



- Expert Verified, Online, **Free**.

 MENU



Google Discussions



Exam Associate Cloud Engineer All Questions

View all questions & answers for the Associate Cloud Engineer exam

[Go to Exam](#)

EXAM ASSOCIATE CLOUD ENGINEER TOPIC 1 QUESTION 111 DISCUSSION

Actual exam question from Google's Associate Cloud Engineer

Question #: 111

Topic #: 1

[\[All Associate Cloud Engineer Questions\]](#)

Your management has asked an external auditor to review all the resources in a specific project. The security team has enabled the Organization Policy called Domain Restricted Sharing on the organization node by specifying only your Cloud Identity domain. You want the auditor to only be able to view, but not modify, the resources in that project. What should you do?

- A. Ask the auditor for their Google account, and give them the Viewer role on the project.
- B. Ask the auditor for their Google account, and give them the Security Reviewer role on the project.
- C. Create a temporary account for the auditor in Cloud Identity, and give that account the Viewer role on the project.
- D. Create a temporary account for the auditor in Cloud Identity, and give that account the Security Reviewer role on the project.

[Show Suggested Answer](#)

by  **SIX** at June 5, 2020, 5:42 p.m.

Comments

Type your comment...

[Submit](#)

dan80 **Highly Voted** 4 years, 4 months ago

C - https://cloud.google.com/iam/docs/roles-audit-logging#scenario_external_auditors

upvoted 52 times

spudleymcdudley 4 years, 3 months ago

This guy is right!

upvoted 7 times

ESP_SAP **Highly Voted** 4 years, 2 months ago

Correct Answer is (C):

roles/viewer Read access to all resources. Get and list access for all resources.

Using primitive roles

The following table lists the primitive roles that you can grant to access a project, the description of what the role does, and the permissions bundled within that role. Avoid using primitive roles except when absolutely necessary. These roles are very powerful, and include a large number of permissions across all Google Cloud services. For more details on when you should use primitive roles, see the Identity and Access Management FAQ.

IAM predefined roles are much more granular, and allow you to carefully manage the set of permissions that your users have access to. See Understanding Roles for a list of roles that can be granted at the project level. Creating custom roles can further increase the control you have over user permissions.

https://cloud.google.com/resource-manager/docs/access-control-proj#using_primitive_roles

upvoted 21 times

kayceec **Most Recent** 4 months ago

Selected Answer: C

the key word is "organisation Policy called Domain Restricted sharing." his external google account wont work

upvoted 1 times

Ankit_EC_ran 7 months, 1 week ago

Selected Answer: C

CORRECT ANSWER IS C

upvoted 1 times

ogerber 10 months, 3 weeks ago

Selected Answer: C

Domain Restricted Sharing: Since your organization has the Domain Restricted Sharing policy enabled, sharing resources with accounts outside your Cloud Identity domain isn't allowed. Therefore, options A and B, which involve using the auditor's Google account, aren't feasible.

upvoted 3 times

kelliott 10 months, 4 weeks ago

C, without doubt

upvoted 1 times

thewalker 11 months ago

Selected Answer: D

D

As per the documentation, Security Reviewer is more narrow role than the basic Viewer role:

<https://cloud.google.com/iam/docs/understanding-roles#iam.securityReviewer>

<https://cloud.google.com/iam/docs/understanding-roles#viewer>

upvoted 2 times

Rahaf99 11 months, 1 week ago

Selected Answer: C

It could be A, But C is more practical and you don't have to give the auditor extra 3 seconds of work, and yourself for deleting him after he finishes

upvoted 3 times

BAofBK 11 months, 2 weeks ago

The correct answer is C

upvoted 1 times

scanner2 1 year, 1 month ago

Selected Answer: C

The Resource Manager provides a domain restriction constraint that can be used in organization policies to limit resource sharing based on domain or organization resource. This constraint allows you to restrict the set of identities that are allowed to be used in Identity and Access Management policies.

Organization policies can use this constraint to limit resource sharing to identities that belong to a particular organization resource.

<https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains>

? ? ? upvoted 1 times

? ? Captain1212 1 year, 1 month ago

Selected Answer: C

C is more correct

? ? ? upvoted 1 times

? ? Neha_Pallavi 1 year, 1 month ago

Correct Answer is (C):

? ? ? upvoted 1 times

? ? WendyLC 1 year, 4 months ago

Selected Answer: C

Correct Answer is (C):

Answer A is wrong because we can't use the the auditor Google account, security team has enabled the Organization Policy specifying only one Cloud Identity domain.

? ? ? upvoted 1 times

? ? Shenannigan 1 year, 5 months ago

Selected Answer: C

Answer is definitely C

Please review this as it seems to be looked over in the other comments

<https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains>

(a google account that isn't part of the domain will not work unless you specifically allow exceptions at the project level and that was not defined in the answers)

? ? ? upvoted 1 times

? ? sabrinakloud 1 year, 6 months ago

Selected Answer: C

i believe it is C

? ? ? upvoted 1 times

? ? thaliath 1 year, 9 months ago

Correct answer is C. A is not correct. You can not ask someone to create a personal google account. He/she has no obligation to do so

? ? ? upvoted 1 times

? ? alex000 1 year, 9 months ago

Selected Answer: A

From: https://cloud.google.com/iam/docs/job-functions/auditing#scenario_external_auditors

"The organization creates a Google group for these external auditors and adds the current auditor to the group. This group is monitored and is typically granted access to the dashboard application.

During normal access, the auditors' Google group is only granted access to view the historic logs stored in BigQuery. If any anomalies are discovered, the group is granted permission to view the actual Cloud Logging Admin Activity logs via the dashboard's elevated access mode. At the end of each audit period, the group's access is then revoked."

? ? ? upvoted 2 times

[Load full discussion...](#)

Start Learning for free



Social Media

Facebook , Twitter

YouTube , Reddit

Pinterest



We are the biggest and most updated IT certification exam material website.

Using our own resources, we strive to strengthen the IT professionals community for free.



© 2024 ExamTopics

ExamTopics doesn't offer Real Microsoft Exam Questions. ExamTopics doesn't offer Real Amazon Exam Questions. ExamTopics Materials do not contain actual questions and answers from Cisco's Certification Exams.

CFA Institute does not endorse, promote or warrant the accuracy or quality of ExamTopics. CFA® and Chartered Financial Analyst® are registered trademarks owned by CFA Institute.