes it Should be VPC Peering. <https://cloud.google.com/vpc/docs/vpc-peering>
upvoted 3 times

🗲️ 👤 **Sheeda** 1 year, 4 months ago
Should be A
upvoted 4 times

Which two security characteristics are related to the use of VPC peering to connect two VPC networks? (Choose two.)

- A. Central management of routes, firewalls, and VPNs for peered networks
- B. Non-transitive peered networks; where only directly peered networks can communicate
- C. Ability to peer networks that belong to different Google Cloud Platform organizations
- D. Firewall rules that can be created with a tag from one peered network to another peered network
- E. Ability to share specific subnets across peered networks

🗲️ 👤 **DebasishLowes** Highly Voted 👍 9 months, 3 weeks ago

Ans : BC

upvoted 7 times

🗲️ 👤 **dtmtor** Most Recent ⌚ 10 months ago

Answer is BC

upvoted 2 times

🗲️ 👤 **Aniyadu** 1 year ago

B&C is the right answer

upvoted 2 times

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

The answers marked in the question seem to be referring to _shared_ VPC capabilities.

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - BC

upvoted 2 times

🗲️ 👤 **CHECK666** 1 year, 3 months ago

BC is the answer.

upvoted 2 times

🗲️ 👤 **cipher90** 1 year, 4 months ago

AD is correct "Security Characteristics"

upvoted 1 times

🗲️ 👤 **mte_tech34** 1 year, 3 months ago

No it's not. "You cannot use a tag or service account from one peered network in the other peered network." ->
<https://cloud.google.com/vpc/docs/vpc-peering>

upvoted 2 times

🗲️ 👤 **mlyu** 1 year, 4 months ago

Ans should be BC

https://cloud.google.com/vpc/docs/vpc-peering#key_properties

upvoted 4 times

🗲️ 👤 **MohitA** 1 year, 4 months ago

agree BC

upvoted 1 times

🗲️ 👤 **ownez** 1 year, 4 months ago

Correct.

B: "Only directly peered networks can communicate. Transitive peering is not supported."

C: " You can make services available privately across different VPC networks within and across organizations."

upvoted 2 times

🗲️ 👤 **Mihai89** 1 year, 1 month ago

Agree with BC

upvoted 1 times

A patch for a vulnerability has been released, and a DevOps team needs to update their running containers in Google Kubernetes Engine (GKE). How should the DevOps team accomplish this?

- A. Use Puppet or Chef to push out the patch to the running container.
- B. Verify that auto upgrade is enabled; if so, Google will upgrade the nodes in a GKE cluster.
- C. Update the application code or apply a patch, build a new image, and redeploy it.
- D. Configure containers to automatically upgrade when the base image is available in Container Registry.

🗲️ 👤 **TNT87** Highly Voted 👍 11 months, 1 week ago

<https://cloud.google.com/containers/security>

Containers are meant to be immutable, so you deploy a new image in order to make changes. You can simplify patch management by rebuilding your images regularly, so the patch is picked up the next time a container is deployed. Get the full picture of your environment with regular image security reviews.

C is better

upvoted 8 times

🗲️ 👤 **DebasishLowes** Highly Voted 👍 9 months, 3 weeks ago

Ans : C

upvoted 5 times

🗲️ 👤 **Rhehehe** Most Recent 🕒 3 weeks, 2 days ago

Its actually B.

Patching a vulnerability involves upgrading to a new GKE or Anthos version number. GKE and Anthos versions include versioned components for the operating system, Kubernetes components, and other containers that make up the Anthos platform. Fixing some vulnerabilities requires only a control plane upgrade, performed automatically by Google on GKE, while others require both control plane and node upgrades.

To keep clusters patched and hardened against vulnerabilities of all severities, we recommend using node auto-upgrade on GKE (on by default). On other Anthos platforms, Google recommends upgrading your Anthos components at least monthly.

Ref: <https://cloud.google.com/kubernetes-engine/docs/resources/security-patching>

upvoted 1 times

🗲️ 👤 **SuperDevops** 2 months ago

I took the test yesterday and didn't pass, NO ISSUE is from here. The questions are totally new Whizlabs it's OK

upvoted 1 times

🗲️ 👤 **sriz** 2 months ago

u got questions from Whizlabs?

upvoted 1 times

🗲️ 👤 **Aniyadu** 1 year ago

The question asked is "team needs to update their running containers" if its was auto enabled there was no need to update manually. so my answer will be C.

upvoted 2 times

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

Me voy definitivamente con la C, dado que actualizar los nodos con autoupgrade no tiene nada que ver con los contenedores, la vulnerabilidad en este caso se debe aplicar con respecto a contenedor ósea aplicación por lo que la respuesta C es la correcta.

upvoted 3 times

🗲️ 👤 **soukumar369** 1 year, 1 month ago

Translaed : 'm definitely going with C, since updating the nodes with autoupgrade has nothing to do with the containers, the vulnerability in this case must be applied with respect to the application bone container so the C answer is correct.

upvoted 1 times

🗲️ 👤 **jonclem** 1 year, 2 months ago

Answer B is correct as per the Video Google Kubernetes Engine (GKE) Security on Linuxacademy.

upvoted 2 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - C

upvoted 3 times

🗲️ 👤 **Rantu** 1 year, 3 months ago

C is the correct answer as this is the way to patch, build, re-deploy

upvoted 3 times

🗨️ 👤 **Namaste** 1 year, 3 months ago

Answer is C.

upvoted 3 times

🗨️ 👤 **ownez** 1 year, 3 months ago

I would go for C because some reported CVEs will take time to be published and approval in CVE advisory portal. Once approved, it will notify to all necessary third party.

Hence, this requires a lot of time and left people exposed to the vulnerability.

Answer is C.

upvoted 3 times

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

Answer should be B.. Auto upgrade

upvoted 2 times

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

Auto upgrade of the Nodes does not upgrade the container code which needs the patch

upvoted 3 times

🗨️ 👤 **Mohita** 1 year, 4 months ago

Answer is B

upvoted 1 times


🗨️ 👤 **MohitA** 1 year, 4 months ago


Sorry It should be C

upvoted 5 times


A customer wants to deploy a large number of 3-tier web applications on Compute Engine.
How should the customer ensure authenticated network separation between the different tiers of the application?

- A. Run each tier in its own Project, and segregate using Project labels.
- B. Run each tier with a different Service Account (SA), and use SA-based firewall rules.
- C. Run each tier in its own subnet, and use subnet-based firewall rules.
- D. Run each tier with its own VM tags, and use tag-based firewall rules.


-  **genesis3k**


Highly Voted 

1 year, 2 months ago

Answer is B. Keyword is 'authenticated". Reference below:
"Isolate VMs using service accounts when possible"
"even though it is possible to uses tags for target filtering in this manner, we recommend that you use service accounts where possible. Target tags are not access-controlled and can be changed by someone with the instanceAdmin role while VMs are in service. Service accounts are access-controlled, meaning that a specific user must be explicitly authorized to use a service account. There can only be one service account per instance, whereas there can be multiple tags. Also, service accounts assigned to a VM can only be changed when the VM is stopped."
<https://cloud.google.com/solutions/best-practices-vpc-design#isolate-vms-service-accounts>
upvoted 16 times
-  **gu9singg**

9 months, 3 weeks ago


document says about subnet isolation
upvoted 1 times
-  **mistryminded**

Most Recent 

1 month, 1 week ago


Selected Answer: B

Answer is B - <https://cloud.google.com/vpc/docs/firewalls#service-accounts-vs-tags>
upvoted 1 times

 **gu9singg**


9 months, 3 weeks ago

C: is incorrect, we need to authenticate, network rules does not apply and not a recommend best practice from google
upvoted 1 times

 **gu9singg**


9 months, 3 weeks ago

C: is incorrect because we need to spend lot of time designing the network topology etc, google recommended practice is to use simple network design with automation in mind, so service account provides those, hence final decision goes to B
upvoted 2 times

 **gu9singg**


9 months, 3 weeks ago

Correct answer is B
upvoted 2 times

 **DebasishLowes**


9 months, 3 weeks ago

Ans : C
upvoted 1 times

 **singhjoga**


1 year ago

B as per best practices <https://cloud.google.com/solutions/best-practices-vpc-design>
upvoted 3 times

 **Fellipo**

1 year, 2 months ago


B exists?
upvoted 1 times

 **[Removed]**

1 year, 2 months ago


Ans - C
https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations#networking_and_security

https://cloud.google.com/solutions/best-practices-vpc-design#addresses_and_subnets
upvoted 1 times

 **Rantu**


1 year, 3 months ago

Authenticated separation is the key here. Ideally it should be tag based firewall rule separation. However authenticated word creates confusion. My best judgement is B
upvoted 2 times


 **CHECK666**

1 year, 3 months ago


C is the answer.
upvoted 1 times

-  **Wooky** 1 year, 3 months ago

should be C

upvoted 1 times
-  **MohitA** 1 year, 4 months ago

A should be correct

upvoted 1 times
-  **MohitA** 1 year, 4 months ago

Sorry B seems to be more appropriate


upvoted 3 times

Question #51


Topic 1

A manager wants to start retaining security event logs for 2 years while minimizing costs. You write a filter to select the appropriate log entries. Where should you export the logs?


- A. BigQuery datasets
- B. Cloud Storage buckets
- C. StackDriver logging
- D. Cloud Pub/Sub topics

-  **jayk22** 2 months, 2 weeks ago


Ans B. Validated.

upvoted 1 times
-  **DebasishLowes** 10 months, 1 week ago


Ans: B

upvoted 4 times
-  **[Removed]** 1 year, 2 months ago

Ans - B


upvoted 1 times
-  **Raushanr** 1 year, 3 months ago

Ans is B

upvoted 1 times
-  **mlyu** 1 year, 4 months ago

Ans B

Cloud storage is always considered when minimize cost

upvoted 2 times
-  **MohitA** 1 year, 4 months ago

Agree B

upvoted 1 times

For compliance reasons, an organization needs to ensure that in-scope PCI Kubernetes Pods reside on "in-scope" Nodes only. These Nodes can only contain the "in-scope" Pods.
How should the organization achieve this objective?

- A. Add a nodeSelector field to the pod configuration to only use the Nodes labeled inscope: true.
- B. Create a node pool with the label inscope: true and a Pod Security Policy that only allows the Pods to run on Nodes with that label.
- C. Place a taint on the Nodes with the label inscope: true and effect NoSchedule and a toleration to match in the Pod configuration.
- D. Run all in-scope Pods in the namespace "in-scope-pci".

🗨️ 👤 **SuperDevops** 2 months ago

I took the test yesterday and didn't pass, NO ISSUE is from here. The questions are totally new
Whizlabs it's OK
upvoted 1 times

🗨️ 👤 **pythonrocks** 6 months, 1 week ago

A(nodeSelector) is hard and stronger than C (Taints, which only repels) for k8s scheduling. so A.
upvoted 3 times

🗨️ 👤 **heftjustice** 3 weeks, 1 day ago

Ref: <https://kubernetes.io/docs/concepts/scheduling-eviction/assign-pod-node/>
upvoted 1 times

🗨️ 👤 **umashankar_a** 6 months, 1 week ago

Answer C:
The Question clearly states : Pods reside on "in-scope" Nodes only. These Nodes can only contain the "in-scope" Pods. It's clearly Taints and Toleration scenario.
Taints and tolerations work together to ensure that pods are not scheduled onto inappropriate nodes. One or more taints are applied to a node; this marks that the node should not accept any pods that do not tolerate the taints.
Above Line is from : <https://kubernetes.io/docs/concepts/scheduling-eviction/taint-and-toleration/>
upvoted 4 times

🗨️ 👤 **keresh** 8 months ago

C seems to be best because you add the control on the node level, this way you make sure that it cannot be overridden, by a pod configuration.
"Taints and tolerations are a flexible way to steer pods away from nodes or evict pods that shouldn't be running." from
<https://kubernetes.io/docs/concepts/scheduling-eviction/taint-and-toleration/>
upvoted 4 times

🗨️ 👤 **VIKNOOK** 8 months ago

C
kubectl taint nodes node1 key1=value1:NoSchedule

places a taint on node node1. The taint has key key1, value value1, and taint effect NoSchedule. This means that no pod will be able to schedule onto node1 unless it has a matching toleration.
upvoted 3 times

🗨️ 👤 **iamoct** 9 months, 4 weeks ago

A
<https://kubernetes.io/docs/concepts/scheduling-eviction/assign-pod-node/>
upvoted 2 times

🗨️ 👤 **[Removed]** 1 year, 2 months ago

Ans - A
https://cloud.google.com/solutions/scope-and-size-kubernetes-engine-clusters#workload_mobility
upvoted 2 times

🗨️ 👤 **Rantu** 1 year, 3 months ago

A is the answer nodeSelector. Taint is needed when we don't want to schedule anything on a tainted node except xyz pods (with toleration for those nodes).
upvoted 3 times



🗨️ 👤 **Namaste** 1 year, 3 months ago

A is the Answer. NodeSelector
upvoted 2 times

🗨️ 👤 **Akku1614** 1 year, 4 months ago

Answer is C, as Taint helps to repel unwanted pods and tolerance on specific pod helps to schedule a specific pod on tainted node.

upvoted 4 times

  **mlyu** 1 year, 4 months ago

Ans is A

When you define a Service, you can indirectly control which node pool it is deployed into. The node pool is not dependent on the configuration of the Service, but on the configuration of the Pod.

https://cloud.google.com/kubernetes-engine/docs/concepts/node-pools#deploying_services_to_specific_node_pools

upvoted 3 times

  **MohitA** 1 year, 4 months ago

B i think

upvoted 3 times

In an effort for your company messaging app to comply with FIPS 140-2, a decision was made to use GCP compute and network services. The messaging app architecture includes a Managed Instance Group (MIG) that controls a cluster of Compute Engine instances. The instances use Local SSDs for data caching and UDP for instance-to-instance communications. The app development team is willing to make any changes necessary to comply with the standard. Which options should you recommend to meet the requirements?

- A. Encrypt all cache storage and VM-to-VM communication using the BoringCrypto module.
- B. Set Disk Encryption on the Instance Template used by the MIG to customer-managed key and use BoringSSL for all data transit between instances.
- C. Change the app instance-to-instance communications from UDP to TCP and enable BoringSSL on clients' TLS connections.
- D. Set Disk Encryption on the Instance Template used by the MIG to Google-managed Key and use BoringSSL library on all instance-to-instance communications.

