

 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 221 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 221

Topic #: 1

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

You define central security controls in your Google Cloud environment. For one of the folders in your organization, you set an organizational policy to deny the assignment of external IP addresses to VMs. Two days later, you receive an alert about a new VM with an external IP address under that folder.

What could have caused this alert?

- A. The VM was created with a static external IP address that was reserved in the project before the organizational policy rule was set.
- B. The organizational policy constraint wasn't properly enforced and is running in "dry run" mode.
- C. A project level, the organizational policy control has been overwritten with an "allow" value.
- D. The policy constraint on the folder level does not have any effect because of an "allow" value for that constraint on the organizational level.

[Show Suggested Answer](#)

by  [gcp4test](#) at Aug. 4, 2023, 2:41 p.m.

## Comments

Type your comment...

  **1209apl** 3 months, 2 weeks ago

**Selected Answer: C**

As other mentions, Org policies are not retroactive. But, the external IP assignment would be done after the Org policy was set. It is then, when the policy will prevent the VM to get assigned an External IP. That's why option A is not the right answer. However, as option C mentions, you can override the policy at project level to be more permissive, which would allow you to create new instances with external IP associated.

   upvoted 1 times

  **YourFriendlyNeighborhoodSpider** 4 months, 1 week ago

**Selected Answer: A**

- :Enforcement of most organization policies is not retroactive
- The policies are merged and the DENY value takes precedence ([https://cloud.google.com/resource-manager/docs/organization-policy/understanding-hierarchy#reconciling\\_policy\\_conflicts](https://cloud.google.com/resource-manager/docs/organization-policy/understanding-hierarchy#reconciling_policy_conflicts))



   upvoted 1 times

  **KLei** 7 months ago

**Selected Answer: A**

- :Enforcement of most organization policies is not retroactive
- The policies are merged and the DENY value takes precedence ([https://cloud.google.com/resource-manager/docs/organization-policy/understanding-hierarchy#reconciling\\_policy\\_conflicts](https://cloud.google.com/resource-manager/docs/organization-policy/understanding-hierarchy#reconciling_policy_conflicts))


   upvoted 2 times

  **Pime13** 7 months, 3 weeks ago

**Selected Answer: A**

[https://cloud.google.com/resource-manager/docs/organization-policy/creating-managing-policies#creating\\_and\\_editing\\_policies](https://cloud.google.com/resource-manager/docs/organization-policy/creating-managing-policies#creating_and_editing_policies)

Enforcement of most organization policies is not retroactive. If a new organization policy sets a restriction on an action or state that a service is already in, the policy is considered to be in violation, but the service will not stop its original behavior. Organization policy constraints that are retroactive note this property in their description.

   upvoted 2 times

  **BPzen** 8 months ago

**Selected Answer: A**

When you define an organizational policy in Google Cloud, it applies to future actions and configurations, not to resources that already exist or were configured before the policy was set. If a static external IP address had been reserved in the project prior to the policy being applied, it could be assigned to a new VM after the policy enforcement starts. This would result in a VM with an external IP address, despite the organizational policy.

C. A project-level organizational policy control has been overwritten with an "allow" value.

Organizational policies propagate from the top (organization) to the bottom (project), unless specifically overridden. However, the question specifies the policy was applied at the folder level, which would affect all projects under that folder. This is less likely unless explicitly overridden at the project level, which the question does not suggest.

   upvoted 2 times


  **MoAk** 8 months ago

**Selected Answer: B**

Tricky one tbh. dry-run mode for org policies now exist and so technically speaking, answer B could now be the answer to the Q. Either way its between B or C in my opinion.



