Google

Exam Questions Professional-Cloud-Network-Engineer

Google Cloud Certified - Professional Cloud Network Engineer

NEW QUESTION 1
You are configuring a new application that will be exposed behind an external load balancer with both IPv4 and IPv6 addresses and support TCP pass-through on port 443. You will have backends in two regions:
us-west1 and us-east1. You want to serve the content with the lowest possible latency while ensuring high availability and autoscaling. Which configuration should you use?

A. Use global SSL Proxy Load Balancing with backends in both regions.
B. Use global TCP Proxy Load Balancing with backends in both regions.
C. Use global external HTTP(S) Load Balancing with backends in both regions.
D. Use Network Load Balancing in both regions, and use DNS-based load balancing to direct traffic to the closest region.

Answer: D

NEW QUESTION 2
You are designing a hybrid cloud environment. Your Google Cloud environment is interconnected with your on-premises network using HA VPN and Cloud Router in a central transit hub VPC. The Cloud Router is configured with the default settings. Your on-premises DNS server is located at 192.168.20.88. You need to ensure that your Compute Engine resources in multiple spoke VPCs can resolve on-premises private hostnames using the domain corp.altostrat.com while also resolving Google Cloud hostnames. You want to follow Google-recommended practices. What should you do?

A. Create a private forwarding zone in Cloud DNS for ‘corp.altostrat.com’ called corp-altostrat-com that points to 192.168.20.88. Associate the zone with the hub VPC.Create a private peering zone in Cloud DNS for ‘corp.altostrat.com’ called corp-altostrat-com associated with the spoke VPCs, with the hub VPC as the target.Set a custom route advertisement on the Cloud Router for 35.199.192.0/19. Configure VPC peering in the spoke VPCs to peer with the hub VPC.
B. Create a private forwarding zone in Cloud DNS for ‘corp.altostrat.com’ called corp-altostrat-com that points to 192.168.20.88.Associate the zone with the hub VP
C. Create a private peering zone in Cloud DNS for ‘corp.altostrat.com’ called corp-altostrat-com associated with the spoke PCs, with the hub VPC as the target.Set a custom route advertisement on the Cloud Router for 35.199.192.0/19.
D. Create a private forwarding zone in Cloud DNS for ‘corp.altostrat.com’ called corp-altostrat-com that points to 192.168.20.88. Associate the zone with the hub VPC.Create a private peering zone in Cloud DNS for ‘corp.altostrat.com’ called corp-altostrat-com associated with the spoke VPCs, with the hub VPC as the target.Set a custom route advertisement on the Cloud Router for 35.199.192.0/19.Create a hub-and-spoke VPN deployment in each spoke VPC to connect back to the on-premises network directly.
E. Create a private forwarding zone in Cloud DNS for ‘corp altostrat.com’ called corp-altostrat-com that points to 192. 168.20.88. Associate the zone with the hub VPC.Create a private peering zone in Cloud DNS for ‘corp.altostrat.com’ called corp-altostrat-com associated with the spoke VPCs, with the hub VPC as the target.Sat a custom route advertisement on the Cloud Router for 35.199.192.0/19.Create a hub and spoke VPN deployment in each spoke VPC to connect back to the hub VPC.

Answer: A

NEW QUESTION 3
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.
• Each organization has enabled full connectivity between all of its projects by using Shared VPC.
• 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.
• There are no prefix overlaps between the two organizations.
• Both organizations already have firewall rules that allow all inbound and outbound traffic from the 10.0.0.0/8 address space.
• 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.

Answer: BC

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

NEW QUESTION 4
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.

Answer: D

Explanation:
https://cloud.google.com/load-balancing/docs/https/adding-backend-buckets-to-load-balancers#using_cloud_cdn 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

NEW QUESTION 5
You just finished your company's migration to Google Cloud and configured an architecture with 3 Virtual Private Cloud (VPC) networks: one for Sales, one for Finance, and one for Engineering. Every VPC contains over 100 Compute Engine instances, and now developers using instances in the Sales VPC and the Finance VPC require private connectivity between each other. You need to allow communication between Sales and Finance without compromising performance or security. What should you do?

A. Configure an HA VPN gateway between the Finance VPC and the Sales VPC.
B. Configure the instances that require communication between each other with an external IP address.
C. Create a VPC Network Peering connection between the Finance VPC and the Sales VPC.
D. Configure Cloud NAT and a Cloud Router in the Sales and Finance VPCs.

Answer: C

NEW QUESTION 6
You need to centralize the Identity and Access Management permissions and email distribution for the WebServices Team as efficiently as possible.
What should you do?

A. Create a Google Group for the WebServices Team.
B. Create a G Suite Domain for the WebServices Team.
C. Create a new Cloud Identity Domain for the WebServices Team.
D. Create a new Custom Role for all members of the WebServices Team.

Answer: A

NEW QUESTION 7
You want to configure load balancing for an internet-facing, standard voice-over-IP (VOIP) application. Which type of load balancer should you use?