🗲️  **subhala** Highly Voted 👍 1 year, 1 month ago

when I revisited this, Now I think A is correct. In A - We will use an approved encryption method for encrypting Local SSD and VM to VM communication. In B and D, we are still using GCP's encryption algorithms and are not FIPS 140-2 approved. Moreover only the BoringCrypto is FIPS 140-2 approved and not the Boring SSL. I see A as evidently correct. ownez, genesis3k, MohitA has explained this and provided the right links too.

upvoted 9 times

🗲️  **[Removed]** Most Recent ⌚ 9 months ago

D is the correct answer

upvoted 2 times

🗲️  **DebasishLowes** 9 months, 3 weeks ago

Ans : A

upvoted 1 times

🗲️  **TNT87** 10 months, 1 week ago

<https://cloud.google.com/security/compliance/fips-140-2-validated>

Google Cloud Platform uses a FIPS 140-2 validated encryption module called BoringCrypto (certificate 3318) in our production environment. This means that both data in transit to the customer and between data centers, and data at rest are encrypted using FIPS 140-2 validated encryption. The module that achieved FIPS 140-2 validation is part of our BoringSSL library.

Ans A

upvoted 3 times

🗲️  **TNT87** 11 months, 1 week ago

A is the answer <https://boringssl.googlesource.com/boringssl/+/master/crypto/fipsmodule/FIPS.md>

upvoted 2 times

🗲️  **chetz12** 1 year ago

I think A is correct as that's the only one support FIPS140 module

upvoted 3 times

🗲️  **[Removed]** 1 year, 2 months ago

Ans - B

upvoted 1 times

🗲️  **genesis3k** 1 year, 2 months ago

Agree Answer is A definitely.

"BoringSSL as a whole is not FIPS validated. However, there is a core library (called BoringCrypto) that has been FIPS validated"


<https://boringssl.googlesource.com/boringssl/+/master/crypto/fipsmodule/FIPS.md>

upvoted 3 times

🗲️  **saaurabh1805** 1 year, 2 months ago

For me correct answer is B

upvoted 1 times

🗲️  **ownez** 1 year, 3 months ago

Answer is A.

BoringSSL as a whole is not FIPS validated.

<https://boringssl.googlesource.com/boringssl/+/master/crypto/fipsmodule/FIPS.md>

upvoted 2 times

🗲️  **mte_tech34** 1 year, 3 months ago

According to <https://cloud.google.com/security/compliance/fips-140-2-validated>

"Google's Local SSD storage product is automatically encrypted with NIST approved ciphers, but Google's current implementation for this product doesn't have a FIPS 140-2 validation certificate. If you require FIPS-validated encryption on Local SSD storage, you must provide your own encryption with a FIPS-validated cryptographic module."

So only A seems to be correct, as BoringSSL is FIPS-140-2 validated.

upvoted 1 times

  **mte_tech34** 1 year, 3 months ago


I meant BoringCrypto, not BoringSSL, as it's not the same thing and only BoringCrypto is FIPS validated. BoringSSL is not (see <https://boringssl.googlesource.com/boringssl/+master/crypto/fipsmodule/FIPS.md>), so definitely only A can be correct answer.

upvoted 1 times

  **Raushanr** 1 year, 3 months ago

Another reasoning on Google Documentation-You cannot use your own keys with local SSDs because local SSDs do not persist beyond the life of a virtual machine. Local SSDs are already protected with an ephemeral encryption key that Google does not retain.



upvoted 2 times

  **Raushanr** 1 year, 3 months ago

Answer-B

Reasoning from Google-Google's Local SSD storage product is automatically encrypted with NIST approved ciphers, but Google's current implementation for this product doesn't have a FIPS 140-2 validation certificate. If you require FIPS-validated encryption on Local SSD storage, you must provide your own encryption with a FIPS-validated cryptographic module.



upvoted 3 times

  **ownez** 1 year, 4 months ago

I think it is B.



https://services.google.com/fh/files/misc/googlecloud_european_commitments_whitepaper.pdf

upvoted 3 times

  **ownez** 1 year, 4 months ago

This is because "The instances use Local SSDs for data caching" and in the documentation says "If you require FIPS-validated encryption on Local SSD storage, you must provide your own encryption with a FIPS-validated cryptographic module."

upvoted 1 times

  **mlyu** 1 year, 4 months ago

Agreed ans is D

upvoted 1 times

  **MohitA** 1 year, 4 months ago

<https://cloud.google.com/security/compliance/fips-140-2-validated>

upvoted 1 times

A customer has an analytics workload running on Compute Engine that should have limited internet access. Your team created an egress firewall rule to deny (priority 1000) all traffic to the internet. The Compute Engine instances now need to reach out to the public repository to get security updates. What should your team do?

- A. Create an egress firewall rule to allow traffic to the CIDR range of the repository with a priority greater than 1000.
- B. Create an egress firewall rule to allow traffic to the CIDR range of the repository with a priority less than 1000.
- C. Create an egress firewall rule to allow traffic to the hostname of the repository with a priority greater than 1000.
- D. Create an egress firewall rule to allow traffic to the hostname of the repository with a priority less than 1000.

  **dtmtor** Highly Voted 10 months ago

Answer is B. Lower number is higher priority and dest is only IP ranges in firewall rules
upvoted 14 times

  **Rithac** Most Recent 7 months ago

I think I am confusing myself by overthinking the wording of this question. I know the answer is A or B since "using hostname is not one of the options in firewall egress rule destination" I also know that "The firewall rule priority is an integer from 0 to 65535, inclusive. Lower integers indicate higher priorities." I know that I could resolve this by setting TCP port 80 rule to a priority of 500 (smaller number, but higher priority) and be done. Where i'm second guessing myself, is Google referring to the integer or strictly priority? If integer then i'd choose B "priority less than 1000 (smaller number)", if priority then i'd choose A "priority greater than 1000" (still the lower number). Have I thoroughly confused this question? I'm leaning toward the answer being "A":
upvoted 1 times

  **DebasishLowes** 9 months, 3 weeks ago

Ans : B
upvoted 3 times

  **ronron89** 1 year, 1 month ago

Answer: B
https://cloud.google.com/vpc/docs/firewalls#rule_assignment
The priority of the second rule determines whether TCP traffic to port 80 is allowed for the webserver targets:

If the priority of the second rule is set to a number greater than 1000, it has a lower priority, so the first rule denying all traffic applies.

If the priority of the second rule is set to 1000, the two rules have identical priorities, so the first rule denying all traffic applies.

If the priority of the second rule is set to a number less than 1000, it has a higher priority, thus allowing traffic on TCP 80 for the webserver targets. Absent other rules, the first rule would still deny other types of traffic to the webserver targets, and it would also deny all traffic, including TCP 80, to instances without the webserver tag.
upvoted 4 times

  **[Removed]** 1 year, 2 months ago



Ans - B
upvoted 2 times

  **Raushanr** 1 year, 3 months ago

The firewall rule priority is an integer from 0 to 65535, inclusive. Lower integers indicate higher priorities. If you do not specify a priority when creating a rule, it is assigned a priority of 1000.
upvoted 1 times



  **Raushanr** 1 year, 3 months ago

Answer-B
upvoted 4 times

  **ownez** 1 year, 4 months ago



It should be B.

Firewall rules can be only specify by IPv4 address or IPv4 block in CIDR.
And it must be lesser priority than 1000 because if more than that, it will overwrite the deny rule.
upvoted 2 times

  **ownez** 1 year, 4 months ago



Sorry It should be A.

"Priority: the numeric evaluation order of the rule. A rule with a priority of 1 is evaluated first. Priorities must be unique for each rule. A good practice is to give rules priority numbers that allow later insertion (such as 100, 200, 300)."
upvoted 1 times

  **ownez** 1 year, 3 months ago

Correction. B

upvoted 3 times

  **mlyu** 1 year, 4 months ago

Ans should be A

using hostname is not one of the options in firewall egress rule destination

https://cloud.google.com/vpc/docs/firewalls#gcp_firewall_rule_summary_table

upvoted 2 times

Question #55

Topic 1

You want data on Compute Engine disks to be encrypted at rest with keys managed by Cloud Key Management Service (KMS). Cloud Identity and Access

Management (IAM) permissions to these keys must be managed in a grouped way because the permissions should be the same for all keys.

What should you do?

- A. Create a single KeyRing for all persistent disks and all Keys in this KeyRing. Manage the IAM permissions at the Key level.
- B. Create a single KeyRing for all persistent disks and all Keys in this KeyRing. Manage the IAM permissions at the KeyRing level.
- C. Create a KeyRing per persistent disk, with each KeyRing containing a single Key. Manage the IAM permissions at the Key level.
- D. Create a KeyRing per persistent disk, with each KeyRing containing a single Key. Manage the IAM permissions at the KeyRing level.

  **TNT87** Highly Voted  11 months, 1 week ago

Ans B

<https://cloud.netapp.com/blog/gcp-cvo-blg-how-to-use-google-cloud-encryption-with-a-persistent-disk>

upvoted 8 times

  **[Removed]** Most Recent  9 months ago

How about A?

upvoted 1 times

  **[Removed]** 9 months ago

oh, the same permission ,then I choose B

upvoted 2 times

  **DebasishLowes** 9 months, 3 weeks ago



Ans : B

upvoted 3 times

  **[Removed]** 1 year, 2 months ago

Ans - B

upvoted 1 times

  **Raushanr** 1 year, 3 months ago

Answer-B

upvoted 1 times

  **Namaste** 1 year, 3 months ago

B is the right answer

upvoted 1 times

  **Mohita** 1 year, 4 months ago

B should be the answer

upvoted 4 times

A company is backing up application logs to a Cloud Storage bucket shared with both analysts and the administrator. Analysts should only have access to logs that do not contain any personally identifiable information (PII). Log files containing PII should be stored in another bucket that is only accessible by the administrator.

What should you do?

- A. Use Cloud Pub/Sub and Cloud Functions to trigger a Data Loss Prevention scan every time a file is uploaded to the shared bucket. If the scan detects PII, have the function move into a Cloud Storage bucket only accessible by the administrator.
- B. Upload the logs to both the shared bucket and the bucket only accessible by the administrator. Create a job trigger using the Cloud Data Loss Prevention API. Configure the trigger to delete any files from the shared bucket that contain PII.
- C. On the bucket shared with both the analysts and the administrator, configure Object Lifecycle Management to delete objects that contain any PII.
- D. On the bucket shared with both the analysts and the administrator, configure a Cloud Storage Trigger that is only triggered when PII data is uploaded. Use Cloud Functions to capture the trigger and delete such files.

🗲️ 👤 **Mohita** Highly Voted 👍 1 year, 4 months ago

A is the ans
upvoted 11 times

🗲️ 👤 **[Removed]** Most Recent ⌚ 9 months ago

I also choose A.
upvoted 3 times

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

Answer A
<https://codelabs.developers.google.com/codelabs/cloud-storage-dlp-functions#0>
<https://www.youtube.com/watch?v=0TmO1f-Ox40>
upvoted 4 times

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

Ans : A
upvoted 2 times

🗲️ 👤 **soukumar369** 1 year ago

Correct answer is A : Data Loss Prevention scan
upvoted 2 times

🗲️ 👤 **soukumar369** 1 year ago

A is correct.
upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - A
upvoted 1 times

🗲️ 👤 **genesis3k** 1 year, 2 months ago

Answer is A.
upvoted 1 times

🗲️ 👤 **passtest100** 1 year, 3 months ago

SHOULD BE A
upvoted 1 times

A customer terminates an engineer and needs to make sure the engineer's Google account is automatically deprovisioned. What should the customer do?

- A. Use the Cloud SDK with their directory service to remove their IAM permissions in Cloud Identity.
- B. Use the Cloud SDK with their directory service to provision and deprovision users from Cloud Identity.
- C. Configure Cloud Directory Sync with their directory service to provision and deprovision users from Cloud Identity.
- D. Configure Cloud Directory Sync with their directory service to remove their IAM permissions in Cloud Identity.

🗨️ 👤 **DebasishLowes** 10 months, 1 week ago

Ans is C

upvoted 1 times

🗨️ 👤 **[Removed]** 1 year, 2 months ago

Ans - C

upvoted 4 times

🗨️ 👤 **MohitA** 1 year, 4 months ago

C is the Answer

upvoted 4 times

🗨️ 👤 **ownez** 1 year, 4 months ago

Agree with C.

"https://cloud.google.com/identity/solutions/automate-user-provisioning#cloud_identity_automated_provisioning"

"Cloud Identity has a catalog of automated provisioning connectors, which act as a bridge between Cloud Identity and third-party cloud apps."

upvoted 7 times

An organization is evaluating the use of Google Cloud Platform (GCP) for certain IT workloads. A well-established directory service is used to manage user identities and lifecycle management. This directory service must continue for the organization to use as the "source of truth" directory for identities.

Which solution meets the organization's requirements?

- A. Google Cloud Directory Sync (GCDS)
- B. Cloud Identity
- C. Security Assertion Markup Language (SAML)
- D. Pub/Sub

🗲️ 👤 **subhala** Highly Voted 👍 1 year, 1 month ago

GCDS -? It helps sync up from the source of truth (any IdP like ldap, AD) to Google identity. In this scenario, the question is what can be a good identity service by itself, hence B is the right answer.

upvoted 9 times

🗲️ 👤 **mikelabs** Highly Voted 👍 1 year, 1 month ago

GCDS is an app to sync users, groups and other features from AD to Cloud Identity. But, in this question, the customer needs to know what's the product on GCP that meet with this. So, I think the answer is B.

upvoted 7 times

🗲️ 👤 **Bill831231** Most Recent 🕒 1 month ago

seems there is nothing metioned about what they have on premise, so B is better

upvoted 1 times

🗲️ 👤 **syllox** 8 months, 2 weeks ago

Answer A

upvoted 3 times

🗲️ 👤 **WakandaF** 8 months, 3 weeks ago

A or B?

upvoted 2 times

🗲️ 👤 **desertlotus1211** 10 months ago

The answer is A:

With Google Cloud Directory Sync (GCDS), you can synchronize the data in your Google Account with your Microsoft Active Directory or LDAP server. GCDS doesn't migrate any content (such as email messages, calendar events, or files) to your Google Account. You use GCDS to synchronize your Google users, groups, and shared contacts to match the information in your LDAP server.

The questions says the well established directory service is the 'source of truth' not GCP... So LDAP or AD is the source... GCDS will sync that to match those, not replace them...

upvoted 5 times

🗲️ 👤 **DebasishLowes** 10 months, 1 week ago

Ans : B as per the question.

upvoted 1 times

🗲️ 👤 **asee** 10 months, 3 weeks ago

My Answer will go for A (GCDS), noticed the question is mentioning about "A directory service 'is used' " / "must continue" instead of "A directory service 'will be used' ". So here my understanding is the organization has already using their own directory service. Therefore Answer B - Cloud identity may not be an option.

upvoted 3 times

🗲️ 👤 **KWatHK** 12 months ago

Ans is B because the questions said "the well-established directory must continue for the organization to use as the source of truth" so that the user access to GCP must authenticated by the existing directory. Cloud Identity support to federate it to 3rd party/ADFS using SAML.

