⬅ **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 167 DISCUSSION**

Actual exam question from Google's Professional Cloud Security Engineer
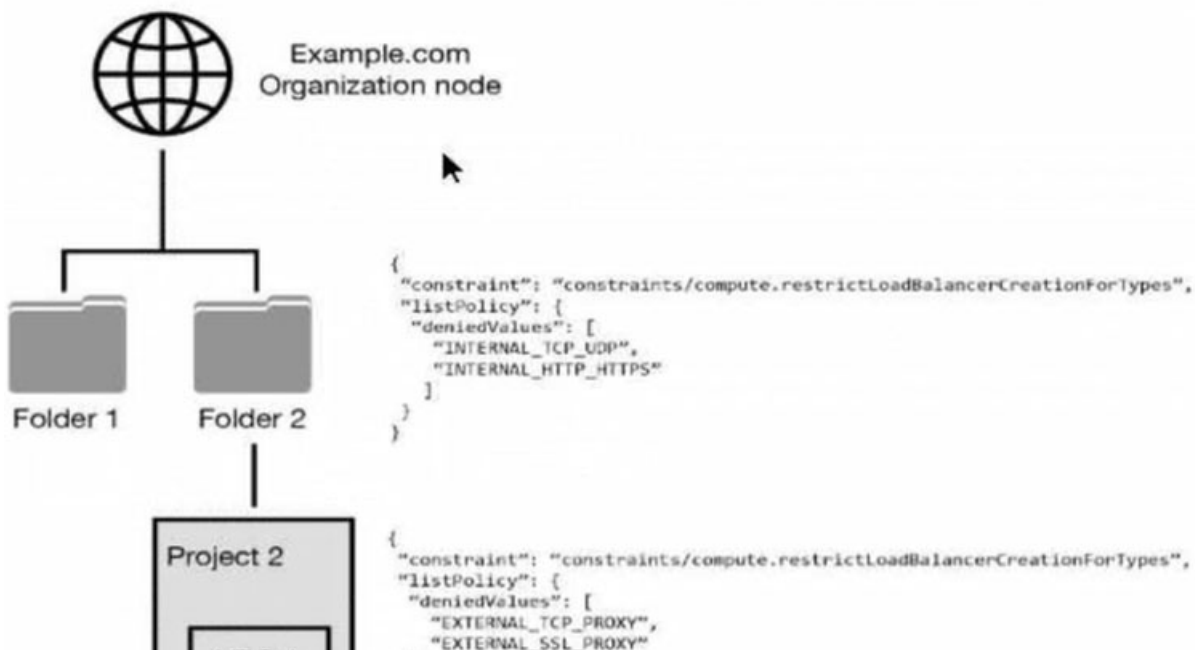
Question #: 167

Topic #: 1

[All Professional Cloud Security Engineer Questions]

You have the following resource hierarchy. There is an organization policy at each node in the hierarchy as shown. Which load balancer types are denied in VPC
A?

A. All load balancer types are denied in accordance with the global node's policy.

B. INTERNAL_TCP_UDP, INTERNAL_HTTP_HTTPS is denied in accordance with the folder's policy.

C. EXTERNAL_TCP_PROXY, EXTERNAL_SSL_PROXY are denied in accordance with the project's policy.

D. EXTERNAL_TCP_PROXY, EXTERNAL_SSL_PROXY, INTERNAL_TCP_UDP, and INTERNAL_HTTP_HTTPS are denied in accordance with the folder and project's policies.

Show Suggested Answer

by �️ tangac at *Sept. 3, 2022, 3:11 p.m.*

Comments

Type your comment...

Submit

🔲 👤 **tangac** `Highly Voted 👍` 2 years, 10 months ago

`Selected Answer: A`

the good answer is A as indicated here : https://cloud.google.com/load-balancing/docs/org-policy-constraints#gcloud

👍 ↩️ 🚩 upvoted 14 times

> 🔲 👤 **AzureDP900** 2 years, 8 months ago
>
> yes, It is A
>
> 👍 ↩️ 🚩 upvoted 3 times

🔲 👤 **mjcts** `Highly Voted 👍` 1 year, 6 months ago

`Selected Answer: A`

"inheritFromParent" param is by default set to "true" if not explicitly set

👍 ↩️ 🚩 upvoted 5 times

🔲 👤 **JohnDohertyDoe** `Most Recent ⊘` 7 months ago

`Selected Answer: D`

DENY values at a lower level override higher-level policies if they have more restrictive constraints, so answer cannot be A.

👍 ↩️ 🚩 upvoted 1 times

🔲 👤 **BPzen** 8 months ago

`Selected Answer: A`

Explanation:
The global policy applies across the entire resource hierarchy unless explicitly overridden. Because it denies all load balancer types, no load balancers can be created in VPC A. The folder and project policies are redundant in this scenario since they are less restrictive than the global policy.

