

🔗 Google Discussions



Exam Professional Data Engineer All Questions

View all questions & answers for the Professional Data Engineer exam

[Go to Exam](#)

📄 EXAM PROFESSIONAL DATA ENGINEER TOPIC 1 QUESTION 187 DISCUSSION

Actual exam question from Google's Professional Data Engineer

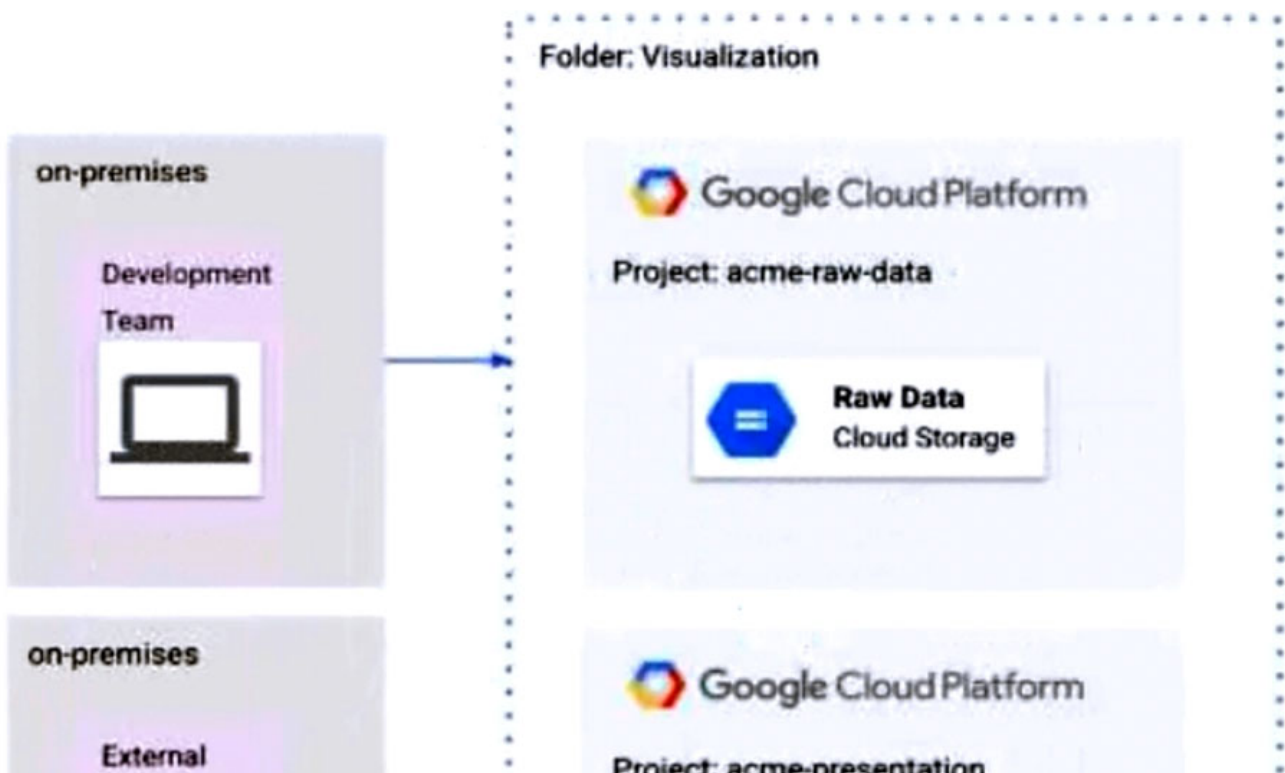
Question #: 187

Topic #: 1

[\[All Professional Data Engineer Questions\]](#)

The Development and External teams have the project viewer Identity and Access Management (IAM) role in a folder named Visualization. You want the

Development Team to be able to read data from both Cloud Storage and BigQuery, but the External Team should only be able to read data from BigQuery. What should you do?





- A. Remove Cloud Storage IAM permissions to the External Team on the acme-raw-data project.
- B. Create Virtual Private Cloud (VPC) firewall rules on the acme-raw-data project that deny all ingress traffic from the External Team CIDR range.
- C. Create a VPC Service Controls perimeter containing both projects and BigQuery as a restricted API. Add the External Team users to the perimeter's Access Level.
- D. Create a VPC Service Controls perimeter containing both projects and Cloud Storage as a restricted API. Add the Development Team users to the perimeter's Access Level.

Show Suggested Answer

by [AWSandeep](#) at Sept. 2, 2022, 11:02 p.m.

Comments

Type your comment...

Submit

AWSandeep Highly Voted 2 years, 2 months ago

Selected Answer: D

D. Create a VPC Service Controls perimeter containing both projects and Cloud Storage as a restricted API. Add the Development Team users to the perimeter's Access Level.