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - A

upvoted 2 times



🗲️ 👤 **ownez** 1 year, 4 months ago



GCDS is a part of CI's feature that synchronizes the data in Google domain to match with AD/LDAP server. This includes users, groups contacts etc are synchronized/migrated to match.



Hence, I would go B.



"<https://se-cloud-experts.com/wp/wp-content/themes/se-it/images/pdf/google-cloud-identity-services.pdf>"



upvoted 3 times

  **ownez** 1 year, 4 months ago
Sorry. It's A.
upvoted 2 times

  **bogdant** 1 year, 4 months ago
Isn't it A?
upvoted 2 times

  **MohitA** 1 year, 4 months ago
Agree A
upvoted 3 times

  **Sheeda** 1 year, 4 months ago
That is used to sync, not the directly itself
upvoted 1 times



  **Fellipo** 1 year, 2 months ago
A well-established directory service , so "A"
upvoted 2 times



Question #59



Topic 1



Which international compliance standard provides guidelines for information security controls applicable to the provision and use of cloud services?

- A. ISO 27001
- B. ISO 27002
- C. ISO 27017
- D. ISO 27018

  **asee** 10 months, 3 weeks ago
Yes, My answer also goes to C and my last compliance related project is also working on ISO27017 in order to extend the scope to Cloud service user/provider.
upvoted 3 times

  **[Removed]** 1 year, 2 months ago
Ans - C
upvoted 2 times

  **Namaste** 1 year, 3 months ago
CCSP Question...C is the Answer
upvoted 2 times

  **ownez** 1 year, 4 months ago
C is correct.

"<https://www.iso.org/standard/43757.html>"
upvoted 3 times

You will create a new Service Account that should be able to list the Compute Engine instances in the project. You want to follow Google-recommended practices.

What should you do?

- A. Create an Instance Template, and allow the Service Account Read Only access for the Compute Engine Access Scope.
- B. Create a custom role with the permission compute.instances.list and grant the Service Account this role.
- C. Give the Service Account the role of Compute Viewer, and use the new Service Account for all instances.
- D. Give the Service Account the role of Project Viewer, and use the new Service Account for all instances.

🗲️ 👤 **MohitaA** Highly Voted 👍 1 year, 4 months ago
B, <https://cloud.google.com/compute/docs/access/iam>
upvoted 9 times

🗲️ 👤 **mlyu** 1 year, 4 months ago
Although it is not encourage to use custome role, but last sentence in the answer C makes B be the only option
upvoted 2 times

🗲️ 👤 **[Removed]** Most Recent ⌚ 9 months ago
I think C is good
upvoted 3 times

🗲️ 👤 **DebasishLowes** 9 months, 3 weeks ago
Ans : B
upvoted 1 times

🗲️ 👤 **dtmtor** 10 months ago
Ans is B
upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago
Ans - B
upvoted 1 times

🗲️ 👤 **genesis3k** 1 year, 2 months ago
Answer is B, based on least privilege principle.
upvoted 1 times

An organization is starting to move its infrastructure from its on-premises environment to Google Cloud Platform (GCP). The first step the organization wants to take is to migrate its ongoing data backup and disaster recovery solutions to GCP. The organization's on-premises production environment is going to be the next phase for migration to GCP. Stable networking connectivity between the on-premises environment and GCP is also being implemented.

Which GCP solution should the organization use?

- A. BigQuery using a data pipeline job with continuous updates via Cloud VPN
- B. Cloud Storage using a scheduled task and gsutil via Cloud Interconnect
- C. Compute Engines Virtual Machines using Persistent Disk via Cloud Interconnect
- D. Cloud Datastore using regularly scheduled batch upload jobs via Cloud VPN

🗨️  **rr4444** 2 weeks ago

Selected Answer: C

Disaster recover made me think C Compute Engines Virtual Machines using Persistent Disk via Cloud Interconnect

Disaster recovery with remote backup alone, when all prod is on premise, will take too long to be viable. The VMs don't need to be running when no disaster

upvoted 2 times

🗨️  **DebasishLowes** 9 months, 3 weeks ago

Ans : B

upvoted 2 times

🗨️  **[Removed]** 1 year, 2 months ago


Ans - V

upvoted 1 times

🗨️  **[Removed]** 1 year, 2 months ago

Typo - it's B

upvoted 2 times

🗨️  **ownez** 1 year, 4 months ago

Agree B.

https://cloud.google.com/solutions/dr-scenarios-for-data#production_environment_is_on-premises

upvoted 2 times

A customer wants to make it convenient for their mobile workforce to access a CRM web interface that is hosted on Google Cloud Platform (GCP). The CRM can only be accessed by someone on the corporate network. The customer wants to make it available over the internet. Your team requires an authentication layer in front of the application that supports two-factor authentication. Which GCP product should the customer implement to meet these requirements?

- A. Cloud Identity-Aware Proxy
- B. Cloud Armor
- C. Cloud Endpoints
- D. Cloud VPN

🗲️ 👤 **asee** Highly Voted 👍 10 months, 3 weeks ago

My answer is going for A.
Cloud IAP is integrated with Google Sign-in which Multi-factor authentication can be enabled.
<https://cloud.google.com/iap/docs/concepts-overview>
upvoted 9 times

🗲️ 👤 **Mohita** Highly Voted 👍 1 year, 4 months ago

A is the Answer
upvoted 5 times

🗲️ 👤 **[Removed]** Most Recent ⌚ 1 year, 2 months ago

Ans - A
upvoted 3 times

🗲️ 👤 **passtest100** 1 year, 3 months ago

SHOULD BE A
upvoted 4 times

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

Answer -A
upvoted 3 times

Your company is storing sensitive data in Cloud Storage. You want a key generated on-premises to be used in the encryption process. What should you do?

- A. Use the Cloud Key Management Service to manage a data encryption key (DEK).
- B. Use the Cloud Key Management Service to manage a key encryption key (KEK).
- C. Use customer-supplied encryption keys to manage the data encryption key (DEK).
- D. Use customer-supplied encryption keys to manage the key encryption key (KEK).

  **HateMicrosoft** Highly Voted 10 months, 1 week ago

The answer is: C

This is a Customer-supplied encryption keys (CSEK).

We generate our own encryption key and manage it on-premises.

A KEK never leaves Cloud KMS. There is no KEK or KMS on-premises.

Encryption at rest by default, with various key management options

<https://cloud.google.com/security/encryption-at-rest>

upvoted 7 times

  **Bill831231** Most Recent 1 month ago

sounds D is the correct one.

The raw CSEK is combined with a per-persistent disk cryptographic nonce to generate a CSEK-derived key. This key is used as the key encryption key in Google Compute Engine for your data.

https://cloud.google.com/security/encryption/customer-supplied-encryption-keys#compute_engine

upvoted 1 times

  **rr4444** 2 weeks ago

Nope cos being used as the KEK means that this CSEK KEK is used to MANAGE the DEK

upvoted 1 times

  **Bwitch** 1 month, 1 week ago

Selected Answer: C

"on-premise" has to be a customer-supplied key. Everything else is from the GCP platform.

upvoted 2 times

  **major_querty** 1 month, 3 weeks ago

The answer is C

The question says: "you want to use a key generated on-premise", so A and B must be wrong.

Between DEK and KEK, the documentation says the following:

The process of encrypting data is to generate a DEK locally, encrypt data with the DEK, use a KEK to wrap the DEK, and then store the encrypted data and the wrapped DEK. The KEK never leaves Cloud KMS.

Thus, it must be C.

https://cloud.google.com/kms/docs/envelope-encryption#how_to_encrypt_data_using_envelope_encryption

upvoted 2 times

  **idtroo** 9 months, 2 weeks ago

Ans: D

https://cloud.google.com/kms/docs/envelope-encryption#other_options

"With CSEK, you supply your own AES-256 key to serve as the KEK, and your key protects the DEKs that protect your data. Your CSEK key is protected by an additional layer of protection, using a Cloud KMS key."

upvoted 2 times

  **rr4444** 2 weeks ago

Nope cos being used as the KEK means that this CSEK KEK is used to MANAGE the DEK

upvoted 1 times

  **iamoct** 9 months, 4 weeks ago

The important message is "to manage"

So, CSEK used to manage DEK

upvoted 3 times

  **rr4444** 2 weeks ago

Exactly

upvoted 1 times

  **CloudTrip** 10 months, 3 weeks ago

You provide a raw CSEK as part of an API call. This key is transmitted from the Google front end to the storage system's memory. This key is used as the key encryption key in Google Cloud Storage for your data.

The raw CSEK is used to unwrap wrapped chunk keys, to create raw chunk keys in memory. These are used to decrypt data chunks stored in the storage systems. These keys are used as the data encryption keys (DEK) in Google Cloud Storage for your data.

As the question mentions about Cloud Storage so may be Answer will be C


upvoted 2 times

  **TNT87** 11 months, 1 week ago

A

<https://cloud.google.com/security/encryption-at-rest/customer-supplied-encryption-keys>

upvoted 2 times

  **TNT87** 10 months, 3 weeks ago

Ans C <https://cloud.google.com/security/encryption-at-rest>

upvoted 3 times

  **hector2050** 11 months, 1 week ago

C : CSEK is the KEK.

upvoted 1 times

  **iptorrent786** 11 months, 3 weeks ago

Answer: C

<https://cloud.google.com/security/encryption-at-rest/customer-supplied-encryption-keys>

upvoted 4 times

  **deardeer** 11 months, 4 weeks ago

Answer is D. A key generated on-premises is CSEK. And here is a graph to compare use CSEK in Cloud Storage.

https://cloud.google.com/security/encryption-at-rest/customer-supplied-encryption-keys#cloud_storage

upvoted 2 times

  **deardeer** 11 months ago

not D, its C. I recheck it again, and I realized I was wrong.

upvoted 2 times

  **singhjoga** 1 year ago

C - CSEK is KEK -> used to unwrap/create(manage) DEK.

See below at <https://cloud.google.com/security/encryption-at-rest/customer-supplied-encryption-keys>

You provide a raw CSEK as part of an API call. This key is used as the key encryption key in Google Cloud Storage for your data.

The raw CSEK is used to unwrap wrapped chunk keys, to create raw chunk keys in memory. These keys are used as the data encryption keys (DEK) in Google Cloud Storage for your data.

upvoted 2 times

  **Rodine** 12 months ago


You use KEK to wrap and unwrap DEK. DEK is located centrally so when you import it from onpremise it cant act as DEK... so in this case CSEK act as KEK.

upvoted 1 times

  **Topsy** 1 year ago

D- <https://cloud.google.com/security/encryption-at-rest/customer-supplied-encryption-keys>

upvoted 2 times

  **mondigo** 1 year, 1 month ago

C


<https://cloud.google.com/security/encryption-at-rest/customer-supplied-encryption-keys>

upvoted 1 times

  **mondigo** 1 year ago

should be D

upvoted 2 times

  **VivekA** 1 year, 1 month ago

Ans: A

Cloud Storage doesn't support CSEK hence option D is eliminated.

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

upvoted 1 times

  **[Removed]** 1 year, 2 months ago

Ans - A

upvoted 1 times

  **[Removed]** 1 year, 2 months ago

Sry.. D

upvoted 1 times

  **genesis3k** 1 year, 2 months ago

Answer is D.

"With CSEK, you supply your own AES-256 key to serve as the KEK, and your key protects the DEKs that protect your data. Your CSEK key is protected by an additional layer of protection, using a Cloud KMS key."

https://cloud.google.com/kms/docs/envelope-encryption#other_options

upvoted 2 times

Last week, a company deployed a new App Engine application that writes logs to BigQuery. No other workloads are running in the project. You need to validate that all data written to BigQuery was done using the App Engine Default Service Account. What should you do?

- A. 1. Use StackDriver Logging and filter on BigQuery Insert Jobs. 2. Click on the email address in line with the App Engine Default Service Account in the authentication field. 3. Click Hide Matching Entries. 4. Make sure the resulting list is empty.
- B. 1. Use StackDriver Logging and filter on BigQuery Insert Jobs. 2. Click on the email address in line with the App Engine Default Service Account in the authentication field. 3. Click Show Matching Entries. 4. Make sure the resulting list is empty.
- C. 1. In BigQuery, select the related dataset. 2. Make sure the App Engine Default Service Account is the only account that can write to the dataset.
- D. 1. Go to the IAM section on the project. 2. Validate that the App Engine Default Service Account is the only account that has a role that can write to BigQuery.

🗲️ 👤 **Moe666** Highly Voted 👍 1 year, 1 month ago

the answer is A. They are asking you to validate and not to prevent, hence why C and D are wrong.
upvoted 12 times

🗲️ 👤 **[Removed]** Most Recent ⌚ 9 months ago

I agree with A ,if C and D can not show the past information.
upvoted 2 times

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

Ans : A
upvoted 2 times

🗲️ 👤 **HateMicrosoft** 10 months, 1 week ago

The answer is:A
This one is tricky because we must read the question several times.We need to validate all data written to BigQuery was done by the App Engine Default Service Account, since last week (or probably longer).
Facts:
-Having no workloads running in the project means nothing.
-We could have had a service account writing to BigQuery for a couple of hours and then deleted this service account.

So, the answer A is the only choice.
upvoted 3 times

🗲️ 👤 **HateMicrosoft** 10 months, 1 week ago

The answer is:A
This one is tricky because we must read the question several times.We need to validate all data written to BigQuery was done by the App Engine Default Service Account, since last week (or probably longer).Facts:
-Having no workloads running in the project means nothing.-We could have had a service account writing to BigQuery for a couple of hours and then deleted this service account.

So, the answer A is the only choice.
upvoted 1 times

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

mlx is right. Option B only shows current status. There's nothing to validate another account didn't insert data & then get removed from the dataset access.

Effectively, the answer is to run this query in SD Logs Explorer:

```
resource.type="bigquery_project"
-protoPayload.authenticationInfo.principalEmail="emailAccount"
protoPayload.methodName="google.cloud.bigquery.v2.JobService.InsertJob"
```

upvoted 2 times

🗲️ 👤 **mlx** 1 year, 2 months ago

ans A : B will exclude accesses from other accounts, C and D cannot check past results.
upvoted 4 times



🗲️ 👤 **[Removed]** 1 year, 2 months ago



IMO, Ans - D
upvoted 3 times



🗲️ 👤 **genesis3k** 1 year, 2 months ago



Answer is C.
<https://cloud.google.com/bigquery/docs/dataset-access-controls#dataset-acl>

upvoted 1 times

  **saurabh1805** 1 year, 2 months ago
shouldn't D be correct option here ?
upvoted 1 times

  **passtest100** 1 year, 3 months ago
Choose B.
upvoted 1 times

  **Namaste** 1 year, 3 months ago
A is the answer
upvoted 1 times




  **Namaste** 1 year, 3 months ago
Sorry C is correct
upvoted 1 times




Question #65



Topic 1



Your team wants to limit users with administrative privileges at the organization level.
Which two roles should your team restrict? (Choose two.)