A. HTTP(S) load balancer
B. Network load balancer
C. Internal TCP/UDP load balancer
D. TCP/SSL proxy load balancer

Answer: B

NEW QUESTION 8
You have deployed a proof-of-concept application by manually placing instances in a single Compute Engine zone. You are now moving the application to production, so you need to increase your application availability and ensure it can autoscale.
How should you provision your instances?

A. Create a single managed instance group, specify the desired region, and select Multiple zones for the location.
B. Create a managed instance group for each region, select Single zone for the location, and manuallydistribute instances across the zones in that region.
C. Create an unmanaged instance group in a single zone, and then create an HTTP load balancer for the instance group.
D. Create an unmanaged instance group for each zone, and manually distribute the instances across the desired zones.

Answer: A

Explanation:
https://cloud.google.com/compute/docs/instance-groups/creating-groups-of-managed-instances

NEW QUESTION 9
You want to establish a dedicated connection to Google that can access Cloud SQL via a public IP address and that does not require a third-party service provider.
Which connection type should you choose?

A. Carrier Peering
B. Direct Peering
C. Dedicated Interconnect
D. Partner Interconnect

Answer: B

Explanation:
When established, Direct Peering provides a direct path from your on-premises network to Google services, including Google Cloud products that can be exposed through one or more public IP addresses. Traffic from Google's network to your on-premises network also takes that direct path, including traffic from VPC networks in your projects. Google Cloud customers must request that direct egress pricing be enabled for each of their projects after they have established Direct Peering with Google. For more information, see Pricing.

NEW QUESTION 10
You are deploying a global external TCP load balancing solution and want to preserve the source IP address of the original layer 3 payload.
Which type of load balancer should you use?

A. HTTP(S) load balancer
B. Network load balancer
C. Internal load balancer
D. TCP/SSL proxy load balancer

Answer: D

Explanation:
By default TCP/SSL proxy load balancer original client IP address and port information is not preserved, but it can be preserved using the PROXY protocol:
https://cloud.google.com/load-balancing/docs/tcp#target-proxies
https://medium.com/google-cloud/preserving-client-ips-through-google-clouds-global-tcp-and-ssl-proxy-load-ba

NEW QUESTION 10
You have an application running on Compute Engine that uses BigQuery to generate some results that are stored in Cloud Storage. You want to ensure that none of the application instances have external IP addresses.
Which two methods can you use to accomplish this? (Choose two.)

A. Enable Private Google Access on all the subnets.
B. Enable Private Google Access on the VPC.
C. Enable Private Services Access on the VPC.
D. Create network peering between your VPC and BigQuery.
E. Create a Cloud NAT, and route the application traffic via NAT gateway.

Answer: AE

Explanation:
https://cloud.google.com/nat/docs/overview#interaction-pga Specifications https://cloud.google.com/vpc/docs/configure-private-google-access#specifications

NEW QUESTION 13
You have a web application that is currently hosted in the us-central1 region. Users experience high latency when traveling in Asia. You've configured a network load balancer, but users have not experienced a performance improvement. You want to decrease the latency.
What should you do?

A. Configure a policy-based route rule to prioritize the traffic.
B. Configure an HTTP load balancer, and direct the traffic to it.
C. Configure Dynamic Routing for the subnet hosting the application.
D. Configure the TTL for the DNS zone to decrease the time between updates.

Answer: B

NEW QUESTION 14
You are designing a new global application using Compute Engine instances that will be exposed by a global HTTP(S) load balancer. You need to secure your application from distributed denial-of-service and application layer (layer 7) attacks. What should you do?

A. Configure VPC Service Controls and create a secure perimete
B. Define fine-grained perimeter controls and enforce that security posture across your Google Cloud services and projects.
C. Configure a Google Cloud Armor security policy in your project, and attach it to the backend service to secure the application.
D. Configure VPC firewall rules to protect the Compute Engine instances against distributed denial-of-service attacks.
E. Configure hierarchical firewall rules for the global HTTP(S) load balancer public IP address at the organization level.

Answer: C

NEW QUESTION 17
You recently noticed a recurring daily spike in network usage in your Google Cloud project. You need to identify the virtual machine (VM) instances and type of traffic causing the spike in traffic utilization while minimizing the cost and management overhead required. What should you do?

A. Enable VPC Flow Logs and send the output to BigQuery for analysis.
B. Enable Firewall Rules Logging for all allowed traffic and send the output to BigQuery for analysis.
C. Configure Packet Mirroring to send all traffic to a V
D. Use Wireshark on the VM to identity traffic utilization for each VM in the VPC.
E. Deploy a third-party network appliance and configure it as the default gatewa
F. Use the third-party network appliance to identify users with high network traffic.

Answer: C

NEW QUESTION 18
You recently deployed Compute Engine instances in regions us-west1 and us-east1 in a Virtual Private Cloud (VPC) with default routing configurations. Your company security policy mandates that virtual machines (VMs) must not have public IP addresses attached to them. You need to allow your instances to fetch updates from the internet while preventing external access. What should you do?

