EXAM ASSOCIATE CLOUD ENGINEER TOPIC 1 QUESTION 1 DISCUSSION

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

Every employee of your company has a Google account. Your operational team needs to manage a large number of instances on Compute Engine. Each member of this team needs only administrative access to the servers. Your security team wants to ensure that the deployment of credentials is operationally efficient and must be able to determine who accessed a given instance. What should you do?

A. Generate a new SSH key pair. Give the private key to each member of your team. Configure the public key in the metadata of each instance.

B. Ask each member of the team to generate a new SSH key pair and to send you their public key. Use a configuration management tool to deploy those keys on each instance.

C. Ask each member of the team to generate a new SSH key pair and to add the public key to their Google account. Grant the ι€compute.osAdminLoginι€ role to the Google group corresponding to this team.

D. Generate a new SSH key pair. Give the private key to each member of your team. Configure the public key as a project-wide public SSH key in your Cloud Platform project and allow project-wide public SSH keys on each instance.

Show Suggested Answer

by zakhili at *May 31, 2020, 9:40 p.m.*

Comments

Type your comment...

Submit

dan80 Highly Voted 1 month ago

C is correct - https://cloud.google.com/compute/docs/instances/managing-instance-access

upvoted 81 times

adedj99 1 month ago

We recommend collecting users with the same responsibilities into groups and assigning IAM roles to the groups rather than to individual users. For example, you can create a "data scientist" group and assign appropriate roles to enable interaction with BigQuery and Cloud Storage. When a new data scientist joins your team, you can simply add them to the group and they will inherit the defined permissions. You can create and manage groups through the Admin Console.

upvoted 15 times

zakhili Highly Voted 4 years, 4 months ago

Send private key to users is not safe, i think it's C

upvoted 22 times

aarthi_13 Most Recent 3 weeks, 6 days ago

. Which Kubernetes component would you use to ensure traffic is correctly routed to pods running your application?
A. Pod router
B. Deployment
C. Service
D. PersistentIPClaim

Cloud anyone please tell me the answer?

upvoted 1 times

ryan_m 3 years, 1 month ago

C. Service

upvoted 2 times

Buruguduystunstugudunstuy 3 weeks, 6 days ago

Selected Answer: C

Option C is correct because asking each member of the team to generate a new SSH key pair and to add the public key to their Google account allows the security team to manage the deployment of credentials efficiently.

It also allows the security team to determine who accessed a given instance because the public key is associated with the Google account of the user.

Granting the "compute.osAdminLogin" role to the Google group corresponding to this team ensures that all members of the team have administrative access to the servers.

upvoted 5 times

JohnPhan 3 weeks, 6 days ago

Selected Answer: C

C is correct
In this scenario, granting the "compute.osAdminLogin" role to a Google group corresponding to the operational team would be the best option. This role would provide each team member with administrative access to instances, and by adding their public key to their Google account, they can use it to authenticate their access to instances without the need for a separate key management system. Additionally, the security team's requirement for auditing access can be met by using Cloud Audit Logging to log all access to the instances.

upvoted 5 times

ovokpus 3 weeks, 6 days ago

Selected Answer: C

Avoiding the other options:

Distributing a single private key to multiple members is not a best practice as it doesn't provide individual accountability.
Manually deploying public keys on each instance using a configuration management tool can be cumbersome and doesn't provide the flexibility and integration that Google's IAM provides.
By following the recommended approach, the organization can maintain a secure, traceable, and efficient method for managing access to Compute Engine instances.

upvoted 1 times

noopy 3 weeks, 6 days ago

Selected Answer: C

C is the most appropriate. In this option, each team member generates their own SSH key pair and adds the public key to their Google account. By granting the `compute.osAdminLogin` role to the corresponding Google group for this team, security is enhanced, and operational efficiency is improved. This setup also allows precise tracking of which member accessed which instance.

upvoted 3 times

harsh5kalsait 3 weeks, 6 days ago

Best Choice: C

Option C is the best approach because it uses Google Cloud IAM roles to control access, integrates with Google accounts for individual credential management, and supports efficient auditing and access tracking. Each user will have their own SSH key, and their actions can be traced through IAM logs, providing both security and accountability.

upvoted 2 times

BhooChaal 2 months ago

There is something which you must know. NEVER SHARE PRIVATE KEY.

upvoted 2 times

Greg1102 3 months ago

Why in the world would I give the private key to each member of my team. The answer is C

upvoted 1 times

subha.elumalai 5 months ago

D https://cloud.google.com/compute/docs/instances/adding-removing-ssh-keys

upvoted 1 times

keybin 6 months, 2 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

7b00725 6 months, 3 weeks ago

Selected Answer: C

C is Correct

upvoted 1 times

Viswanathan83 7 months, 3 weeks ago

C is correct

upvoted 1 times

pumajd 7 months, 3 weeks ago

Selected Answer: D

Because they need administrative access only on the machines

upvoted 1 times

Ele24 8 months ago

Selected Answer: C

C is Correct

upvoted 1 times

beginnercloud 8 months, 1 week ago

Selected Answer: C

C is correct

upvoted 1 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.