Google Discussions

EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 14 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 14
Topic #: 1
[All Professional Cloud Security Engineer Questions]

A business unit at a multinational corporation signs up for GCP and starts moving workloads into GCP. The business unit creates a Cloud Identity domain with an organizational resource that has hundreds of projects.
Your team becomes aware of this and wants to take over managing permissions and auditing the domain resources.
Which type of access should your team grant to meet this requirement?

A. Organization Administrator

B. Security Reviewer

C. Organization Role Administrator

D. Organization Policy Administrator

Show Suggested Answer

by mozammil89 at *March 19, 2020, 3:59 p.m.*

Comments

Type your comment...

Submit

ffdd1234 Highly Voted 4 years, 6 months ago

Answer A > Its the only one that allow you to manage permissions on the projects
answer B > dont have any iam set permission so is not correct
C > organizationRoleAdmin let you only create custom roles, you cant assign it to anyone (so with thisone you cant manage permissions just create roles)
D> org policyes are for manage the ORG policies constrains , that is not about project permissions,
for me the correct is A

upvoted 29 times

zanhsieh Highly Voted 4 years, 7 months ago

C. After carefully review this link:
https://cloud.google.com/iam/docs/understanding-roles
my opinion is based on 'the least privilege' practice, that future domain shall not get granted automatically:
A - Too broad permissions. The question asked "The business unit creates a Cloud Identity domain..." does not imply your team should be granted for ALL future domain(s) (domain = folder) permission management.
B - Security Reviewer does not have "set*" permission. All this role could do is just looking, not management.
C - The best answer so far. Only the domain current created and underneath iam role assignment as well as change.
D - Too broad permissions on the organization level. In other words, this role could make policy but future domains admin could hijack the role names / policies to do not desired operations.

upvoted 12 times

zzaric 3 years, 3 months ago

C - can't do a job - they have to manage the IAP permissions, C doesn't have setIAM permissions and the role is only for creating Custom Roles - see the permissions that it contains:

iam.roles.create
iam.roles.delete
iam.roles.get
iam.roles.list
iam.roles.undelete
iam.roles.update
resourcemanager.organizations.get
resourcemanager.organizations.getIamPolicy
resourcemanager.projects.get
resourcemanager.projects.getIamPolicy
resourcemanager.projects.list

upvoted 6 times

zzaric 3 years, 3 months ago

IAM - not IAP - typo

upvoted 1 times

Loved 2 years, 8 months ago

"If you have an organization associated with your Google Cloud account, the Organization Role Administrator role enables you to administer all custom roles in your organization", it can not be C

upvoted 2 times

PankajKapse Most Recent 10 months, 2 weeks ago

Selected Answer: A

as mentioned by ffdd1234's answer

upvoted 1 times

dija123 1 year, 4 months ago

Selected Answer: A

A. Organization Administrato

upvoted 1 times

okhascorpio 1 year, 9 months ago

gpt says both A. and C can be used. I don't know, too many similar answers, cant say for certain which one is correct answer anymore. How can one pass the exam like this????

upvoted 1 times

aliounegdiop 1 year, 10 months ago

A. Organization Administrator

Here's why:

Organization Administrator: This role provides full control over all resources and policies within the organization, including permissions and auditing. It allows your team to manage permissions, policies, and configurations at the organizational level, making it the most appropriate choice when you need comprehensive control.

Security Reviewer: This role focuses on reviewing and assessing security configurations but doesn't grant the level of control

needed for managing permissions and auditing at the organizational level.

Organization Role Administrator: This role allows management of IAM roles at the organization level but doesn't provide control over policies and auditing.

Organization Policy Administrator: This role allows for the management of organization policies, but it doesn't cover permissions and auditing.

upvoted 3 times

elad17 2 years, 3 months ago

Selected Answer: A

A is the only role that gives you management permissions and not just viewing / role editing.

upvoted 4 times

Ishu_awsguy 2 years, 6 months ago

i would go with A. Audit of all domain resources might have a very broad scope and C might not have those permissions. Because it is audit , i believe its a responsible job so A can be afforded

upvoted 2 times

GCP72 2 years, 11 months ago

Selected Answer: C

The correct answer is C

upvoted 1 times

Medofree 3 years, 3 months ago

Answer is A, among the 4, it is the only role able de manage permissions

upvoted 3 times

Lancyqusa 3 years, 7 months ago

The answer must be A - check out the example that allows the CTO to setup permissions for the security team: https://cloud.google.com/iam/docs/job-functions/auditing#scenario_operational_monitoring

upvoted 2 times

OSNG 3 years, 11 months ago

Its A.
They are looking for Domain Resources Management i.e. Projects, Folders, Permissions. and only Organization Administrator is the only option allows it. Moreover, Organization Administrator is the only option that falls under "Used IN: Resource Manager"
roles/resourcemanager.organizationAdmin

upvoted 1 times

[Removed] 4 years, 4 months ago

C is the answer.
Here are the permissions available to organizationRoleAdmin

iam.roles.create
iam.roles.delete
iam.roles.undelete
iam.roles.get
iam.roles.list
iam.roles.update
resourcemanager.projects.get
resourcemanager.projects.getIamPolicy
resourcemanager.projects.list
resourcemanager.organizations.get
resourcemanager.organizations.getIamPolicy

There are sufficient as per least privilege policy. You can do user management as well as auditing.

upvoted 5 times

DebasishLowes 4 years, 4 months ago

Ans : D. As it's related to Resources, so definitely policy comes into picture.

upvoted 1 times

HateMicrosoft 4 years, 5 months ago

Correct is D
https://cloud.google.com/resource-manager/docs/organization-policy/overview

upvoted 2 times

BhupalS 4 years, 7 months ago

Role Permissions
roles/iam.organizationRoleAdmin iam.roles.create

iam.roles.delete
iam.roles.undelete
iam.roles.get
iam.roles.list
iam.roles.update
resourcemanager.projects.get
resourcemanager.projects.getIamPolicy
resourcemanager.projects.list
resourcemanager.organizations.get
resourcemanager.organizations.getIamPolicy

upvoted 1 times

FatCharlie 4 years, 8 months ago

The confusion here, in my opinion, is that the question is asking for the ability to manage roles & audit _DOMAIN_ resources.

Domain resources in the GCP hierarchy are folders & projects, because those are the only things that can be directly under an Organization (aka Domain).

The Organization Role Admin is the option that gives you the ability to manage custom roles & list folders & projects.

upvoted 5 times

Load full discussion...