- A. Organization Administrator
- B. Super Admin
- C. GKE Cluster Admin
- D. Compute Admin
- E. Organization Role Viewer

  **HateMicrosoft** Highly Voted  10 months, 1 week ago
The correct anwser is : A&B
-resourcemanager.organizationAdmin
-Cloud Identity super admin(Old G-Suite Google Workspace)
upvoted 8 times

  **Bingo21** Most Recent  10 months, 3 weeks ago
It says "limit users with administrative privileges" - D doesnt give you admin privileges. AB is the closest to what the question is looking for.
upvoted 3 times

  **[Removed]** 1 year, 2 months ago
Ans - AB
upvoted 2 times

  **Mohita** 1 year, 4 months ago
AB are the one
upvoted 4 times

  **singhjoga** 1 year ago
There is no such role as "Super Admin". There is a Super Admin user. which has the "Owner" role to the how Organisation.
Answer is probably A and D.
upvoted 2 times

An organization's security and risk management teams are concerned about where their responsibility lies for certain production workloads they are running in

Google Cloud Platform (GCP), and where Google's responsibility lies. They are mostly running workloads using Google Cloud's Platform-as-a-Service (PaaS) offerings, including App Engine primarily.

Which one of these areas in the technology stack would they need to focus on as their primary responsibility when using App Engine?

- A. Configuring and monitoring VPC Flow Logs
- B. Defending against XSS and SQLi attacks
- C. Manage the latest updates and security patches for the Guest OS
- D. Encrypting all stored data

🗲️ 👤 **[Removed]** Highly Voted 👍 9 months ago

Why not B? that is application layer work, must be done by customer.
upvoted 5 times

🗲️ 👤 **Arad** Most Recent ⌚ 1 month, 3 weeks ago

Correct answer is B.
Look at the diagram here: <https://cloud.google.com/blog/products/containers-kubernetes/exploring-container-security-the-shared-responsibility-model-in-gke-container-security-shared-responsibility-model-gke>
upvoted 2 times

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

Ans : B
upvoted 4 times

🗲️ 👤 **soukumar369** 1 year ago

Answer is B bcz in SaaS customer is responsible for "Defending against XSS and SQLi attacks"
upvoted 3 times

🗲️ 👤 **soukumar369** 1 year ago

In PaaS*
upvoted 2 times

🗲️ 👤 **ronron89** 1 year, 1 month ago

Since its a PAAS answer is B.
upvoted 4 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - B
upvoted 2 times

🗲️ 👤 **genesis3k** 1 year, 2 months ago

Answer is B, because App Engine doesn't automatically protects from XSS and SQLi attacks for App Engine application.
upvoted 4 times

🗲️ 👤 **saaurabh1805** 1 year, 2 months ago

B is incorrect answer, that is managed by google at default on appspot urls. i will go with option D
upvoted 1 times

🗲️ 👤 **rr4444** 2 weeks ago

Nope, they need detection e.g. by Web Security Scanner, and then resolution in the app code
upvoted 1 times

🗲️ 👤 **passtest100** 1 year, 3 months ago

should be D
upvoted 1 times

🗲️ 👤 **rr4444** 2 weeks ago

Nope, they need detection e.g. by Web Security Scanner, and then resolution in the app code
upvoted 1 times

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

Answer-B
upvoted 2 times

🗲️ 👤 **Mohita** 1 year, 4 months ago

B is the Ans
upvoted 2 times

A customer is running an analytics workload on Google Cloud Platform (GCP) where Compute Engine instances are accessing data stored on Cloud Storage.

Your team wants to make sure that this workload will not be able to access, or be accessed from, the internet.

Which two strategies should your team use to meet these requirements? (Choose two.)

- A. Configure Private Google Access on the Compute Engine subnet
- B. Avoid assigning public IP addresses to the Compute Engine cluster.
- C. Make sure that the Compute Engine cluster is running on a separate subnet.
- D. Turn off IP forwarding on the Compute Engine instances in the cluster.
- E. Configure a Cloud NAT gateway.

🗲️ 👤 **MohitA** Highly Voted 👍 1 year, 4 months ago

AB suits well
upvoted 15 times

🗲️ 👤 **DebasishLowes** Highly Voted 👍 9 months, 3 weeks ago

Ans : AB
upvoted 5 times

🗲️ 👤 **pfilourenco** Most Recent 🕒 8 months ago

B and E:
"make sure that this workload will not be able to access, or be accessed from, the internet."
If we have cloud NAT we are able to access the internet! Also with public IP.
upvoted 1 times

🗲️ 👤 **[Removed]** 9 months ago

Not A <https://cloud.google.com/vpc/docs/private-google-access>
upvoted 1 times

🗲️ 👤 **tanfromvn** 6 months, 2 weeks ago

A_B, why not A? Private access just accepts traffic in GCP and to GG API
upvoted 2 times

🗲️ 👤 **[Removed]** 9 months ago

NOt D, because by de fault IP forwarding is disabled. You do not need to turn it off.
upvoted 1 times

🗲️ 👤 **[Removed]** 9 months ago

So B and E is the right answer.
upvoted 2 times

🗲️ 👤 **ffdd1234** 11 months, 3 weeks ago

if you Avoid assigning public IP addresses to the Compute Engine cluster the instance could access to internet if have a nat gateway, maybe the answer is A and D
upvoted 1 times

🗲️ 👤 **ffdd1234** 2 months, 1 week ago

+1 A-D
upvoted 1 times

🗲️ 👤 **ffdd1234** 2 months, 1 week ago

But not sure "Ensure that IP Forwarding feature is not enabled at the Google Compute Engine instance level for security and compliance reasons, as instances with IP Forwarding enabled act as routers/packet forwarders."
IP FW is for route packets could not be D
upvoted 1 times

🗲️ 👤 **Topsy** 1 year ago

A and B is correct
upvoted 3 times



🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - AB
upvoted 2 times

🗲️ 👤 **genesis3k** 1 year, 2 months ago



AB is the correct answer.

upvoted 1 times

  **Wooky** 1 year, 3 months ago

B,D not A
Private google access provides public google api access without public IP

upvoted 1 times

  **Wooky** 1 year, 3 months ago

My mistake, ans is AB.

upvoted 2 times

  **Raushanr** 1 year, 3 months ago

Answer-AB
upvoted 2 times

A customer wants to run a batch processing system on VMs and store the output files in a Cloud Storage bucket. The networking and security teams have decided that no VMs may reach the public internet.
How should this be accomplished?

- A. Create a firewall rule to block internet traffic from the VM.
- B. Provision a NAT Gateway to access the Cloud Storage API endpoint.
- C. Enable Private Google Access on the VPC.
- D. Mount a Cloud Storage bucket as a local filesystem on every VM.

🗲️ 👤 **tanfromvn** Highly Voted 👍 6 months, 2 weeks ago

C-there is no traffic to outside internet
upvoted 6 times

🗲️ 👤 **ZODOGAM** Most Recent 🕒 1 month ago

100% A. Question is 'The networking and security teams have decided that no VMs may reach the public internet.' the ask is to deny VMs from reaching the public internet. I'd go with A ... the rest of the connection (to GCS bucket) causing the confusion.
upvoted 2 times

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

C is wired, because google private access is on subnet level...
D is not a recommended way but it should work...
If I have this in exam, I will go D...
upvoted 3 times

🗲️ 👤 **ThisisJohn** 1 month ago

But keep in mind D will not prevent your VMs from accessing any Internet site
upvoted 1 times

🗲️ 👤 **sleekdunga** 8 months, 3 weeks ago

Quite tricky because you can only enable Google private access via the subnet config and not VPC. But the keyword also says can't traverse the internet which makes C only option with skepticism.
upvoted 1 times

🗲️ 👤 **[Removed]** 9 months ago

private google access allow VMs to connect to internet API without a public IP.
upvoted 1 times

🗲️ 👤 **[Removed]** 9 months, 3 weeks ago

C is the Answer. Since Networking team has already decid(ed) ,I will go with C ,as this is the option stating solution which will enable customer to get its work done.
upvoted 2 times

🗲️ 👤 **ThisisJohn** 1 month ago

Keep in mind C will not prevent your VMs from accessing any Internet site, as by default outbound access is allowed.
upvoted 1 times

🗲️ 👤 **Bingo21** 10 months, 3 weeks ago

Question is 'The networking and security teams have decided that no VMs may reach the public internet.' the ask is to deny VMs from reaching the public internet. I'd go with A ... the rest of the connection (to GCS bucket) causing the confusion.
upvoted 3 times

🗲️ 👤 **gu9singg** 9 months, 3 weeks ago

A: is incorrect
upvoted 1 times

🗲️ 👤 **gu9singg** 9 months, 3 weeks ago

we need to reduce operations work and use google best practice
upvoted 1 times

🗲️ 👤 **CloudTrip** 11 months ago

Here C could be a viable solution but answer B (NAT Gateway) looks more precise as you are intending to connect to a precise target destination than a wider VPC and it will also ensure that the VM traffic is not going to external internet. Refer more details on NAT Gateway here : <https://cloud.google.com/nat/docs/overview>
upvoted 2 times

🗲️ 👤 **cuban123** 1 year ago

Why not consider option A? Deny all traffic from VM to internet. Have connectivity to Cloud storage still available. Satisfies the conditions in question.

upvoted 2 times

🗨️ 👤 **Topsy** 1 year ago

Answer is C- Since Network and Security Team has decided to disable internet access, the only option left is the Google Private Access option

upvoted 3 times

🗨️ 👤 **ThisisJohn** 1 month ago

Keep in mind C will not prevent your VMs from accessing any Internet site, as by default outbound access is allowed.

upvoted 1 times

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

Answer should be C because private google access on the VPC means private google access on the VPC subnets only.

upvoted 2 times

🗨️ 👤 **subhala** 1 year, 1 month ago

Is B a possible solution? can we provision a NAT gateway to access the cloud storage API endpoint?

upvoted 2 times

🗨️ 👤 **iloveme** 1 year, 1 month ago

While initially I believed that it is C , as I did not process the "on the VPC" , the correct answer is D (not necessary the best option I would say , but excluding all others. That is because the Private Google Access is enabled at the SUBNET level , not on the VPC (<https://cloud.google.com/vpc/docs/configure-private-google-access#specifications>)

upvoted 1 times

🗨️ 👤 **iloveme** 1 year, 1 month ago

Now that I think about it , C and D are both incomplete. For C it should say "on all subnets of the VPC / on the subnet level" , and for D it should mention that Private Google Access is enabled . If I get this question on the exam , I will see then and there what I will answer :D

upvoted 1 times

🗨️ 👤 **sharp20** 1 year, 2 months ago

Should be C

By default, when a Compute Engine VM lacks an external IP address assigned to its network interface, it can only send packets to other internal IP address destinations. You can allow these VMs to connect to the set of external IP addresses used by Google APIs and services by enabling Private Google Access on the subnet used by the VM's network interface.

upvoted 2 times

🗨️ 👤 **[Removed]** 1 year, 2 months ago

Ans - C

upvoted 2 times

🗨️ 👤 **zee001** 1 year, 3 months ago

what about option D?

Google cloud states that the below:

Mounting a bucket as a file system

You can use the Cloud Storage FUSE tool to mount a Cloud Storage bucket to your Compute Engine instance. The mounted bucket behaves similarly to a persistent disk even though Cloud Storage buckets are object storage.

upvoted 1 times

🗨️ 👤 **HectorLeon2099** 1 year, 3 months ago

Google never recommends to use FUSE in a Productive Environment.

upvoted 1 times

🗨️ 👤 **Namaste** 1 year, 3 months ago

Answer C

upvoted 3 times

As adoption of the Cloud Data Loss Prevention (DLP) API grows within the company, you need to optimize usage to reduce cost. DLP target data is stored in Cloud Storage and BigQuery. The location and region are identified as a suffix in the resource name. Which cost reduction options should you recommend?

- A. Set appropriate rowsLimit value on BigQuery data hosted outside the US and set appropriate bytesLimitPerFile value on multiregional Cloud Storage buckets.
- B. Set appropriate rowsLimit value on BigQuery data hosted outside the US, and minimize transformation units on multiregional Cloud Storage buckets.
- C. Use rowsLimit and bytesLimitPerFile to sample data and use CloudStorageRegexFileSet to limit scans.
- D. Use FindingLimits and TimespanConfig to sample data and minimize transformation units.

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - C

<https://cloud.google.com/dlp/docs/inspecting-storage#sampling>

https://cloud.google.com/dlp/docs/best-practices-costs#limit_scans_of_files_in_to_only_relevant_files

upvoted 4 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

<https://cloud.google.com/dlp/docs/inspecting-storage#limiting-gcs>

upvoted 1 times

🗲️ 👤 **passtest100** 1 year, 3 months ago

C is the right one.

upvoted 2 times

Your team uses a service account to authenticate data transfers from a given Compute Engine virtual machine instance of to a specified Cloud Storage bucket. An engineer accidentally deletes the service account, which breaks application functionality. You want to recover the application as quickly as possible without compromising security. What should you do?

- A. Temporarily disable authentication on the Cloud Storage bucket.
- B. Use the undelete command to recover the deleted service account.
- C. Create a new service account with the same name as the deleted service account.
- D. Update the permissions of another existing service account and supply those credentials to the applications.

🗲️ 👤 **DebasishLowes** 10 months, 1 week ago

Ans : B

upvoted 3 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - B

upvoted 2 times

🗲️ 👤 **saaurabh1805** 1 year, 2 months ago

B is correct answer here.

<https://cloud.google.com/iam/docs/reference/rest/v1/projects.serviceAccounts/undelete>

upvoted 2 times

🗲️ 👤 **MohitA** 1 year, 4 months ago

B is the Answer

upvoted 2 times

You are the Security Admin in your company. You want to synchronize all security groups that have an email address from your LDAP directory in Cloud IAM.

What should you do?

- A. Configure Google Cloud Directory Sync to sync security groups using LDAP search rules that have "user email address" as the attribute to facilitate one-way sync.
- B. Configure Google Cloud Directory Sync to sync security groups using LDAP search rules that have "user email address" as the attribute to facilitate bidirectional sync.
- C. Use a management tool to sync the subset based on the email address attribute. Create a group in the Google domain. A group created in a Google domain will automatically have an explicit Google Cloud Identity and Access Management (IAM) role.
- D. Use a management tool to sync the subset based on group object class attribute. Create a group in the Google domain. A group created in a Google domain will automatically have an explicit Google Cloud Identity and Access Management (IAM) role.

