Google Discussions

EXAM ASSOCIATE CLOUD ENGINEER TOPIC 1 QUESTION 162 DISCUSSION

Actual exam question from Google's Associate Cloud Engineer
Question #: 162
Topic #: 1
[All Associate Cloud Engineer Questions]

Your company has embraced a hybrid cloud strategy where some of the applications are deployed on Google Cloud. A Virtual Private Network (VPN) tunnel connects your Virtual Private Cloud (VPC) in Google Cloud with your company's on-premises network. Multiple applications in Google Cloud need to connect to an on-premises database server, and you want to avoid having to change the IP configuration in all of your applications when the IP of the database changes.
What should you do?

A. Configure Cloud NAT for all subnets of your VPC to be used when egressing from the VM instances.

B. Create a private zone on Cloud DNS, and configure the applications with the DNS name.

C. Configure the IP of the database as custom metadata for each instance, and query the metadata server.

D. Query the Compute Engine internal DNS from the applications to retrieve the IP of the database.

Show Suggested Answer

by JDoutthere at *March 14, 2021, 12:37 a.m.*

Comments

Type your comment...

Submit

kopper2019 Highly Voted 3 years, 6 months ago

B,
Forwarding zones
Cloud DNS forwarding zones let you configure target name servers for specific private zones. Using a forwarding zone is one way to implement outbound DNS forwarding from your VPC network.

A Cloud DNS forwarding zone is a special type of Cloud DNS private zone. Instead of creating records within the zone, you specify a set of forwarding targets. Each forwarding target is an IP address of a DNS server, located in your VPC network, or in an on-premises network connected to your VPC network by Cloud VPN or Cloud Interconnect.

A does not apply, that is to provide internet access to resources
C, does not apply
D, I don't get it

so B

upvoted 34 times

meh009 3 years, 6 months ago

Agreed, It's B although I chose A intitally. After some careful consideration and understanding how Cloud NAT works, I'm sticking with B
https://cloud.google.com/nat/docs/overview

upvoted 3 times

meh009 3 years, 6 months ago

Further clarification:
''On-premises clients can resolve records in private zones, forwarding zones, and peering zones for which the VPC network has been authorized. On-premises clients use Cloud VPN or Cloud Interconnect to connect to the VPC network.''

upvoted 1 times

djgodzilla 3 years, 4 months ago

this is talking about On-premises client resolving nodes outside their network . the question is about how would the application tier within the VPC would resolve the database server . you're confusing the resolution direction my friend

upvoted 3 times

djgodzilla 3 years, 4 months ago

It is still B , but it's rather outbound forward that's needed here :
DNS outbound Forwarding :
- Set up outbound forwarding private zones to query on-premises servers (On-prem Authoritative Zone: corp.example.com)
- In Cloud Router , add a custom route advertisement for GCP DNS proxies range 35.199.192.0/19 to the on-premises environment.
- Make sure inbound DNS traffic from 35.199.192.0/19 is allowed on on-prem firewall
- Cloud Router should be learning on-prem network route from On-prem Router
https://youtu.be/OH_Jw8NhEGU?t=1283
https://cloud.google.com/dns/docs/best-practices#use_forwarding_zones_to_query_on-premises_servers

upvoted 3 times

MacFreak 2 years, 1 month ago

"A does not apply, that is to provide internet access to resources" - do you really think NAT is only being used between public and private? Well...it's not! :)

upvoted 1 times

pondai Highly Voted 3 years, 7 months ago

https://cloud.google.com/dns/docs/best-practices#best_practices_for_dns_forwarding_zones_and_server_policies
Cloud DNS offers DNS forwarding zones and DNS server policies to allow lookups of DNS names between your on-premises and Google Cloud environment. You have multiple options for configuring DNS forwarding. The following section lists best practices for hybrid DNS setup. These best practices are illustrated in the Reference architectures for hybrid DNS.
So I think B is correct

upvoted 9 times

thewalker Most Recent 11 months ago

Selected Answer: B

B

https://cloud.google.com/dns/docs/overview

upvoted 1 times

scanner2 1 year, 1 month ago

Selected Answer: B

DNS is a hierarchical distributed database that lets you store IP addresses and other data and look them up by name. Cloud DNS lets you publish your zones and records in DNS without the burden of managing your own DNS servers and software.
Cloud DNS offers both public zones and private managed DNS zones. A public zone is visible to the public internet, while a private zone is visible only from one or more Virtual Private Cloud (VPC) networks that you specify.
https://cloud.google.com/dns/docs/overview

upvoted 3 times

Captain1212 1 year, 1 month ago

Selected Answer: B

B is the correct Answer

upvoted 1 times

jrisl1991 1 year, 8 months ago

Selected Answer: B

Based on this - https://cloud.google.com/dns/docs/overview#dns-forwarding-methods B must be the best option. I don't think there's a "typo" (or completely wrongly worded answer) in option D (there's comments saying that instead of Compute Engine it should be on-premise). I believe option D is wrong on purpose to create a confusion.

upvoted 1 times

Charumathi 2 years ago

Selected Answer: B

B is correct answer,
Configure Private Google Access for on-premises hosts,

DNS configuration
Your on-premises network must have DNS zones and records configured so that Google domain names resolve to the set of IP addresses for either private.googleapis.com or restricted.googleapis.com. You can create Cloud DNS managed private zones and use a Cloud DNS inbound server policy, or you can configure on-premises name servers. For example, you can use BIND or Microsoft Active Directory DNS.

https://cloud.google.com/vpc/docs/configure-private-google-access-hybrid#config-domain

upvoted 1 times

aforolt 2 years ago

Ans is D, looks like there is typo

upvoted 1 times

habros 2 years, 2 months ago

B. DNS works best with dynamic IPs.

upvoted 1 times

patashish 2 years, 3 months ago

Correct Ans is B
Ref - https://cloud.google.com/dns/docs/best-practices#best_practices_for_private_zones

upvoted 1 times

deadlydeb 2 years, 3 months ago

Selected Answer: B

B Cloud DNS

upvoted 2 times

AzureDP900 2 years, 4 months ago

B is correct

upvoted 1 times

deadlydeb 2 years, 4 months ago

Selected Answer: B

B: DNS

upvoted 1 times

Mike_Malone 2 years, 9 months ago

ans D
https://cloud.google.com/compute/docs/internal-dns

upvoted 3 times

Bidhanva 2 years, 10 months ago

option B

upvoted 1 times

FernandoJ 2 years, 10 months ago

Selected Answer: B

https://cloud.google.com/dns/docs/overview#:~:text=Create%20an%20inbound,the%20VPC%20network.

upvoted 1 times

gloisv 3 years, 2 months ago

IT's D, because:
A) Cloud NAT direction will be from the cloud resources to the on prem, an the DB is on prem (It will not work if the IP of the database on prem changes, and you have an VPN you should traffic your data trough it).
B) If you create a private zone and configure the applications, if your servers doesnt use the dns will not work.
C) I think is not suitable. I guess you should re-deploy all your Apps with the new conf if the address change.
D) If you have an A record ip of your DB HOST(wich is on prem) in Engine internal DNS and if it changes, you can update the registry quickly to change it to the new IP address, so it will be the best option for sure.

upvoted 3 times

Load full discussion...