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 211 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 211
Topic #: 1
[All Professional Cloud Security Engineer Questions]

Your organization wants to be compliant with the General Data Protection Regulation (GDPR) on Google Cloud. You must implement data residency and operational sovereignty in the EU.

What should you do? (Choose two.)

A. Limit the physical location of a new resource with the Organization Policy Service "resource locations constraint."

B. Use Cloud IDS to get east-west and north-south traffic visibility in the EU to monitor intra-VPC and inter-VPC communication.

C. Limit Google personnel access based on predefined attributes such as their citizenship or geographic location by using Key Access Justifications.

D. Use identity federation to limit access to Google Cloud resources from non-EU entities.

E. Use VPC Flow Logs to monitor intra-VPC and inter-VPC traffic in the EU.

Show Suggested Answer

by pfilourenco at *Aug. 4, 2023, 10:57 a.m.*

Comments

Type your comment...

Submit

Andrei_Z Highly Voted 1 year, 4 months ago

Selected Answer: AC

Just implemented this last month at work

upvoted 9 times

Potatoe2023 Most Recent 9 months ago

Selected Answer: AC

A & C
https://cloud.google.com/assured-workloads/key-access-justifications/docs/assured-workloads

upvoted 1 times

Bettoxicity 9 months, 4 weeks ago

Selected Answer: AD

D: Identity federation allows you to integrate your existing identity provider (IdP) with Google Cloud. This enables users to access Google Cloud resources using their existing credentials from the IdP, ideally located within the EU. By configuring access controls within your IdP, you can restrict access to Google Cloud resources from non-EU entities.

Why not C?:
Doesn't address data location.
Doesn't restrict access from non-EU entities.
Isn't a data residency measure.
Isn't an operational sovereignty measure.

upvoted 2 times

ArizonaClassics 1 year, 4 months ago

To be compliant with GDPR on Google Cloud and implement data residency and operational sovereignty in the EU, you can take the following two actions:

A. Limit the physical location of a new resource with the Organization Policy Service "resource locations constraint."

This will restrict the locations where resources in your Google Cloud organization can be deployed. You can configure this to only allow EU locations, ensuring that data remains within the EU.
C. Limit Google personnel access based on predefined attributes such as their citizenship or geographic location by using Key Access Justifications.

This can help you enforce operational sovereignty by controlling who has access to your data. Key Access Justifications can help you restrict Google personnel access based on certain attributes like geographic location, ensuring that only personnel based in the EU can access the data.

upvoted 1 times

ArizonaClassics 1 year, 5 months ago

So o, for GDPR compliance focusing on data residency and operational sovereignty in the EU, options A and C are the most relevant.

upvoted 1 times

GCBC 1 year, 5 months ago

The correct answers are A and C.

A. Limit the physical location of a new resource with the Organization Policy Service "resource locations constraint." This will ensure that all new resources are created in the EU, which is required for data residency compliance with GDPR.
C. Limit Google personnel access based on predefined attributes such as their citizenship or geographic location by using Key Access Justifications. This will help to ensure that only Google personnel who are authorized to access EU data are able to do so.

upvoted 1 times

cyberpunk21 1 year, 5 months ago

Selected Answer: AC

D is also correct if we're talking in a much bigger scope like using External IDP

upvoted 1 times

ITIFR78 1 year, 5 months ago

Selected Answer: AC

A & C - https://cloud.google.com/architecture/framework/security/data-residency-sovereignty#manage_your_operational_sovereignty

upvoted 1 times

pfilourenco 1 year, 5 months ago

Selected Answer: AC

A & C - https://cloud.google.com/architecture/framework/security/data-residency-sovereignty#manage_your_operational_sovereignty

upvoted 4 times

arpgaur 1 year, 5 months ago

C is incorrect. Key Access Justifications can be used to limit access to specific keys, but they do not prevent Google personnel from accessing other data in your Google Cloud environment.

A and D are the right answers, imo

upvoted 1 times