🗲️ 👤 **[Removed]** 9 months ago

Why A is not correct? GCP provide this sync tool.
upvoted 2 times

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

Incorrect. GCDS is Google Workspace Admin tool.

Correct answer is A. GCDS only syncs one way - <https://support.google.com/a/answer/106368?hl=en>
upvoted 1 times

🗲️ 👤 **DebasishLowes** 10 months, 1 week ago

Ans : A
upvoted 2 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - A
upvoted 2 times

🗲️ 👤 **saurabh1805** 1 year, 2 months ago

A is correct answer here.
upvoted 2 times

🗲️ 👤 **passtest100** 1 year, 3 months ago

Answer - A
upvoted 2 times

🗲️ 👤 **skshak** 1 year, 3 months ago

Answer - A
upvoted 2 times

You are part of a security team investigating a compromised service account key. You need to audit which new resources were created by the service account.

What should you do?

- A. Query Data Access logs.
- B. Query Admin Activity logs.
- C. Query Access Transparency logs.
- D. Query Stackdriver Monitoring Workspace.

🗲️ 👤 **MohitA** Highly Voted 👍 1 year, 4 months ago

B is the Ans

upvoted 5 times

🗲️ 👤 **Fellipo** 1 year, 2 months ago

B it's OK

upvoted 3 times

🗲️ 👤 **ownez** 1 year, 4 months ago

Shouldn't it be A? The question is about which resources were created by the SA.

B (Admin Activity logs) cannot view this. It is only for user's activity such as create, modify or delete a particular SA.

upvoted 1 times

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

"Admin Activity audit logs contain log entries for API calls or other administrative actions that modify the configuration or metadata of resources. For example, these logs record when users create VM instances or change Identity and Access Management permissions".

This is exactly what you want to see. What resources were created by the SA?

<https://cloud.google.com/logging/docs/audit#admin-activity>

upvoted 3 times

🗲️ 👤 **VicF** Most Recent ⌚ 8 months, 3 weeks ago

Ans B

"B" is for actions that modify the configuration or metadata of resources. For example, these logs record when users create VM instances or change Identity and Access Management permissions.

"A" is only for "user-provided" resource data. Data Access audit logs-- except for BigQuery Data Access audit logs-- "are disabled by default"

upvoted 4 times

🗲️ 👤 **[Removed]** 9 months ago

I support B, <https://cloud.google.com/iam/docs/audit-logging>

says IAM logs write into admin log

upvoted 4 times

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

Ans : B

upvoted 3 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - B

upvoted 4 times

You have an application where the frontend is deployed on a managed instance group in subnet A and the data layer is stored on a mysql Compute Engine virtual machine (VM) in subnet B on the same VPC. Subnet A and Subnet B hold several other Compute Engine VMs. You only want to allow the application frontend to access the data in the application's mysql instance on port 3306.

What should you do?

- A. Configure an ingress firewall rule that allows communication from the src IP range of subnet A to the tag "data-tag" that is applied to the mysql Compute Engine VM on port 3306.
- B. Configure an ingress firewall rule that allows communication from the frontend's unique service account to the unique service account of the mysql Compute Engine VM on port 3306.
- C. Configure a network tag "fe-tag" to be applied to all instances in subnet A and a network tag "data-tag" to be applied to all instances in subnet B. Then configure an egress firewall rule that allows communication from Compute Engine VMs tagged with data-tag to destination Compute Engine VMs tagged fe- tag.
- D. Configure a network tag "fe-tag" to be applied to all instances in subnet A and a network tag "data-tag" to be applied to all instances in subnet B. Then configure an ingress firewall rule that allows communication from Compute Engine VMs tagged with fe-tag to destination Compute Engine VMs tagged with data-tag.

🗨️ **major_querty** 1 month, 3 weeks ago

why is it not a?
a seems straight forward

The link which Zuy01 provided for answer b states: For this reason, using a service account is the recommended method for production instances NOT running on a Compute Engine instance.

upvoted 1 times

🗨️ **Zuy01** 5 months ago

B for sure, u can check this :
<https://cloud.google.com/sql/docs/mysql/sql-proxy#using-a-service-account>

upvoted 2 times

🗨️ **DebasishLowes** 9 months, 3 weeks ago

Ans : B
upvoted 2 times

🗨️ **dtmtor** 10 months ago

ans is B
upvoted 2 times

🗨️ **[Removed]** 1 year, 2 months ago

Ans - B
upvoted 4 times

🗨️ **Rantu** 1 year, 3 months ago

B is correct
upvoted 4 times

You are the security admin of your company. You have 3,000 objects in your Cloud Storage bucket. You do not want to manage access to each object individually.

You also do not want the uploader of an object to always have full control of the object. However, you want to use Cloud Audit Logs to manage access to your bucket.

What should you do?

- A. Set up an ACL with OWNER permission to a scope of allUsers.
- B. Set up an ACL with READER permission to a scope of allUsers.
- C. Set up a default bucket ACL and manage access for users using IAM.
- D. Set up Uniform bucket-level access on the Cloud Storage bucket and manage access for users using IAM.

🗨️ 👤 **Fellipo** Highly Voted 👍 1 year, 2 months ago

it's D, <https://cloud.google.com/storage/docs/uniform-bucket-level-access#:~:text=When%20you%20enable%20uniform%20bucket,and%20the%20objects%20it%20contains>.
upvoted 11 times

🗨️ 👤 **ramravella** Most Recent 🕒 6 months, 1 week ago

Answer is A. Read the note below in the below URL

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

Note: You cannot grant discrete permissions for reading or writing ACLs or other metadata. To allow someone to read and write ACLs, you must grant them OWNER permission.

upvoted 1 times

🗨️ 👤 **Zuy01** 5 months ago

the question mention "do not want the uploader of an object to always have full control of the object" that's mean you shouldn't grant the owner permission, hence the best ans is D.

upvoted 2 times

🗨️ 👤 **[Removed]** 9 months ago

A grants Owner???too much for this.

upvoted 2 times

🗨️ 👤 **[Removed]** 1 year, 2 months ago

Ans - D

upvoted 3 times

🗨️ 👤 **saurabh1805** 1 year, 2 months ago

I will go with uniform level access and manage access via IAM,

Hence D.

upvoted 2 times

🗨️ 👤 **passtest100** 1 year, 3 months ago

SHOULD BE D

upvoted 2 times

🗨️ 👤 **skshak** 1 year, 3 months ago

Answer C <https://cloud.google.com/storage/docs/access-control>

Uniform (recommended): Uniform bucket-level access allows you to use Identity and Access Management (IAM) alone to manage permissions. IAM applies permissions to all the objects contained inside the bucket or groups of objects with common name prefixes. IAM also allows you to use features that are not available when working with ACLs, such as IAM Conditions and Cloud Audit Logs.

upvoted 1 times

🗨️ 👤 **skshak** 1 year, 3 months ago

Sorry, It is D. It was typo.

upvoted 3 times

🗨️ 👤 **mlyu** 1 year, 3 months ago

the question stated they need cloud audit log for the GCS access, however uniform bucket-level access has restriction on the cloud audit log.

See <https://cloud.google.com/storage/docs/uniform-bucket-level-access>

The following restrictions apply when using uniform bucket-level access:

Cloud Logging and Cloud Audit Logs cannot export to buckets that have uniform bucket-level access enabled.

upvoted 1 times

  **FatCharlie** 1 year, 1 month ago

They're not saying they want to export the logs to the bucket. They're just saying they want to "use Cloud Audit Logs to manage access to your bucket" (whatever that means).

upvoted 1 times

You need to provide a corporate user account in Google Cloud for each of your developers and operational staff who need direct access to GCP resources.

Corporate policy requires you to maintain the user identity in a third-party identity management provider and leverage single sign-on. You learn that a significant number of users are using their corporate domain email addresses for personal Google accounts, and you need to follow Google recommended practices to convert existing unmanaged users to managed accounts.

Which two actions should you take? (Choose two.)

- A. Use Google Cloud Directory Sync to synchronize your local identity management system to Cloud Identity.
- B. Use the Google Admin console to view which managed users are using a personal account for their recovery email.
- C. Add users to your managed Google account and force users to change the email addresses associated with their personal accounts.
- D. Use the Transfer Tool for Unmanaged Users (TTUU) to find users with conflicting accounts and ask them to transfer their personal Google accounts.
- E. Send an email to all of your employees and ask those users with corporate email addresses for personal Google accounts to delete the personal accounts immediately.

  **VicF** Highly Voted 8 months, 3 weeks ago

A&D.

A- Requires third-party IDp and wants to leverage single sign-on.

D- https://cloud.google.com/architecture/identity/migrating-consumer-accounts#initiating_a_transfer

"In addition to showing you all unmanaged accounts, the transfer tool for unmanaged users lets you initiate an account transfer by sending an account transfer request."

upvoted 7 times

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

Is the answer is A,D

A - Requirement is third-party identity management provider and leverage single sign-on.

D - <https://cloud.google.com/architecture/identity/assessing-existing-user-accounts> (Use the transfer tool for unmanaged users to identify consumer accounts that use an email address that matches one of the domains you've added to Cloud Identity or G Suite.)

upvoted 5 times

  **CloudTrip** Most Recent 10 months, 3 weeks ago

The keyword is here "convert" follow Google recommended practices to convert existing unmanaged users to managed accounts. So why sync unmanaged with Cloud Identity. I would prefer Answers C and D

upvoted 2 times

  **ThisisJohn** 1 month ago

But dont forget about "Corporate policy requires you to maintain the user identity in a third-party identity management provider".

I believe that makes it A and D

upvoted 1 times

  **mikelabs** 1 year, 1 month ago

Answer is C,D. From GSuite Console you can do both.

upvoted 1 times

  **[Removed]** 1 year, 2 months ago


Ans - AD

upvoted 3 times

  **[Removed]** 1 year, 2 months ago



https://cloud.google.com/architecture/identity/migrating-consumer-accounts#initiating_a_transfer

upvoted 5 times

  **saaurabh1805** 1 year, 2 months ago

A, D is correct answer

upvoted 3 times

  **lordb** 1 year, 3 months ago

<https://cloud.google.com/architecture/identity/assessing-existing-user-accounts>

upvoted 2 times

A customer needs an alternative to storing their plain text secrets in their source-code management (SCM) system. How should the customer achieve this using Google Cloud Platform?

- A. Use Cloud Source Repositories, and store secrets in Cloud SQL.
- B. Encrypt the secrets with a Customer-Managed Encryption Key (CMEK), and store them in Cloud Storage.
- C. Run the Cloud Data Loss Prevention API to scan the secrets, and store them in Cloud SQL.
- D. Deploy the SCM to a Compute Engine VM with local SSDs, and enable preemptible VMs.

🗲️ 👤 **FatCharlie** Highly Voted 👍 1 year, 1 month ago

I guess this question was written prior to end of 2019, because Secret Manager is definitely the preferred solution nowadays.

B is best of some bad options.

upvoted 5 times

🗲️ 👤 **Raghucs** Most Recent ⌚ 1 month, 4 weeks ago

Selected Answer: B

B is the best answer.

upvoted 1 times

🗲️ 👤 **HateMicrosoft** 10 months, 1 week ago

Gosh, clearly this is a very old question. Secret Manager is the answer. No matter what choices are there.

upvoted 4 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - B

upvoted 3 times

🗲️ 👤 **saurabh1805** 1 year, 2 months ago

I would prefer secret manager but B is best possible option here.

upvoted 2 times

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

I agree with B

upvoted 2 times

🗲️ 👤 **KILLMAD** 1 year, 10 months ago

Agree that the answer is B

upvoted 4 times

A website design company recently migrated all customer sites to App Engine. Some sites are still in progress and should only be visible to customers and company employees from any location.

Which solution will restrict access to the in-progress sites?

- A. Upload an .htaccess file containing the customer and employee user accounts to App Engine.
- B. Create an App Engine firewall rule that allows access from the customer and employee networks and denies all other traffic.
- C. Enable Cloud Identity-Aware Proxy (IAP), and allow access to a Google Group that contains the customer and employee user accounts.
- D. Use Cloud VPN to create a VPN connection between the relevant on-premises networks and the company's GCP Virtual Private Cloud (VPC) network.

🗲️ 👤 **[Removed]** Highly Voted 👍 1 year, 2 months ago

Ans - C

https://cloud.google.com/iap/docs/concepts-overview#when_to_use_iap

upvoted 7 times

🗲️ 👤 **mlx** Most Recent ⌚ 1 year, 2 months ago

B - I think it is about to restrict access to 2 company networks, we can control access using IPs ranges, So Firewall rules should be sufficient. No need an extra product like IAP.. and also need users in Cloud Identity or other Idp federated..

upvoted 1 times

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

The sites should be accessible from any location, not just from the 2 company networks.

upvoted 2 times

🗲️ 👤 **MohitA** 1 year, 4 months ago

C serves the purpose

upvoted 3 times

🗲️ 👤 **bigdo** 1 year, 5 months ago

c is correct

upvoted 2 times

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

C is very correct

upvoted 2 times

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

C is correct.

upvoted 2 times

A company's application is deployed with a user-managed Service Account key. You want to use Google-recommended practices to rotate the key. What should you do?

- A. Open Cloud Shell and run `gcloud iam service-accounts enable-auto-rotate --iam-account=IAM_ACCOUNT`.
- B. Open Cloud Shell and run `gcloud iam service-accounts keys rotate --iam-account=IAM_ACCOUNT --key=NEW_KEY`.
- C. Create a new key, and use the new key in the application. Delete the old key from the Service Account.
- D. Create a new key, and use the new key in the application. Store the old key on the system as a backup key.

🗨️  **mdc** 7 months, 1 week ago

C is correct. As explained, You can rotate a key by creating a new key, updating applications to use the new key, and deleting the old key. Use the `serviceAccount.keys.create()` method and `serviceAccount.keys.delete()` method together to automate the rotation.

https://cloud.google.com/iam/docs/creating-managing-service-account-keys#deleting_service_account_keys
upvoted 2 times

🗨️  **DebasishLowes** 9 months, 3 weeks ago

Ans : C

upvoted 2 times

🗨️  **[Removed]** 1 year, 2 months ago


Ans - C

https://cloud.google.com/iam/docs/understanding-service-accounts#managing_service_account_keys
upvoted 4 times

🗨️  **ArizonaClassics** 1 year, 4 months ago

C is the right choice for me

upvoted 4 times

🗨️  **aiwaai** 1 year, 4 months ago

Correct Answer: C

upvoted 2 times

Your company runs a website that will store PII on Google Cloud Platform. To comply with data privacy regulations, this data can only be stored for a specific amount of time and must be fully deleted after this specific period. Data that has not yet reached the time period should not be deleted. You want to automate the process of complying with this regulation.

What should you do?

