PROFESSIONAL-CLOUD-NETWORK-ENGINEER Q&As

Professional Cloud Network Engineer

Pass Google PROFESSIONAL-CLOUD-NETWORK-ENGINEER Exam with 100% Guarantee

Following Questions and Answers are all new published by Google Official Exam Center

QUESTION 1

You recently deployed Cloud VPN to connect your on-premises data canter to Google Cloud. You need to monitor the usage of this VPN and set up alerts in case traffic exceeds the maximum allowed. You need to be able to quickly decide whether to add extra links or move to a Dedicated Interconnect. What should you do?

A. In the Network Intelligence Canter, check for the number of packet drops on the VPN.

B. In the Google Cloud Console, use Monitoring Query Language to create a custom alert for bandwidth utilization.

C. In the Monitoring section of the Google Cloud Console, use the Dashboard section to select a default dashboard for VPN usage.

D. In the VPN section of the Google Cloud Console, select the VPN under hybrid connectivity, and then select monitoring to display utilization on the dashboard.

Correct Answer: A

QUESTION 2

You need to enable Cloud CDN for all the objects inside a storage bucket. You want to ensure that all the object in the storage bucket can be served by the CDN.

What should you do in the GCP Console?

A. Create a new cloud storage bucket, and then enable Cloud CDN on it.

B. Create a new TCP load balancer, select the storage bucket as a backend, and then enable Cloud CDN on the backend.

C. Create a new SSL proxy load balancer, select the storage bucket as a backend, and then enable Cloud CDN on the backend.

D. Create a new HTTP load balancer, select the storage bucket as a backend, enable Cloud CDN on the backend, and make sure each object inside the storage bucket is shared publicly.

Correct Answer: D

https://cloud.google.com/load-balancing/docs/https/adding-backend-buckets-to-load-balancers#using_cloud_cdn_with_cloud_storage_buckets Cloud CDN needs HTTP(S) Load Balancers and Cloud Storage bucket has to be shared publicly. https://cloud.google.com/cdn/docs/setting-up-cdn-with-bucket

QUESTION 3

You need to enable Private Google Access for use by some subnets within your Virtual Private Cloud (VPC). Your security team set up the VPC to send all internet-bound traffic back to the on-premises data center for inspection before egressing to the internet, and is also implementing VPC Service Controls in the environment for API-level security control. You have already enabled the subnets for Private Google Access. What configuration changes should you make to enable Private Google Access while adhering to your security team\\'s requirements?

A. Create a private DNS zone with a CNAME record for *.googleapis.com to restricted.googleapis.com, with an A record pointing to Google\\'s restricted API address range. Create a custom route that points Google\\'s restricted API address range to the default internet gateway as the next hop.

B. Create a private DNS zone with a CNAME record for *.googleapis.com to restricted.googleapis.com, with an A record pointing to Google\\'s restricted API address range. Change the custom route that points the default route (0/0) to the default internet gateway as the next hop.

C. Create a private DNS zone with a CNAME record for *.googleapis.com to private.googleapis.com, with an A record painting to Google\\'s private AP address range. Change the custom route that points the default route (0/0) to the default internet gateway as the next hop.

D. Create a private DNS zone with a CNAME record for *.googleapis.com to private.googleapis.com, with an A record pointing to Google\\'s private API address range. Create a custom route that points Google\\'s private API address range to the default internet gateway as the next hop.

Correct Answer: C

QUESTION 4

Your company just completed the acquisition of Altostrat (a current GCP customer). Each company has a separate organization in GCP and has implemented a custom DNS solution. Each organization will retain its current domain and host names until after a full transition and architectural review is done in one year. These are the assumptions for both GCP environments.

1.

Each organization has enabled full connectivity between all of its projects by using Shared VPC.

2.

Both organizations strictly use the 10.0.0.0/8 address space for their instances, except for bastion hosts (for accessing the instances) and load balancers for serving web traffic.

3.

There are no prefix overlaps between the two organizations.

4.

Both organizations already have firewall rules that allow all inbound and outbound traffic from the 10.0.0.0/8 address space.

5.

Neither organization has Interconnects to their on-premises environment.

You want to integrate networking and DNS infrastructure of both organizations as quickly as possible and with minimal downtime.

Which two steps should you take? (Choose two.)

A. Provision Cloud Interconnect to connect both organizations together.

B. Set up some variant of DNS forwarding and zone transfers in each organization.

C. Connect VPCs in both organizations using Cloud VPN together with Cloud Router.

D. Use Cloud DNS to create A records of all VMs and resources across all projects in both organizations.

E. Create a third organization with a new host project, and attach all projects from your company and Altostrat to it using shared VPC.

Correct Answer: BC

https://cloud.google.com/dns/docs/best-practices

QUESTION 5

Your organization uses a Shared VPC architecture with a host project and three service projects. You have Compute Engine instances that reside in the service projects. You have critical workloads in your on-premises data center. You need to ensure that the Google Cloud instances can resolve on-premises hostnames via the Dedicated Interconnect you deployed to establish hybrid connectivity. What should you do?

A. Create a Cloud DNS private forwarding zone in the host project of the Shared VPC that forwards the private zone to the on-premises DNS servers. In your Cloud Router, add a custom route advertisement for the IP 35.199.192.0/19 to the on-premises environment.

B. Create a Cloud DNS private forwarding zone in the host project of the Shared VPC that forwards the Private zone to the on-premises DNS servers. In your Cloud Router, add a custom route advertisement for the IP 169.254 169.254 to the on-premises environment.

C. Configure a Cloud DNS private zone in the host project of the Shared VPC. Set up DNS forwarding to your Google Cloud private zone on your on-premises DNS servers to point to the inbound forwarder IP address in your host project In your Cloud Router, add a custom route advertisement for the IP 169.254 169 254 to the on-premises environment.

D. Configure a Cloud DNS private zone in the host project of the Shared VPC. Set up DNS forwarding to your Google Cloud private zone on your on-premises DNS servers to point to the inbound forwarder IP address in your host project. Configure a DNS policy in the Shared VPC to allow inbound query forwarding with your on-premises DNS server as the alternative DNS server.

Correct Answer: D