Reveal Solution

upvoted 16 times

Oleksandr0501 1 year, 5 months ago

no, https://cloud.google.com/blog/products/serverless/cloud-run-gets-enterprise-grade-network-security-with-vpc-sc?utm_source=youtube&utm_medium=unpaidsoc&utm_campaign=CDR_pri_gcp_m0v4tedeiao_ThisWeekInCloud_082621&utm_content=description

upvoted 1 times

Oleksandr0501 1 year, 5 months ago

damn, i am confused anyway. Can be D.

upvoted 1 times

Oleksandr0501 1 year, 5 months ago

should be D, as i think now, because we create a "magic bulb" around around Cloud storage and Dev team, and it will be protected from external influence like a human cell. Meantime Dev team will still be able to access Bigquery. But external team will not manage to access Cloud storage.

upvoted 1 times

TNT87 2 years, 1 month ago

WHy do you have to put the development team at the access perimeter???

upvoted 1 times

maci_f Highly Voted 1 year, 9 months ago

Selected Answer: D

"The grouping of GCP Project(s) and Service API(s) in the Service Perimeter result in restricting unauthorized access outside of the Service Perimeter to Service API endpoint(s) referencing resources inside of the Service Perimeter."
<https://scalesec.com/blog/vpc-service-controls-in-plain-english/>

Development team: needs to access both Cloud Storage and BQ -> therefore we put the Development team inside a perimeter so it can access both the Cloud Storage and the BQ

External team: allowed to access only BQ -> therefore we put Cloud Storage behind the restricted API and leave the external team outside of the perimeter, so it can access BQ, but is prohibited from accessing the Cloud Storage

   upvoted 10 times

  **josech** **Most Recent** 5 months, 2 weeks ago

Selected Answer: A

It is not a network issue but a IAM permissions issue.
<https://cloud.google.com/iam/docs/deny-overview#inheritance>

   upvoted 4 times

  **Aman47** 10 months, 3 weeks ago

Comments are saying it correct its C

   upvoted 1 times

  **Mamko** 1 year, 1 month ago

It's D for sure

   upvoted 1 times

  **techabhi2_0** 1 year, 2 months ago

A - Simple and straight forward

   upvoted 5 times

  **wan2three** 1 year, 2 months ago

Why not B, I think CD will cause one of the team can not reach one or two of those DBs. A is not correct either


   upvoted 1 times

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

Selected Answer: D

D. VPC Service Controls can create a service perimeter and define a restrictive API (service to protect). In this case, two projects are inside the perimeter and Cloud Storage is defined as the restrictive API. This means only services running on these two projects can access the Cloud Storage. And to allow users to access the Cloud Storage, they need have the access to the service perimeter. Hence, D is the correct answer.


   upvoted 4 times

  **izekc** 1 year, 6 months ago

Selected Answer: C

C is correct

   upvoted 1 times

  **midgoo** 1 year, 7 months ago

Selected Answer: D

D sounds more correct, but if the project is already in the Service Control, would External people can access the BigQuery dataset in that project?

   upvoted 1 times

  **[Removed]** 1 year, 9 months ago

seriously why u guys use VPC? the question never mentioned VPN or Interconnect, how can on-premise use VPC?

A is the answer.

   upvoted 4 times

  **zellck** 1 year, 11 months ago

Selected Answer: D

D is the answer.

   upvoted 1 times

  **TNT87** 1 year, 9 months ago

Answer C, i dnt know if you have studied cloud security? if you have you will know

   upvoted 1 times

  **Oleksandr0501** 1 year, 5 months ago

you might be correct. C.

https://cloud.google.com/blog/products/serverless/cloud-run-gets-enterprise-grade-network-security-with-vpc-sc?utm_source=youtube&utm_medium=unpaidsoc&utm_campaign=CDR_pri_gcp_m0v4tedeiao_ThisWeekInCloud_082621&utm_content=description
https://www.youtube.com/watch?v=ABIY7FexJJI&ab_channel=GoogleCloudTech

👍 🔄 🚩 upvoted 1 times

🗄️ 👤 **Atnafu** 1 year, 11 months ago

C

Extend perimeters to authorized VPN or Cloud Interconnect

You can configure private communication to Google Cloud resources from VPC networks that span hybrid environments with Private Google Access on-premises extensions. A VPC network must be part of a service perimeter for VMs on that network to privately access managed Google Cloud resources within that service perimeter.

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

👍 🔄 🚩 upvoted 2 times

🗄️ 👤 **Atnafu** 1 year, 11 months ago

I meant D Not C

👍 🔄 🚩 upvoted 2 times

🗄️ 👤 **cloudmon** 1 year, 12 months ago

Selected Answer: D

D makes the most sense to me

👍 🔄 🚩 upvoted 4 times

🗄️ 👤 **cloudmon** 1 year, 12 months ago

Because "You want the

Development Team to be able to read data from both Cloud Storage and BigQuery, but the External Team should only be able to read data from BigQuery."

👍 🔄 🚩 upvoted 2 times

🗄️ 👤 **cloudmon** 1 year, 12 months ago

Therefore, Cloud Storage should be the restricted API, and you add the Development Team users to the perimeter's Access Level to allow them to access the restricted API.

👍 🔄 🚩 upvoted 3 times

🗄️ 👤 **yu_** 2 years ago

why C?

I thought the development team would not be able to access BigQuery as I would include BigQuery in the service perimeter and add External Team to the access level

👍 🔄 🚩 upvoted 1 times

🗄️ 👤 **jkhong** 1 year, 11 months ago

Exactly, why would we need to consider BigQuery as a restricted service when it can already be accessed by both Dev and External team. The restricted service we are concerned with is Cloud Storage. If we go with C, we are only adding the external team into the access level... this means that the development team still wouldn't be able to access it

👍 🔄 🚩 upvoted 2 times

🗄️ 👤 **josrojgra** 2 years ago

Selected Answer: C

Answer C

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

👍 🔄 🚩 upvoted 1 times

🗄️ 👤 **TNT87** 2 years ago

Selected Answer: C

Answer C

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

👍 🔄 🚩 upvoted 4 times

[Load full discussion...](#)

Platform

- > Home
- > Examtopics PRO
- > All Exams
- > Training Courses