- A. Store the data in a single Persistent Disk, and delete the disk at expiration time.
- B. Store the data in a single BigQuery table and set the appropriate table expiration time.
- C. Store the data in a single Cloud Storage bucket and configure the bucket's Time to Live.
- D. Store the data in a single BigTable table and set an expiration time on the column families.

🗨️ 👤 **KILLMAD** Highly Voted 👍 1 year, 10 months ago

I believe the Answer is C not B.

This isn't data which needs to be analyzed, so I don't understand why would it be stored in BQ when having data stored in GCS seems much more reasonable.

I think the only thing about answer C which throws me off is the fact that they don't mention object life cycle management
upvoted 8 times

🗨️ 👤 **mozammil89** 1 year, 10 months ago

Answer C is correct. The TTL is common use case of Cloud Storage life cycle management. Here is what GCP says:

"To support common use cases like setting a Time to Live (TTL) for objects, retaining noncurrent versions of objects, or "downgrading" storage classes of objects to help manage costs, Cloud Storage offers the Object Lifecycle Management feature. This page describes the feature as well as the options available when using it. To learn how to enable Object Lifecycle Management, and for examples of lifecycle policies, see Managing Lifecycles."

<https://cloud.google.com/storage/docs/lifecycle>
upvoted 3 times

🗨️ 👤 **DebasishLowes** Most Recent 🕒 9 months, 3 weeks ago

Ans : C
upvoted 2 times

🗨️ 👤 **[Removed]** 1 year, 2 months ago

Ans - C
upvoted 4 times

🗨️ 👤 **aiwaai** 1 year, 4 months ago

Correct Answer: C
upvoted 2 times

🗨️ 👤 **Ganshank** 1 year, 7 months ago

The answers need to be worded better.
If we're taking the terms literally as specified in the options, then C cannot be the correction answer since there's no Time to Live configuration for a GCS bucket, only Lifecycle Policy.
With BigQuery, there is no row-level expiration, although we could create this behavior using Partitioned Tables. So this could be a potential answer.
D - it is possible to simulate cell-level TTL (<https://cloud.google.com/bigtable/docs/gc-cell-level>), so this too could be a potential answer, especially when different cells need different TTLs.
Between B & D, BigQuery follows a pay-as-you-go model and its storage costs are comparable to GCS storage costs. So this would be the more appropriate solution.
upvoted 3 times

🗨️ 👤 **smart123** 1 year, 6 months ago

The Buckets do have "Time to Live" feature.
<https://cloud.google.com/storage/docs/lifecycle>

Hence 'C' is the answer
upvoted 4 times

🗨️ 👤 **jonclem** 1 year, 9 months ago

I believe B is correct.

Setting a TTL of 14 days on the bucket via LifeCycle will not cause the bucket itself to be deleted after 14 days, instead it will cause each object uploaded to that bucket to be deleted 14 days after it was created
upvoted 2 times

🗨️ 👤 **xhova** 1 year, 9 months ago

Answer is C. You dont need the bucket to be deleted, you need the PII data stored to be deleted.

upvoted 5 times

A large financial institution is moving its Big Data analytics to Google Cloud Platform. They want to have maximum control over the encryption process of data stored at rest in BigQuery.
What technique should the institution use?

- A. Use Cloud Storage as a federated Data Source.
- B. Use a Cloud Hardware Security Module (Cloud HSM).
- C. Customer-managed encryption keys (CMEK).
- D. Customer-supplied encryption keys (CSEK).

🗲️ 👤 **Ganshank** Highly Voted 👍 1 year, 7 months ago

CSEK is only supported in Google Cloud Storage and Compute Engine, therefore D cannot be the right answer. Ideally, it would be client-side encryption, with BigQuery providing another round of encryption of the encrypted data - https://cloud.google.com/bigquery/docs/encryption-at-rest#client_side_encryption, but since that is not one of the options, we can go with C as the next best option.
upvoted 11 times

🗲️ 👤 **smart123** 1 year, 7 months ago

Option 'C' is correct. Option 'D' is not correct as CSEK a feature in Google Cloud Storage and Google Compute Engine only.
upvoted 3 times

🗲️ 👤 **DebasishLowes** Most Recent ⌚ 9 months, 3 weeks ago

Ans : C
upvoted 1 times

🗲️ 👤 **Aniyadu** 1 year ago

I feel C is the right answer. if customer wants to manage the keys from on-premises then D would be correct.
upvoted 2 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - C
upvoted 2 times

🗲️ 👤 **saurabh1805** 1 year, 2 months ago

C is correct answer as CSEK is not available for big query.
upvoted 2 times

🗲️ 👤 **MohitaA** 1 year, 4 months ago

C is the right answer as CSEC is only available for CS and CE's
upvoted 1 times

🗲️ 👤 **aiwaai** 1 year, 4 months ago

Correct Answer: C
upvoted 1 times

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

C is the RIGHT ONE!!!

If you want to manage the key encryption keys used for your data at rest, instead of having Google manage the keys, use Cloud Key Management Service to manage your keys. This scenario is known as customer-managed encryption keys (CMEK).
<https://cloud.google.com/bigquery/docs/encryption-at-rest>
upvoted 1 times

🗲️ 👤 **ArizonaClassics** 1 year, 4 months ago

ALSO READ : <https://cloud.google.com/bigquery/docs/customer-managed-encryption>
upvoted 1 times

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

Ans is C. BigQuery does not support CSEK. <https://cloud.google.com/security/encryption-at-rest>. <https://cloud.google.com/security/encryption-at-rest>
upvoted 4 times

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

I also feel D is right
upvoted 1 times

🗲️ 👤 **xhova** 1 year, 9 months ago

Answer is D. For max control you don't want to store the Key with Google.

upvoted 3 times

  **jonclem** 1 year, 9 months ago

For maximum control surely D is the correct answer.

CSEK:

<https://cloud.google.com/security/encryption-at-rest/customer-supplied-encryption-keys>

CMEK

<https://cloud.google.com/bigquery/docs/encryption-at-rest>

upvoted 2 times

Question #6

Topic 2

An organization is migrating from their current on-premises productivity software systems to G Suite. Some network security controls were in place that were mandated by a regulatory body in their region for their previous on-premises system. The organization's risk team wants to ensure that network security controls are maintained and effective in G Suite. A security architect supporting this migration has been asked to ensure that network security controls are in place as part of the new shared responsibility model between the organization and Google Cloud.

What solution would help meet the requirements?

- A. Ensure that firewall rules are in place to meet the required controls.
- B. Set up Cloud Armor to ensure that network security controls can be managed for G Suite.
- C. Network security is a built-in solution and Google's Cloud responsibility for SaaS products like G Suite.
- D. Set up an array of Virtual Private Cloud (VPC) networks to control network security as mandated by the relevant regulation.

  **ESP_SAP** Highly Voted  1 year, 1 month ago

Correct Answer is (C):

GSuite is Saas application.

Shared responsibility “Security of the Cloud” - GCP is responsible for protecting the infrastructure that runs all of the services offered in the GCP Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run GCP Cloud services.

upvoted 5 times

  **Topsy** Highly Voted  1 year ago

Answer is C- Review this Youtube Video- <https://www.youtube.com/watch?v=D2zf0SgNdUw>, scroll to 7:55, it would show you the Shared Responsibility model- With Gsuite being a SaaS product, Network Security is handled by Google

upvoted 5 times

  **FatCharlie** Most Recent  1 year, 1 month ago

Except for C, none of the options are possible in G Suite. There are no firewall, VPC, or Cloud Armor options there as far as I know.

upvoted 4 times

  **[Removed]** 1 year, 2 months ago


Ans - A

upvoted 2 times

  **saaurabh1805** 1 year, 2 months ago

Question is asking for Network security group, Hence i will go with Option A

upvoted 1 times

  **skshak** 1 year, 3 months ago

Answer is C. Gsuite is SaaS

upvoted 2 times

Your company is using Cloud Dataproc for its Spark and Hadoop jobs. You want to be able to create, rotate, and destroy symmetric encryption keys used for the persistent disks used by Cloud Dataproc. Keys can be stored in the cloud. What should you do?

- A. Use the Cloud Key Management Service to manage the data encryption key (DEK).
- B. Use the Cloud Key Management Service to manage the key encryption key (KEK).
- C. Use customer-supplied encryption keys to manage the data encryption key (DEK).
- D. Use customer-supplied encryption keys to manage the key encryption key (KEK).

🗨️ 👤 **mte_tech34** Highly Voted 👍 1 year, 3 months ago

Answer is B.

<https://cloud.google.com/dataproc/docs/concepts/configuring-clusters/customer-managed-encryption>

"The CMEK feature allows you to create, use, and revoke the key encryption key (KEK). Google still controls the data encryption key (DEK)."

upvoted 9 times

🗨️ 👤 **passtest100** 1 year, 3 months ago

SHOULD BE A.

NO envelope encryption is mentioned in the question.

upvoted 2 times

🗨️ 👤 **Arad** 1 month, 2 weeks ago

Correct answer is B, and A is wrong!

envelope encryption is default mechanism in CMEK when used for Dataproc, please check this link:

This PD and bucket data is encrypted using a Google-generated data encryption key (DEK) and key encryption key (KEK). The CMEK feature allows you to create, use, and revoke the key encryption key (KEK). Google still controls the data encryption key (DEK). For more information on Google data encryption keys, see Encryption at Rest.

<https://cloud.google.com/dataproc/docs/concepts/configuring-clusters/customer-managed-encryption>

upvoted 1 times

🗨️ 👤 **[Removed]** Most Recent 🕒 9 months ago

I also support B, but A is also good ,because kek is hosted within KMS, also the real DEK can be uploaded there ,or just in the database.

upvoted 2 times

🗨️ 👤 **DebasishLowes** 10 months, 1 week ago

Ans : B.

upvoted 2 times

🗨️ 👤 **[Removed]** 1 year, 2 months ago

Ans - B

upvoted 2 times

🗨️ 👤 **saurabh1805** 1 year, 2 months ago

Answer is B,

<https://cloud.google.com/dataproc/docs/concepts/configuring-clusters/customer-managed-encryption>

upvoted 3 times

A company allows every employee to use Google Cloud Platform. Each department has a Google Group, with all department members as group members. If a department member creates a new project, all members of that department should automatically have read-only access to all new project resources. Members of any other department should not have access to the project. You need to configure this behavior. What should you do to meet these requirements?

- A. Create a Folder per department under the Organization. For each department's Folder, assign the Project Viewer role to the Google Group related to that department.
- B. Create a Folder per department under the Organization. For each department's Folder, assign the Project Browser role to the Google Group related to that department.
- C. Create a Project per department under the Organization. For each department's Project, assign the Project Viewer role to the Google Group related to that department.
- D. Create a Project per department under the Organization. For each department's Project, assign the Project Browser role to the Google Group related to that department.

🗨️ 👤 **ownez** Highly Voted 👍 1 year, 3 months ago
Shouldn't it be A?

Project Browser has least permissions comparing to Project Viewer. The question is about have read-access to all new project resources.

roles/browser - Read access to browse the hierarchy for a project, including the folder, organization, and IAM policy. This role doesn't include permission to view resources in the project.

<https://cloud.google.com/iam/docs/understanding-roles#project-roles>
upvoted 15 times

🗨️ 👤 **singhjoga** 1 year ago
Correct, it is A. Project Browser does not have access to the resources inside the project, which is the requirement in the question.
upvoted 4 times

🗨️ 👤 **sylox** Most Recent 🕒 8 months, 2 weeks ago
It's A , browser is :
Read access to browse the hierarchy for a project, including the folder, organization, and IAM policy. This role doesn't include permission to view resources in the project.
<https://cloud.google.com/iam/docs/understanding-roles#project-roles>
upvoted 2 times

🗨️ 👤 **[Removed]** 9 months ago
either A or C because must be project viewer ,browser is not enough.<https://cloud.google.com/iam/docs/understanding-roles>
upvoted 1 times

🗨️ 👤 **[Removed]** 9 months ago
Why not A?
upvoted 1 times

🗨️ 👤 **desertlotus1211** 9 months, 3 weeks ago
The answer is A:

<https://stackoverflow.com/questions/54778596/whats-the-difference-between-project-browser-role-and-project-viewer-role-in-go#:~:text=8-,What's%20the%20difference%20between%20Project%20Browser%20role%20and,role%20in%20Google%20Cloud%20Platfor m&text=According%20to%20the%20console%20popup,read%20access%20to%20those%20resources.>
upvoted 2 times

🗨️ 👤 **CloudTrip** 10 months, 3 weeks ago
I think it's B. As the question says all members of that department should automatically have read-only access to all new project resources but browser will only provide the get, list permissions not read only permission so viewer seems to be more accurate here.

roles/browser
Read access to browse the hierarchy for a project, including the folder, organization, and IAM policy. This role doesn't include permission to view resources in the project.
resourceManager.folders.get
resourceManager.folders.list
resourceManager.organizations.get
resourceManager.projects.get
resourceManager.projects.getIamPolicy
resourceManager.projects.list



roles/viewer Viewer Permissions for read-only actions that do not affect state, such as viewing (but not modifying) existing resources or data.

upvoted 1 times

  **subhala** 1 year, 1 month ago

Question says - If a department member creates a new project, all members of that department should automatically have read-only access to all new project resources. and @ownez provided documentation that says - browser role doesn't include perm to view resources in the project. Hence B is the right answer.

upvoted 1 times

  **Fellipo** 1 year, 2 months ago

A it's OK

upvoted 2 times

  **[Removed]** 1 year, 2 months ago

Ans - A

upvoted 2 times

  **cipher90** 1 year, 3 months ago

Answer is B: "have read-only access to all new project resources." So it has to be in a folder to cascade the permissions to new projects carried.

upvoted 1 times

A customer's internal security team must manage its own encryption keys for encrypting data on Cloud Storage and decides to use customer-supplied encryption keys (CSEK).

How should the team complete this task?

- A. Upload the encryption key to a Cloud Storage bucket, and then upload the object to the same bucket.
- B. Use the gsutil command line tool to upload the object to Cloud Storage, and specify the location of the encryption key.
- C. Generate an encryption key in the Google Cloud Platform Console, and upload an object to Cloud Storage using the specified key.
- D. Encrypt the object, then use the gsutil command line tool or the Google Cloud Platform Console to upload the object to Cloud Storage.

🗲️ 👤 **FatCharlie** Highly Voted 👍 1 year, 1 month ago

The fact is, both B & D would work. I lean towards B because it allows you to manage the file using GCP tools later as long as you keep that key around.