👍 ↩️ 🚩 upvoted 1 times

🔲 👤 **kalbd2212** 8 months, 2 weeks ago

Outcome:

Both the folder-level and project-level denials will be enforced. This is because they apply to different types of traffic and don't conflict with each other. Essentially, the restrictions are combined.

Key Concepts

Inheritance: Policies are inherited down the hierarchy. A project inherits policies from its parent folder, and the folder inherits from the organization.
Overriding: A lower level policy can override a higher-level policy only if it is more restrictive.
Constraints: Organization Policies use "constraints" to define restrictions.

1 In your case, the constraints are likely related to VPC firewall rules.

👍 ↩ 🏳 upvoted 1 times

⊟ 👤 **luamail78** 9 months ago

Selected Answer: D

https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints
the org constrain is nor a valid value

👍 ↩ 🏳 upvoted 1 times

⊟ 👤 **nah99** 8 months, 1 week ago

https://cloud.google.com/resource-manager/reference/rest/v1/Policy#allvalues

👍 ↩ 🏳 upvoted 1 times

⊟ 👤 **oezgan** 1 year, 4 months ago

i asked Gemini here is the answer: In the scenario you described, the following load balancer types would be denied in a VPC defined within the project in the subfolder:

external_tcp_proxy
external_ssl_proxy
Here's the breakdown of how Org policy constraints are enforced with inheritance:

Organization Level Constraint: This denies all load balancers.
Subfolder Constraint: This overrides the organization-level constraint and only denies internal_tcp_udp and internal_http_https load balancers.
Project Level Constraint: This further refines the allowed types within the subfolder by denying external_tcp_proxy and external_ssl_proxy load balancers.

👍 ↩ 🏳 upvoted 1 times

⊟ 👤 **Nachtwaker** 1 year, 4 months ago

Selected Answer: D

Policies are inherited, so folder and project must be merged. Keep in mind, deny policies are always applied, and when conflicting with an allow policy the deny has higher prio and will overrule the allow. So, merge all the deny policies and the result is D.

👍 ↩ 🏳 upvoted 2 times

⊟ 👤 **pbrvgl** 1 year, 8 months ago

My option is A. If "inheritFromParent" is not explicitly set, the default behavior in GCP if for inheritance to prevail. Based on this assumption, the project inherits from the folder and the organization above, all constraints are merged at the project level.

👍 ↩ 🏳 upvoted 4 times

⊟ 👤 **mjcts** 1 year, 6 months ago

This is correct

👍 ↩ 🏳 upvoted 2 times

⊟ 👤 **steveurkel** 1 year, 8 months ago

Answer is C..
If the policy is set to merge with parent, the json output will show:
"inheritFromParent": true
If the policy is set to replace the parent policy, that line is missing, which is the same as the output in the diagram.
Therefore, the parent policy is replaced with the child policies and only the project level conditions are in effect.

👍 ↩ 🏳 upvoted 1 times

⊟ 👤 **desertlotus1211** 1 year, 10 months ago

The issue we don't know what the value is of 'inheritFromParent'. Is it false of true?
If true then A is correct.... if false then C is correct

👍 ↩ 🏳 upvoted 1 times

⊟ 👤 **WheresWally** 2 years, 2 months ago

The answer should be C
Link: https://cloud.google.com/resource-manager/docs/organization-policy/understanding-hierarchy
Inheritance
A resource node that has an organization policy set by default supersedes any policy set by its parent nodes in the hierarchy.
However, if a resource node has set inheritFromParent = true, then the effective Policy of the parent resource is inherited, merged, and reconciled to evaluate the resulting effective policy.
Project 2 has an organisation policy set and there's no mention of any inheritance.

👍 ↩ 🏳 upvoted 3 times

⊟ 👤 **gcpengineer** 2 years, 2 months ago

why do u assume inheritance is false here?

👍 ↩ 🏳 upvoted 1 times

gcpengineer 2 years, 2 months ago

Deny take precendence

👍 ↩ 🏳 upvoted 1 times

---

hxhwing 2 years, 6 months ago

Selected Answer: C

Project is not inheriting from parent policy, but customize its own

👍 ↩ 🏳 upvoted 4 times

---

madhu81321 2 years, 8 months ago

Selected Answer: D

There are restrictions at folder level too.

👍 ↩ 🏳 upvoted 2 times

TheBuckler 2 years, 9 months ago

NVM - the answer actually is A. The Org has it's own restrictions too!

👍 ↩ 🏳 upvoted 3 times

> **Table2022** 2 years, 9 months ago
>
> Agreed with A, good one!
>
> 👍 ↩ 🏳 upvoted 2 times

TheBuckler 2 years, 9 months ago

The answer is D. We also need to consider the Load Balancer types that are restricted at the Folder level as well as the Project level.

👍 ↩ 🏳 upvoted 2 times

[Removed] 2 years, 10 months ago

Selected Answer: A

It's A.

👍 ↩ 🏳 upvoted 2 times