<https://cloud.google.com/resource-manager/docs/organization-policy/dry-run-policy>

   upvoted 3 times

  **shmoeee** 1 year, 4 months ago

"under that folder"...

   upvoted 1 times

  **desertlotus1211** 1 year, 5 months ago

Answer A:

f a static external IP address was reserved before the organizational policy to deny the assignment of external IP addresses to VMs was enacted, creating a VM and attaching this pre-reserved static external IP address would not violate the policy.

   upvoted 2 times

  **winston9** 1 year, 6 months ago

**Selected Answer: D**

in this scenario, the alert is triggered because the VM creation violates the folder level "deny" policy, but that restriction is

In this scenario, the alert is triggered because the VM creation violates the folder-level "deny" policy, but that restriction is nullified by the overriding "allow" value inherited from the organization-level policy.

   upvoted 1 times

  **winston9** 1 year, 5 months ago

I will change it to A, usually organization policy constraints are not retroactive, it could be retroactively enforced if properly labeled as such on the Organization Policy Constraints page, but the question does not mention this.

   upvoted 1 times

  **MMNB2023** 1 year, 8 months ago

**Selected Answer: A**

According to this link <https://cloud.google.com/compute/docs/ip-addresses/reserve-static-external-ip-address#disableexternalip>

   upvoted 2 times

  **MMNB2023** 1 year, 8 months ago

Sorry the right answer is C. We talk about a "new VM" in the question.

   upvoted 1 times

  **MMNB2023** 1 year, 8 months ago

I think A is correct answer. Because this policy organization is not retroactive. <https://cloud.google.com/compute/docs/ip-addresses/reserve-static-external-ip-address#disableexternalip>

   upvoted 1 times

  **MisterHairy** 1 year, 8 months ago

**Selected Answer: C**

The correct answer is C. At a project level, the organizational policy control has been overwritten with an "allow" value.

Policies can be overridden at a lower level (like a project). So, if an "allow" policy was set at the project level, it would override the "deny" policy set at the folder level. This could allow a VM with an external IP address to be created under that folder, despite the folder-level policy.



Changes to organizational policies can take time to propagate and be enforced across all resources, but in this case, the alert was received two days after the policy was set, which should have been sufficient time for the policy to take effect. Therefore, options A, B, and D are less likely.

   upvoted 2 times

  **EVEGCP** 1 year, 8 months ago

A: Enforcement of most organization policies is not retroactive. If a new organization policy sets a restriction on an action or state that a service is already in, the policy is considered to be in violation, but the service will not stop its original behavior. [https://cloud.google.com/resource-manager/docs/organization-policy/creating-managing-policies#creating\\_and\\_editing\\_policies](https://cloud.google.com/resource-manager/docs/organization-policy/creating-managing-policies#creating_and_editing_policies)

   upvoted 2 times

  **vividg** 1 year, 10 months ago

[https://cloud.google.com/resource-manager/docs/organization-policy/understanding-hierarchy#reconciling\\_policy\\_conflicts](https://cloud.google.com/resource-manager/docs/organization-policy/understanding-hierarchy#reconciling_policy_conflicts) Says "The policies are merged and the DENY value takes precedence"

So.. How can C be the answer?

   upvoted 4 times

  **daidai75** 1 year, 3 months ago

This scenario happens when "inheritFromParent = true". If "inheritFromParent = false", the "reconciling\_policy\_conflicts" rule will not work.

   upvoted 1 times

  **Xoxoo** 1 year, 10 months ago

**Selected Answer: C**

Here's why option C is the likely cause:

Overriding Policy at the Project Level: Google Cloud allows for policies to be set at different levels of the resource hierarchy, such as the organization, folder, or project level. If a policy is set at the organization or folder level to deny external IP addresses but is then overridden with an "allow" value at the project level, it would take precedence, allowing VMs within that project to have external IP addresses.

Alert Trigger: When an organizational policy constraint is overridden at a lower level (e.g., project), it can lead to situations where the policy is not enforced as expected. This can result in alerts or notifications when policy violations occur.

   upvoted 3 times

  **cyberpunk21** 1 year, 11 months ago

**Selected Answer: C**

- A. Even if IP created after org policy was set it wont allow to use it
- B. we can preview the org policy function using dry run (Preview mode) in this policy won't deny the usage, but it will notify.
- C. we cant put deny org policy at org policy and expect it will override with allow value

👍 ↩ 🚩 upvoted 3 times

🗂️ 👤 **Simon6666** 1 year, 11 months ago

**Selected Answer: C**

C should be correct

<https://cloud.google.com/resource-manager/docs/organization-policy/understanding-hierarchy>

👍 ↩ 🚩 upvoted 2 times

[Load full discussion...](#)



## Platform

> Home

> Examtopics PRO

> All Exams

> Training Courses



© 2024 ExamTopics