B is definitely incomplete though, as the boto file does need to be updated.

upvoted 5 times

🗲️ 👤 **[Removed]** Most Recent 🕒 9 months ago

CD are not right because Google Cloud Console does not support CSEK. must choose from A and B

upvoted 1 times

🗲️ 👤 **DebasishLowes** 10 months, 1 week ago

Ans : B. Because if you encrypt the object using CSEK, then you can't use google cloud console to upload the object.

upvoted 4 times

🗲️ 👤 **VivekA** 1 year, 1 month ago

Ans: B

CSEK doesn't work on Cloud Shell or Cloud Console for Cloud Storage

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

upvoted 3 times

🗲️ 👤 **VivekA** 1 year, 1 month ago

D can't be an option - Refer restriction section.

[https://cloud.google.com/storage/docs/encryption/customer-supplied-](https://cloud.google.com/storage/docs/encryption/customer-supplied-keys#:~:text=You%20cannot%20use%20the%20Google,a%20customer%2Dsupplied%20encryption%20key.)

[keys#:~:text=You%20cannot%20use%20the%20Google,a%20customer%2Dsupplied%20encryption%20key.](https://cloud.google.com/storage/docs/encryption/customer-supplied-keys#:~:text=You%20cannot%20use%20the%20Google,a%20customer%2Dsupplied%20encryption%20key.)

upvoted 1 times

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

Ans is C

upvoted 1 times

🗲️ 👤 **Fellipo** 1 year, 2 months ago

if Option B was correct you have to modify your boto file which is not the full option.

upvoted 3 times

🗲️ 👤 **Fellipo** 1 year, 2 months ago

B is correct , sorry

upvoted 4 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - D

upvoted 4 times

🗲️ 👤 **saaurabh1805** 1 year, 2 months ago

Option B is closed and correct one.

upvoted 3 times

🗲️ 👤 **saaurabh1805** 1 year, 2 months ago

*closest

upvoted 1 times

🗲️ 👤 **skshak** 1 year, 3 months ago

Sorry, Answer is C. - Generate a key in cloud shell and then upload the object using that key

upvoted 1 times

🗲️ 👤 **skshak** 1 year, 3 months ago

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

Answer B

upvoted 4 times

Question #10

Topic 2

While migrating your organization's infrastructure to GCP, a large number of users will need to access GCP Console. The Identity Management team already has a well-established way to manage your users and want to keep using your existing Active Directory or LDAP server along with the existing SSO password.

What should you do?

- A. Manually synchronize the data in Google domain with your existing Active Directory or LDAP server.
- B. Use Google Cloud Directory Sync to synchronize the data in Google domain with your existing Active Directory or LDAP server.
- C. Users sign in directly to the GCP Console using the credentials from your on-premises Kerberos compliant identity provider.
- D. Users sign in using OpenID (OIDC) compatible IdP, receive an authentication token, then use that token to log in to the GCP Console.

  **ThisisJohn** 4 weeks, 1 day ago

Selected Answer: D

My vote goes for D.

From the blog post linked below " users' passwords are not synchronized by default. Only the identities are synchronized, unless you make an explicit choice to synchronize passwords (which is not a best practice and should be avoided)".

Also, from GCP documentation "Authenticating with OIDC and AD FS" <https://cloud.google.com/anthos/clusters/docs/on-prem/1.6/how-to/oidc-adfs>

Blog post quoted above <https://cloud.google.com/blog/products/identity-security/using-your-existing-identity-management-system-with-google-cloud-platform>

upvoted 1 times

  **rr4444** 2 weeks ago

D sounds nice, but the user doesn't "use" the token.... that's used in the integration with Cloud Identity. So answer must be B, GCDS

upvoted 1 times

  **DebasishLowes** 10 months, 1 week ago

Ans : B

upvoted 4 times

  **[Removed]** 1 year, 2 months ago

Ans - B

upvoted 3 times

  **saurabh1805** 1 year, 2 months ago

B is correct answer here.

upvoted 3 times

Your team wants to make sure Compute Engine instances running in your production project do not have public IP addresses. The frontend application Compute

Engine instances will require public IPs. The product engineers have the Editor role to modify resources. Your team wants to enforce this requirement.

How should your team meet these requirements?

- A. Enable Private Access on the VPC network in the production project.
- B. Remove the Editor role and grant the Compute Admin IAM role to the engineers.
- C. Set up an organization policy to only permit public IPs for the front-end Compute Engine instances.
- D. Set up a VPC network with two subnets: one with public IPs and one without public IPs.

🗨️ 👤 **saurabh1805** Highly Voted 👍 1 year, 2 months ago
C is correct option here, Refer below link for more details.

<https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints#constraints-for-specific-services>
upvoted 6 times

🗨️ 👤 **FatCharlie** 1 year, 1 month ago
More specifically, it's the "Restrict VM IP Forwarding" constraint under Compute Engine
upvoted 2 times

🗨️ 👤 **FatCharlie** 1 year, 1 month ago
Sorry, no. It's the one under that :)

"Define allowed external IPs for VM instances"
upvoted 2 times

🗨️ 👤 **DebasishLowes** Most Recent 🕒 10 months, 1 week ago
Ans : C
upvoted 3 times

🗨️ 👤 **[Removed]** 1 year, 2 months ago
Ans - C
upvoted 4 times

🗨️ 👤 **HectorLeon2099** 1 year, 3 months ago
I'll go with A
upvoted 2 times

A company is running their webshop on Google Kubernetes Engine and wants to analyze customer transactions in BigQuery. You need to ensure that no credit card numbers are stored in BigQuery

What should you do?

- A. Create a BigQuery view with regular expressions matching credit card numbers to query and delete affected rows.
- B. Use the Cloud Data Loss Prevention API to redact related infoTypes before data is ingested into BigQuery.
- C. Leverage Security Command Center to scan for the assets of type Credit Card Number in BigQuery.
- D. Enable Cloud Identity-Aware Proxy to filter out credit card numbers before storing the logs in BigQuery.

🗲️ 👤 **saurabh1805** Highly Voted 👍 1 year, 2 months ago

B is correct answer here.

upvoted 6 times

🗲️ 👤 **saurabh1805** 1 year, 2 months ago

<https://cloud.google.com/bigquery/docs/scan-with-dlp>

upvoted 2 times

🗲️ 👤 **rr4444** Most Recent ⌚ 2 weeks ago

Selected Answer: B

D is silly

upvoted 1 times

🗲️ 👤 **[Removed]** 9 months ago

D is impossible. I support B

upvoted 2 times

🗲️ 👤 **DebasishLowes** 10 months, 1 week ago

Ans : B

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - B

upvoted 3 times

🗲️ 👤 **passtest100** 1 year, 3 months ago

B is the answer

upvoted 2 times

🗲️ 👤 **Mohita** 1 year, 4 months ago

B is the answer

upvoted 2 times

In a shared security responsibility model for IaaS, which two layers of the stack does the customer share responsibility for? (Choose two.)

- A. Hardware
- B. Network Security
- C. Storage Encryption
- D. Access Policies
- E. Boot

🗲️ 👤 **DebasishLowes** Highly Voted 👍 9 months, 3 weeks ago

Ans : BD

upvoted 6 times

🗲️ 👤 **rr4444** Most Recent 🕒 2 weeks ago

Selected Answer: BD

BD <https://cloud.google.com/blog/products/containers-kubernetes/exploring-container-security-the-shared-responsibility-model-in-gke-container-security-shared-responsibility-model-gke>

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - BD

upvoted 3 times

🗲️ 👤 **saaurabh1805** 1 year, 2 months ago

B and D is correct option.

upvoted 3 times

🗲️ 👤 **passtest100** 1 year, 3 months ago

B and D

upvoted 3 times

🗲️ 👤 **lordb** 1 year, 3 months ago

B and D

upvoted 3 times

An engineering team is launching a web application that will be public on the internet. The web application is hosted in multiple GCP regions and will be directed to the respective backend based on the URL request.

Your team wants to avoid exposing the application directly on the internet and wants to deny traffic from a specific list of malicious IP addresses. Which solution should your team implement to meet these requirements?

- A. Cloud Armor
- B. Network Load Balancing
- C. SSL Proxy Load Balancing
- D. NAT Gateway

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

Ans : A

upvoted 4 times

🗲️ 👤 **BillBaits** 2 months, 1 week ago

Think so

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - A

upvoted 3 times

🗲️ 👤 **mlyu** 1 year, 4 months ago

Definitely B

upvoted 2 times

🗲️ 👤 **ownez** 1 year, 3 months ago

Should be A? Cloud armor can deny traffic by defining IP addresses list rule and to avoid exposing the application directly on the internet.

While Network LB is using Google Cloud firewalls to control or filter access to the backend VMs.

Answer is A.

upvoted 5 times

🗲️ 👤 **mlyu** 1 year, 3 months ago

you are correct. Answer is A

The Cloud armor able to directed user traffic to an external HTTP(S) load balancer enters the PoP closest to the user in Premium Tier.

<https://cloud.google.com/armor/docs/security-policy-overview#edge-security>

upvoted 4 times

Your company operates an application instance group that is currently deployed behind a Google Cloud load balancer in us-central-1 and is configured to use the Standard Tier network. The infrastructure team wants to expand to a second Google Cloud region, us-east-2. You need to set up a single external IP address to distribute new requests to the instance groups in both regions. What should you do?

- A. Change the load balancer backend configuration to use network endpoint groups instead of instance groups.
- B. Change the load balancer frontend configuration to use the Premium Tier network, and add the new instance group.
- C. Create a new load balancer in us-east-2 using the Standard Tier network, and assign a static external IP address.
- D. Create a Cloud VPN connection between the two regions, and enable Google Private Access.

🗨️ 👤 **Fellipo** Highly Voted 👍 1 year, 2 months ago

In Premium Tier: Backends can be in any region and any VPC network.

In Standard Tier: Backends must be in the same region as the forwarding rule, but can be in any VPC network.
upvoted 7 times

🗨️ 👤 **saurabh1805** Highly Voted 👍 1 year, 2 months ago

I will also go with Option B
upvoted 5 times

🗨️ 👤 **DebasishLowes** Most Recent ⌚ 9 months, 3 weeks ago

Ans : B
upvoted 2 times

🗨️ 👤 **mlyu** 1 year, 4 months ago

Should be B
In Standard Tier LB, Backends must be in the same region
https://cloud.google.com/load-balancing/docs/load-balancing-overview#backend_region_and_network
upvoted 4 times

You are the security admin of your company. Your development team creates multiple GCP projects under the "implementation" folder for several dev, staging, and production workloads. You want to prevent data exfiltration by malicious insiders or compromised code by setting up a security perimeter. However, you do not want to restrict communication between the projects.

What should you do?

- A. Use a Shared VPC to enable communication between all projects, and use firewall rules to prevent data exfiltration.
- B. Create access levels in Access Context Manager to prevent data exfiltration, and use a shared VPC for communication between projects.
- C. Use an infrastructure-as-code software tool to set up a single service perimeter and to deploy a Cloud Function that monitors the "implementation" folder via Stackdriver and Cloud Pub/Sub. When the function notices that a new project is added to the folder, it executes Terraform to add the new project to the associated perimeter.
- D. Use an infrastructure-as-code software tool to set up three different service perimeters for dev, staging, and prod and to deploy a Cloud Function that monitors the "implementation" folder via Stackdriver and Cloud Pub/Sub. When the function notices that a new project is added to the folder, it executes Terraform to add the new project to the respective perimeter.

🗨️ **jonclem** Highly Voted 1 year, 1 month ago

I'd also go with option B and here's why:
<https://cloud.google.com/access-context-manager/docs/overview>

Option A was a consideration until I came across this: <https://cloud.google.com/security/data-loss-prevention/preventing-data-exfiltration>
upvoted 9 times

🗨️ **eshtanaka** Most Recent 2 months, 1 week ago

Correct answer is C. See the description for "automatically secured folder" https://github.com/terraform-google-modules/terraform-google-vpc-service-controls/tree/master/examples/automatic_folder
upvoted 2 times

🗨️ **nilb94** 4 months, 3 weeks ago

Think it should be C. Access Context Manager docs say it is for ingress. Service Controls seems correct for exfiltration, and projects must be allowed to communicate with each other so they need to be in a single service perimeter.
upvoted 2 times

🗨️ **dzhu** 4 months, 4 weeks ago

I think this is C. Communication between the project is necessary tied to VPC, but you need to include all projects under implementation folder in a single VPCSC
upvoted 3 times

🗨️ **desertlotus1211** 9 months, 3 weeks ago

Answer is B:
<https://cloud.google.com/access-context-manager/docs/overview>

You need to read the question AND Answer carefully before selecting.
Answer A is in Answer B
upvoted 2 times

🗨️ **DebasishLowes** 9 months, 3 weeks ago

Ans : A. To make the communication between different projects, shared vpc is required.
upvoted 1 times

🗨️ **HateMicrosoft** 10 months, 1 week ago

The correct answer is :B
Access Context Manager
<https://cloud.google.com/access-context-manager/docs/overview>

Preventing Data Exfiltration
<https://cloud.google.com/security/data-loss-prevention/preventing-data-exfiltration>
upvoted 3 times

🗨️ **deardeer** 11 months, 2 weeks ago

D is the answer. This question is about sharing across perimeters. https://cloud.google.com/vpc-service-controls/docs/share-across-perimeters#service_perimeter_bridges
upvoted 2 times

🗨️ **mlx** 1 year, 2 months ago

could be D : use case needs service controls and security perimeter
upvoted 2 times

🗨️ **saurabh1805** 1 year, 2 months ago

B is correct answer. Firewall can never stop data exfiltration.

upvoted 4 times

  **ZODOGAM** 1 month ago



This does not solve the data leak

upvoted 1 times

  **[Removed]** 1 year, 2 months ago

Ans - A

upvoted 1 times

  **Rantu** 1 year, 3 months ago

A is the answer

upvoted 1 times

  **ZODOGAM** 1 month ago

This does not solve data exfiltration

upvoted 1 times

You are on your company's development team. You noticed that your web application hosted in staging on GKE dynamically includes user data in web pages without first properly validating the inputted data. This could allow an attacker to execute gibberish commands and display arbitrary content in a victim user's browser in a production environment.

How should you prevent and fix this vulnerability?

- A. Use Cloud IAP based on IP address or end-user device attributes to prevent and fix the vulnerability.
- B. Set up an HTTPS load balancer, and then use Cloud Armor for the production environment to prevent the potential XSS attack.
- C. Use Web Security Scanner to validate the usage of an outdated library in the code, and then use a secured version of the included library.
- D. Use Web Security Scanner in staging to simulate an XSS injection attack, and then use a templating system that supports contextual auto-escaping.

