EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 302 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 302
Topic #: 1
[All Professional Cloud Security Engineer Questions]

You manage a Google Cloud organization with many projects located in various regions around the world. The projects are protected by the same Access Context Manager access policy. You created a new folder that will host two projects that process protected health information (PHI) for US-based customers. The two projects will be separately managed and require stricter protections. You are setting up the VPC Service Controls configuration for the new folder. You must ensure that only US-based personnel can access these projects and restrict Google Cloud API access to only BigQuery and Cloud Storage within these projects. What should you do?

A. • Create a scoped access policy, add the new folder under “Select resources to include in the policy,” and assign an administrator under “Manage principals.”
• For the service perimeter, specify the two new projects as “Resources to protect” in the service perimeter configuration.
• Set “Restricted services” to “all services,” set “VPC accessible services” to “Selected services,” and specify only BigQuery and Cloud Storage under “Selected services.”

B. • Enable Identity Aware Proxy in the new projects.
• Create an Access Context Manager access level with an “IP Subnetworks” attribute condition set to the US-based corporate IP range.
• Enable the “Restrict Resource Service Usage” organization policy at the new folder level with an “Allow” policy type and set both “storage.googleapis.com” and “bigquery.googleapis.com” under “Custom values.”

C. • Edit the organization-level access policy and add the new folder under “Select resources to include in the policy.”
• Specify the two new projects as “Resources to protect” in the service perimeter configuration.
• Set “Restricted services” to “all services,” set “VPC accessible services” to “Selected services,” and specify only BigQuery and Cloud Storage.
• Edit the existing access level to add a “Geographic locations” condition set to “US.”

D. • Configure a Cloud Interconnect connection or a Virtual Private Network (VPN) between the on-premises environment and the Google Cloud organization.
• Configure the VPC firewall policies within the new projects to only allow connections from the on-premises IP address range.
• Enable the Restrict Resource Service Usage organization policy on the new folder with an “Allow” policy type, and set both “storage.googleapis.com” and “bigquery.googleapis.com” under “Custom values.”

Show Suggested Answer

by abdelrahman89 at *Oct. 4, 2024, 10:01 p.m.*

Comments

Type your comment...

Submit

JohnDohertyDoe 7 months ago

Selected Answer: A

Editing the existing policy would affect all the projects (question clearly states there are projects all around the world). While A does not cover the US restriction, it seems to be the best answer.

upvoted 1 times

MoAk 8 months ago

Selected Answer: C

Only one that restricts access to US personnel

upvoted 1 times

nah99 8 months ago

Could it be D? Question doesn't mention on-prem, but if limiting to the US on-prem IP range, then this gets it done

upvoted 2 times

vamgcp 8 months ago

Selected Answer: C

Edits the Organization-Level Access Policy: This ensures that the stricter access controls, including the geographic location restriction, are applied to the new folder and its projects while maintaining the existing policy for other projects in the organization.
Service Perimeter: Defining the service perimeter specifically for the two new projects creates a security boundary around the PHI data, preventing data exfiltration.
Restricting Services: Limiting access to only BigQuery and Cloud Storage minimizes the potential attack surface and reduces the risk of unauthorized data access to other services.
Geographic Location Condition: By adding the "Geographic locations" condition to the existing access level, you ensure that only users accessing the resources from within the US are granted access, meeting the requirement for US-based personnel access.

upvoted 1 times

kalbd2212 8 months, 1 week ago

going with A

upvoted 1 times

kalbd2212 8 months, 1 week ago

i don't C is the right answer "Edit the existing access level to add a “Geographic locations” condition set to “US.”"

editing the exciting access policy will impact the exciting projects using it

upvoted 2 times

nah99 8 months ago

Yep, and they mention there being projects located around the world

upvoted 1 times

siheom 9 months, 3 weeks ago

Selected Answer: C

The best solution to meet the requirements of restricting access to US-based personnel and limiting Google Cloud API access to only BigQuery and Cloud Storage for the two new projects processing PHI is C.

upvoted 3 times

abdelrahman89 9 months, 3 weeks ago

C - Centralized Access Control: Editing the organization-level access policy ensures consistency and reduces the management overhead compared to creating a separate scoped policy.
VPC Service Controls for Isolation: Defining the new projects as "Resources to protect" isolates them within the service perimeter. Restricting services to "all services" and then allowing only BigQuery and Cloud Storage provides granular control over API access.
Geographic Location Restriction: Adding a "Geographic locations" condition set to "US" in the existing access level ensures that only users accessing from US locations can utilize the access policy and access these resources.

upvoted 1 times