

🔗 Google Discussions



Exam Professional Cloud Security Engineer All Questions

View all questions & answers for the Professional Cloud Security Engineer exam

[Go to Exam](#)

📄 EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 90 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 90

Topic #: 1

[\[All Professional Cloud Security Engineer Questions\]](#)

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.




[Show Suggested Answer](#)

by [Rantu](#) at Oct. 8, 2020, 7:43 p.m.

Comments

Type your comment...

Submit

  **jonclem** Highly Voted  4 years, 8 months 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 17 times

  **dzhu** Highly Voted  3 years, 11 months 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 11 times

  **YourFriendlyNeighborhoodSpider** Most Recent  4 months, 2 weeks ago

Selected Answer: B

B. Create access levels in Access Context Manager to prevent data exfiltration, and use a shared VPC for communication between projects.

Explanation:

Access Context Manager allows you to define access levels based on various attributes, such as the user's identity and the context of their request, which can help limit actions that could be used for data exfiltration. This setup allows you to enforce security policies around sensitive data while still allowing communication through a Shared VPC.

Shared VPC enables networking between different projects, ensuring that resources can communicate securely without exposing them to the public internet or compromising security policies.

   upvoted 1 times

  **BPzen** 8 months ago

Selected Answer: C

Explanation:

To prevent data exfiltration while allowing communication between projects, a single service perimeter is the best approach. This creates a secure boundary around all projects under the "implementation" folder, ensuring that resources within the perimeter can communicate while preventing unauthorized access or data transfer outside the perimeter. Automating the addition of new projects to the service perimeter ensures scalability and compliance with organizational security requirements.

   upvoted 1 times

  **Betotoxicity** 1 year, 4 months ago

Selected Answer: D

Similitudes con la opción C:

Uso de IaC y Cloud Function: La opción D también utiliza una herramienta de IaC (Terraform) y una Cloud Function para automatizar la creación y gestión de los service perimeters.

Monitoreo con Stackdriver y Cloud Pub/Sub: Se utiliza Stackdriver y Cloud Pub/Sub para detectar la creación de nuevos proyectos.

Diferencias con la opción C:

Cantidad de service perimeters: La opción D crea tres service perimeters diferentes (dev, staging, prod), mientras que la opción C solo crea uno.

Asignación automática de proyectos: La función Cloud de la opción D asigna automáticamente los nuevos proyectos al perímetro de servicio correspondiente. En la opción C, la asignación de proyectos a los service perimeters se debe realizar manualmente.

   upvoted 1 times

  **Sukon_Desknot** 1 year, 5 months ago

Selected Answer: D

Using Access Context Manager service perimeters provides a security boundary to prevent data exfiltration.

Separate perimeters for dev, staging, prod provides appropriate isolation.

Shared VPC allows communication between projects within the perimeter.

The Cloud Function automatically adds new projects to the right perimeter via Terraform.



This meets all requirements - security perimeter to prevent data exfiltration, communication between projects, and automatic perimeter assignment for new projects.

   upvoted 1 times

  **ssk119** 1 year, 11 months ago

just having vpc alone does not protect with data exfiltration. The correct answer is B

   upvoted 1 times

  **desertlotus1211** 1 year, 11 months ago

you'd have to re-create the projects as a Host VPC... can't do that... too much work

   upvoted 1 times

  **[Removed]** 2 years ago

Selected Answer: C

"C"

As others noted, VPC Service Controls are designed specifically to protect against the risks described in the question. Only one Service perimeter is needed which excludes "D".

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

   upvoted 2 times

  **fad3r** 2 years, 4 months ago

This question is very old. The answer is VPC Service controls.

Highly doubt this is still relevant.

   upvoted 5 times

  **soltium** 2 years, 9 months ago

Selected Answer: C

C. The keyword "prevent data exfiltration by malicious insiders or compromised code" is listed as the benefits of VPC service control

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

Only C and D creates service perimeters, but D creates three and doesn't specify a bridge to connect those service perimeters so I choose C as the answer.


   upvoted 4 times

  **AwesomeGCP** 2 years, 9 months ago

Selected Answer: C

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.

   upvoted 1 times

  **cloudprincipal** 3 years, 1 month ago

Selected Answer: C

eshtanaka is right: https://github.com/terraform-google-modules/terraform-google-vpc-service-controls/tree/master/examples/automatic_folder

   upvoted 3 times

  **sudarchary** 3 years, 6 months ago

Answer is A. Please focus on "security perimeter" and "compromised code".

   upvoted 1 times

  **eshtanaka** 3 years, 8 months 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 3 times

  **nilb94** 3 years, 11 months 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 3 times

  **desertlotus1211** 4 years, 4 months 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** 4 years, 4 months ago

Ans : A. To make the communication between different projects, shared vpc is required.

   upvoted 1 times

[Load full discussion...](#)



Platform

> [Home](#)

> [Examtopics PRO](#)

> [All Exams](#)

> [Training Courses](#)



© 2024 ExamTopics