🗨️ **Lancyqusa** 2 weeks, 2 days ago

It should be C because the web security scanner will identify the library known to contain the security issue as in the examples here - https://cloud.google.com/security-command-center/docs/how-to-use-web-security-scanner#example_findings . Once the security issue is identified, the vulnerability can be fixed by a secure version of that library.

upvoted 1 times

🗨️ **DebasishLowes** 9 months, 3 weeks ago

Ans : D

upvoted 2 times

🗨️ **deardeer** 11 months, 2 weeks ago

Answer is D. There is mention about simulating in Web Security Scanner. "Web Security Scanner cross-site scripting (XSS) injection testing *simulates* an injection attack by inserting a benign test string into user-editable fields and then performing various user actions."

<https://cloud.google.com/security-command-center/docs/how-to-remediate-web-security-scanner-findings#xss>

upvoted 4 times

🗨️ **ThisisJohn** 4 weeks, 1 day ago

Agree. Also from your link

"There are various ways to fix this problem. The recommended fix is to escape all output and use a templating system that supports contextual auto-escaping."

So escaping is a way to fix the issue, which is required by the question

upvoted 1 times

🗨️ **pyc** 11 months, 2 weeks ago

C,

D is wrong, as Security Scanner can't "simulate" anything. It's a scanner.

B is not right, as Armor can't do input data validation, it just deny/allow IP/CIDR.

upvoted 1 times

🗨️ **desertlotus1211** 9 months, 3 weeks ago

Yes it can simulate... Read the documentation first...

upvoted 3 times

🗨️ **KarVaid** 1 year ago

<https://cloud.google.com/security-command-center/docs/concepts-web-security-scanner-overview>

Security Scanner should be able to scan for XSS vulnerabilities as well. Option D is better.

upvoted 2 times

🗨️ **KarVaid** 1 year ago

Cloud armor can prevent the vulnerability but to fix it, you would need Security scanner.

upvoted 1 times

🗨️ **Fellipo** 1 year, 2 months ago

B , <https://cloud.google.com/armor>

upvoted 4 times

🗨️ **[Removed]** 1 year, 2 months ago

Ans - D

upvoted 3 times

🗨️ **HectorLeon2099** 1 year, 3 months ago

Answer is B. Web Security Scanner can look for XSS vulnerabilities but can't simulate XSS injection attack.

https://cloud.google.com/armor/docs/rule-tuning#cross-site_scripting_xss

upvoted 3 times

  **FatCharlie** 1 year, 1 month ago

Web Security Scanner does appear to be able to simulate an XSS attack.

"Web Security Scanner cross-site scripting (XSS) injection testing simulates an injection attack by inserting a benign test string into user-editable fields and then performing various user actions. Custom detectors observe the browser and DOM during this test to determine whether an injection was successful and assess its potential for exploitation."

<https://cloud.google.com/security-command-center/docs/how-to-remediate-web-security-scanner-findings#remediate-findings>

upvoted 4 times

  **saurobh1805** 1 year, 2 months ago

Agree B is correct answer here.

upvoted 2 times

  **Jerrard** 1 year, 3 months ago

D. <https://cloud.google.com/security-command-center/docs/concepts-web-security-scanner-overview>

upvoted 4 times

You are part of a security team that wants to ensure that a Cloud Storage bucket in Project A can only be readable from Project B. You also want to ensure that data in the Cloud Storage bucket cannot be accessed from or copied to Cloud Storage buckets outside the network, even if the user has the correct credentials.

What should you do?

- A. Enable VPC Service Controls, create a perimeter with Project A and B, and include Cloud Storage service.
- B. Enable Domain Restricted Sharing Organization Policy and Bucket Policy Only on the Cloud Storage bucket.
- C. Enable Private Access in Project A and B networks with strict firewall rules to allow communication between the networks.
- D. Enable VPC Peering between Project A and B networks with strict firewall rules to allow communication between the networks.

🗨️  **FatCharlie** Highly Voted 1 year, 1 month ago

The answer is A. This is question is covered by an example given for VPC Service Perimeters


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

upvoted 12 times

🗨️  **nilb94** Most Recent 4 months, 3 weeks ago

A - VPC Service Controls

upvoted 1 times

🗨️  **jeeet_** 7 months, 2 weeks ago

Answer is most positively A.

VPC service controls lets Security team create fine-grained Perimeter across projects within organization.

-> Security perimeter for API-Based services like Bigtable instances, Storage and Bigquery datasets.. are a kind of super powers for VPC Service control.

well in my test, I chose option B, but

Domain Restricted Organization policies are for limiting resource sharing based on domain.

so if you're out in internet, and have credentials you still can access resources based on your domain access level. So B option is wrong.

upvoted 1 times

🗨️  **HateMicrosoft** 10 months, 1 week ago

The correct answer is: A

This is obtained by the VPC Service Controls by the perimeter setup.

Overview of VPC Service Controls

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

upvoted 1 times

🗨️  **jonclem** 1 year, 1 month ago

I would say option A is a better fit due to VPC Service Controls.

upvoted 3 times

🗨️  **jonclem** 1 year, 1 month ago

I'd be inclined to agree, option B seems a better fit. Here's my reasoning behind it:

<https://cloud.google.com/access-context-manager/docs/overview>

upvoted 1 times

🗨️  **jonclem** 1 year, 1 month ago


please ignore this comment, wrong question.

upvoted 1 times

🗨️  **saurabh1805** 1 year, 2 months ago

what is being asked is data exfiltration as well and which can be only achieved via VPC perimeter and created a bridge between both project.

upvoted 1 times

🗨️  **Ducle** 1 year, 2 months ago


A is better

upvoted 2 times

🗨️  **[Removed]** 1 year, 2 months ago

Ans - B

upvoted 1 times

🗨️  **Jerrard** 1 year, 3 months ago

B. <https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains>

upvoted 1 times

An organization is migrating from their current on-premises productivity software systems to G Suite. Some network security controls were in place that were mandated by a regulatory body in their region for their previous on-premises system. The organization's risk team wants to ensure that network security controls are maintained and effective in G Suite. A security architect supporting this migration has been asked to ensure that network security controls are in place as part of the new shared responsibility model between the organization and Google Cloud.

What solution would help meet the requirements?

- A. Ensure that firewall rules are in place to meet the required controls.
- B. Set up Cloud Armor to ensure that network security controls can be managed for G Suite.
- C. Network security is a built-in solution and Google's Cloud responsibility for SaaS products like G Suite.
- D. Set up an array of Virtual Private Cloud (VPC) networks to control network security as mandated by the relevant regulation.

🗲️ 👤 **PiotrKam** Highly Voted 👍 1 year, 2 months ago

C, because in shared responsibility model like in GSuite (SaaS) network controls are in place. We can't manage firewall, cloud armor or any other network security solution.

upvoted 13 times

🗲️ 👤 **DebasishLowes** Most Recent ⌚ 10 months, 1 week ago

Ans : C

upvoted 2 times

🗲️ 👤 **Ducle** 1 year, 2 months ago

Should be B, as GSuit is SaaS and only CloudArmour can help on network security with WAF

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - A

upvoted 1 times

Your company is using Cloud Dataproc for its Spark and Hadoop jobs. You want to be able to create, rotate, and destroy symmetric encryption keys used for the persistent disks used by Cloud Dataproc. Keys can be stored in the cloud.

What should you do?

- A. Use the Cloud Key Management Service to manage the data encryption key (DEK).
- B. Use the Cloud Key Management Service to manage the key encryption key (KEK).
- C. Use customer-supplied encryption keys to manage the data encryption key (DEK).
- D. Use customer-supplied encryption keys to manage the key encryption key (KEK).

🗲️ 👤 **DebasishLowes** 10 months, 1 week ago

Ans : B

upvoted 3 times

🗲️ 👤 **[Removed]** 1 year, 2 months ago

Ans - B

<https://cloud.google.com/dataproc/docs/concepts/configuring-clusters/customer-managed-encryption>

upvoted 2 times

🗲️ 👤 **mte_tech34** 1 year, 3 months ago

Answer is B

upvoted 3 times

A company allows every employee to use Google Cloud Platform. Each department has a Google Group, with all department members as group members. If a department member creates a new project, all members of that department should automatically have read-only access to all new project resources. Members of any other department should not have access to the project. You need to configure this behavior.

What should you do to meet these requirements?

- A. Create a Folder per department under the Organization. For each department's Folder, assign the Project Viewer role to the Google Group related to that department.
- B. Create a Folder per department under the Organization. For each department's Folder, assign the Project Browser role to the Google Group related to that department.
- C. Create a Project per department under the Organization. For each department's Project, assign the Project Viewer role to the Google Group related to that department.
- D. Create a Project per department under the Organization. For each department's Project, assign the Project Browser role to the Google Group related to that department.

🗨️ 👤 **[Removed]** 9 months ago

support A, folder over project for automatic has the IAM access. Viewer over browser, to have read access for every resource in on project.
upvoted 3 times

🗨️ 👤 **DebasishLowes** 10 months, 1 week ago

Ans : A
upvoted 2 times

🗨️ 👤 **[Removed]** 1 year, 2 months ago

Ans - A
upvoted 2 times

🗨️ 👤 **[Removed]** 1 year, 2 months ago

https://cloud.google.com/resource-manager/docs/access-control-proj#using_basic_roles
upvoted 1 times

A customer's internal security team must manage its own encryption keys for encrypting data on Cloud Storage and decides to use customer-supplied encryption keys (CSEK).

How should the team complete this task?

- A. Upload the encryption key to a Cloud Storage bucket, and then upload the object to the same bucket.
- B. Use the gsutil command line tool to upload the object to Cloud Storage, and specify the location of the encryption key.
- C. Generate an encryption key in the Google Cloud Platform Console, and upload an object to Cloud Storage using the specified key.
- D. Encrypt the object, then use the gsutil command line tool or the Google Cloud Platform Console to upload the object to Cloud Storage.

🗲️ 👤 **adiaz_** 3 months, 1 week ago

B is the correct.

upvoted 1 times

🗲️ 👤 **Zuy01** 5 months ago

Ans is B.

"You cannot use the Google Cloud Console to download objects that are encrypted with a customer-supplied encryption key. Similarly, when you use the Google Cloud Console to upload an object, you cannot encrypt the object with a customer-supplied encryption key. You can perform these actions with customer-managed encryption keys."

<https://cloud.google.com/storage/docs/encryption/customer-supplied-keys#restrictions>

upvoted 1 times

🗲️ 👤 **DebasishLowes** 10 months, 1 week ago

Ans : B. Because you can't use CSEK to encrypt the object while uploading the object into cloud storage. It can be done by CMEK.

upvoted 2 times

🗲️ 👤 **KarVaid** 1 year ago

The answer should be B where you specify the Encryption key location in the configuration file before you copy the file using gsutil.

upvoted 2 times

🗲️ 👤 **singhjoga** 1 year ago

It is not the location of file but the "Base64-encoded string" of encryption key provided in the boto config gile. Therefore, B is misleading. Only valid option left is D.

upvoted 1 times

🗲️ 👤 **Rodine** 11 months, 4 weeks ago

It cant be D because u cant encrypt an object in console by CSEK, only by CMEK. Just choose a Cloud storage and try to encrypt the bucket by CSEK... its impossible, only CMEK and google... Compute Engine is only the option where u can encrypt the disk by CSEK and paste it into bracket.

upvoted 2 times

🗲️ 👤 **TNT87** 11 months ago

Kindly re-read D, and D is the answer according to documentation. D speaks of CMEK not CSEK...so you wrote the opposite, of which D is the answer.

upvoted 1 times

🗲️ 👤 **TNT87** 11 months ago

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

i mean D speaks of how exactly CSEK works..kindly visit the link

upvoted 1 times

🗲️ 👤 **Topsy** 1 year ago

Answer is B- Similarly, when you use the Google Cloud Console to upload an object, you cannot encrypt the object with a customer-supplied encryption key. You can perform these actions with customer-managed encryption keys.

upvoted 4 times

🗲️ 👤 **singhjoga** 1 year ago

Encryption key is not passed in the command line, but in the boto file as a Base64-encoded string

upvoted 1 times

🗲️ 👤 **mondigo** 1 year ago

D

you do not put location but key in gsutil

you can also use api or code wrote i python to encrpyt

Note: You can alternatively include this information in each gsutil command by using the -o top-level flag: -o "GSUtil:encryption_key=<var>YOUR_ENCRYPTION_KEY</var>"



upvoted 1 times

  **mondigo** 1 year ago

i change my mind to B based on

"Warning: This means that when overwriting or rewriting a CSEK- or CMEK-encrypted object, if encryption_key is not specified, gsutil will replace customer-supplied or customer-managed encryption with Google-managed encryption (or customer-managed encryption if the bucket has a default KMS key set)."

upvoted 2 times

  **Sima158** 1 year, 1 month ago

Answer is B?

upvoted 2 times

  **Sima158** 1 year, 1 month ago

Since you can't use csek in storage

upvoted 1 times

  **ChewB666** 1 year, 1 month ago



Anybody know?

upvoted 1 times

  **saurabh1805** 1 year, 2 months ago

Option C sounder better as you can supply encryption details via boto file and use gutlis to upload and download file.

upvoted 1 times

  **awsrd** 1 year, 2 months ago

you mean B? C does not speak anything about gsutil. with gsutil we can specify key location

upvoted 2 times

  **[Removed]** 1 year, 2 months ago

Ans - D

upvoted 2 times

While migrating your organization's infrastructure to GCP, a large number of users will need to access GCP Console. The Identity Management team already has a well-established way to manage your users and want to keep using your existing Active Directory or LDAP server along with the existing SSO password.

What should you do?

- A. Manually synchronize the data in Google domain with your existing Active Directory or LDAP server.
- B. Use Google Cloud Directory Sync to synchronize the data in Google domain with your existing Active Directory or LDAP server.
- C. Users sign in directly to the GCP Console using the credentials from your on-premises Kerberos compliant identity provider.
- D. Users sign in using OpenID (OIDC) compatible IdP, receive an authentication token, then use that token to log in to the GCP Console.

  **ThisisJohn** 4 weeks, 1 day ago

Selected Answer: D

My vote goes for D.



As per the question, users may be able to keep using their existing passwords. While that is possible with Directory Sync, documentation explicitly mentions it is not recommended "unless you make an explicit choice to synchronize passwords (which is not a best practice and should be avoided)." <https://cloud.google.com/blog/products/identity-security/using-your-existing-identity-management-system-with-google-cloud-platform>

On the other side, there's documentation about "Signing in users with OIDC" <https://cloud.google.com/identity-platform/docs/web/oidc>
upvoted 1 times

  **rr4444** 2 weeks ago

OIDC is nice, but the user doesn't use the token. the client code itself does, with the integration of the OIDC in Cloud Identity. hence B is correct

upvoted 1 times

  **adiaz_** 3 months, 1 week ago

The Ans correct is: B

upvoted 1 times

  **DebasishLowes** 10 months, 1 week ago

Ans : B

upvoted 3 times

  **[Removed]** 1 year, 2 months ago

Ans - B

upvoted 4 times