EXAMTOPICS

- Expert Verified, Online, Free.

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 206 DISCUSSION

Actual exam question from Google's Associate Cloud Engineer

Question #: 206

Topic #: 1

[All Associate Cloud Engineer Questions]

You have two subnets (subnet-a and subnet-b) in the default VPC. Your database servers are running in subnet-a. Your application servers and web servers are running in subnet-b. You want to configure a firewall rule that only allows database traffic from the application servers to the database servers. What should you do?

A. • Create service accounts sa-app and sa-db.
• Associate service account sa-app with the application servers and the service account sa-db with the database servers.
• Create an ingress firewall rule to allow network traffic from source service account sa-app to target service account sa-db.

B. • Create network tags app-server and db-server.
• Add the app-server tag to the application servers and the db-server tag to the database servers.
• Create an egress firewall rule to allow network traffic from source network tag app-server to target network tag db-server.

C. • Create a service account sa-app and a network tag db-server.
• Associate the service account sa-app with the application servers and the network tag db-server with the database servers.
• Create an ingress firewall rule to allow network traffic from source VPC IP addresses and target the subnet-a IP addresses.

D. • Create a network tag app-server and service account sa-db.
• Add the tag to the application servers and associate the service account with the database servers.
• Create an egress firewall rule to allow network traffic from source network tag app-server to target service

... Create an egress firewall rule to allow network traffic from source network tag app-server to target service account sa-db.

Show Suggested Answer

by ⍰georgesouzafarias at *June 23, 2023, 6:38 p.m.*

Comments

Type your comment...

Submit

⍰ ⍰scanner2 `Highly Voted ⍰` 1 year, 1 month ago

`Selected Answer: A`

Both service accounts and network tags can be used for creating a Cloud Firewall rule. The prime word is "to allow network traffic from app server to database server" which is achievable by inbound/ingress rule and not egress rule.
https://cloud.google.com/firewall/docs/firewalls#rule_assignment

⍰ ⍰ ⍰ upvoted 5 times

⍰ ⍰Enamfrancis `Most Recent ⍰` 3 weeks, 5 days ago

`Selected Answer: A`

A IS CORRECT

⍰ ⍰ ⍰ upvoted 1 times

⍰ ⍰Ciupaz 1 month ago

`Selected Answer: B`

By specifying the source and target tags in the firewall rule, you can ensure that only traffic from instances with the app-server tag can reach instances with the db-server tag.

⍰ ⍰ ⍰ upvoted 1 times

⍰ ⍰MariaDoss 10 months, 1 week ago

`Selected Answer: A`

the answer is A

⍰ ⍰ ⍰ upvoted 2 times

⍰ ⍰GP123123 11 months ago

for "allow" rules, restrict them to only allow specific virtual machines by specifying the virtual machine's service account

Refer to https://cloud.google.com/firewall/docs/firewalls

⍰ ⍰ ⍰ upvoted 3 times

⍰ ⍰GP123123 11 months ago

Answer is A

⍰ ⍰ ⍰ upvoted 2 times

⍰ ⍰carlalap 11 months, 1 week ago

Answer is B.
Network tags can be simpler to manage, especially if the access control is based on broader categories (like application servers and database servers) rather than individual instances.
If you need fine-grained control and identity-based access, go with service accounts. If you prefer simplicity and broader categorization, network tags may be a suitable choice.

⍰ ⍰ ⍰ upvoted 1 times

⍰ ⍰carlalap 11 months, 1 week ago

Although what was previously stated is correct, I must correct it. The correct answer would be option A. Creating an ingress firewall rule on the subnet where your database servers are located is the appropriate approach. This rule would control incoming traffic to the database servers, ensuring that only traffic from the specified application servers (identified by network tags or service accounts) is allowed.

⍰ ⍰ ⍰ upvoted 1 times

⍰ ⍰Captain1212 1 year, 1 month ago

`Selected Answer: A`

Answer A is correct as question demands traffic to application to database which can be only be achieved by the ingreess ...

Answer A is correct as question demands traffic to application to database which can be only be achieved by the ingreess rule

☐ ☐ ☐ upvoted 4 times

☐ ☐ tatyavinchu 1 year, 2 months ago

Correct Answer is A

☐ ☐ ☐ upvoted 1 times

☐ ☐ 3arle 1 year, 2 months ago

Selected Answer: A

From the TomFoot link
'for example, allow my "application x" servers to access my "database y."'

☐ ☐ ☐ upvoted 1 times

☐ ☐ juliorevk 1 year, 2 months ago

Selected Answer: B

Even though you could use service accounts for firewall rules, why is B wrong? It seems to do what the question requests and is the standard method.

☐ ☐ ☐ upvoted 3 times

☐ ☐ Ahmed_Y 1 year, 2 months ago

Because we need an ingress firewall.

☐ ☐ ☐ upvoted 3 times

☐ ☐ _F4LLEN_ 1 year, 3 months ago

Selected Answer: A

Service accs can be used for firewall management.

☐ ☐ ☐ upvoted 1 times

☐ ☐ TomFoot 1 year, 3 months ago

Selected Answer: A

You can use service for firewall rules.

https://cloud.google.com/blog/products/gcp/simplify-cloud-vpc-firewall-management-with-service-accounts

☐ ☐ ☐ upvoted 2 times

☐ ☐ gpais 1 year, 3 months ago

Selected Answer: A

A seems to be the most appropriate: https://cloud.google.com/firewall/docs/firewalls

☐ ☐ ☐ upvoted 2 times

☐ ☐ gpais 1 year, 3 months ago

A seems to be the most appropriate: https://cloud.google.com/firewall/docs/firewalls

☐ ☐ ☐ upvoted 2 times

☐ ☐ georgesouzafarias 1 year, 4 months ago

Selected Answer: B

Service account? It doesn't make any sense.
It's clearly a firewall solution.

☐ ☐ ☐ upvoted 3 times

☐ ☐ TomFoot 1 year, 3 months ago

You can use service for firewall rules.

https://cloud.google.com/blog/products/gcp/simplify-cloud-vpc-firewall-management-with-service-accounts

☐ ☐ ☐ upvoted 2 times

Social Media

Facebook , Twitter
YouTube , Reddit
Pinterest

EXAMTOPICS

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.