A. Create a Cloud NAT gateway and Cloud Router in both us-west1 and us-east1.
B. Create a single global Cloud NAT gateway and global Cloud Router in the VPC.
C. Change the instances' network interface external IP address from None to Ephemeral.
D. Create a firewall rule that allows egress to destination 0.0.0.0/0.

Answer: A

NEW QUESTION 21
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-premisesenvironment.
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 projectIn 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.

Answer: D

NEW QUESTION 25
You are designing a hybrid cloud environment for your organization. Your Google Cloud environment is interconnected with your on-premises network using Cloud HA VPN and Cloud Router. The Cloud Router is
configured with the default settings. Your on-premises DNS server is located at 192.168.20.88 and is protected by a firewall, and your Compute Engine resources are located at 10.204.0.0/24. Your Compute Engine resources need to resolve on-premises private hostnames using the domain corp.altostrat.com while still resolving Google Cloud hostnames. You want to follow Google-recommended practices. What should you do?

A. Create a private forwarding zone in Cloud DNS for ‘corp.altostrat.com’ called corp-altostrat-com that points to 192.168.20.88.Configure your on-premises firewall to accept traffic from 10.204.0.0/24. Set a custom route advertisement on the Cloud Router for 10.204.0.0/24
B. Create a private forwarding zone in Cloud DNS for ‘corp.altostrat.com’ called corp-altostrat-com that points to 192.168 20.88.Configure your on-premises firewall to accept traffic from 35.199.192.0/19 Set a custom route advertisement on the Cloud Router for 35.199.192.0/19.
C. Create a private forwarding zone in Cloud DNS for ‘corp .altostrat.com’ called corp-altostrat-com that points to 192.168.20.88.Configure your on-premises firewall to accept traffic from 10.204.0.0/24.Modify the /etc/resolv conf file on your Compute Engine instances to point to 192.168.20 88
D. Create a private zone in Cloud DNS for ‘corp altostrat.com’ called corp-altostrat-com.Configure DNS Server Policies and create a policy with Alternate DNS servers to 192.168.20.88. Configure your on-premises firewall to accept traffic from 35.199.192.0/19.Set a custom route advertisement on the Cloud Router for 35.199.192.0/19.

Answer: D

NEW QUESTION 29
Your company's web server administrator is migrating on-premises backend servers for an application to GCP. Libraries and configurations differ significantly across these backend servers. The migration to GCP will be lift-and-shift, and all requests to the servers will be served by a single network load balancer frontend. You want to use a GCP-native solution when possible.
How should you deploy this service in GCP?

A. Create a managed instance group from one of the images of the on-premises servers, and link thisinstance group to a target pool behind your load balancer.
B. Create a target pool, add all backend instances to this target pool, and deploy the target pool behind your load balancer.
C. Deploy a third-party virtual appliance as frontend to these servers that will accommodate the significant differences between these backend servers.
D. Use GCP's ECMP capability to load-balance traffic to the backend servers by installing multiple equal-priority static routes to the backend servers.

Answer: B

NEW QUESTION 31
You need to configure the Border Gateway Protocol (BGP) session for a VPN tunnel you just created between two Google Cloud VPCs, 10.1.0.0/16 and 172.16.0.0/16. You have a Cloud Router (router-1) in the 10.1.0.0/16 network and a second Cloud Router (router-2) in the 172.16.0.0/16 network. Which configuration should you use for the BGP session?

A. C:\Users\Admin\Desktop\Data\Odt data\Untitled.jpg

Router	BGP Interface Name	BGP IP	BGP Peer IP	Peer ASN
router-1	if-tunnel-a-to-b-if-0	169.254.0.254	169.254.0.254	65502
router-2	if-tunnel-b-to-a-if-0	169.254.0.254	169.254.0.254	65501

B. C:\Users\Admin\Desktop\Data\Odt data\Untitled.jpg

Router	BGP Interface Name	BGP IP	BGP Peer IP	Peer ASN
router-1	if-tunnel-a-to-b-if-0	10.1.0.1	172.16.0.1	15052
router-2	if-tunnel-b-to-a-if-0	172.16.0.1	10.1.0.1	15501

C. C:\Users\Admin\Desktop\Data\Odt data\Untitled.jpg

Router	BGP Interface Name	BGP IP	BGP Peer IP	Peer ASN
router-1	if-tunnel-a-to-b-if-0	169.254.20.1	169.254.20.2	65002
router-2	if-tunnel-b-to-a-if-0	169.254.20.2	169.254.20.1	65001

D. C:\Users\Admin\Desktop\Data\Odt data\Untitled.jpg

Router	BGP Interface Name	BGP IP	BGP Peer IP	Peer ASN
router-1	if-tunnel-a-to-b-if-0	172.16.0.254	10.1.0.254	16552
router-2	if-tunnel-b-to-a-if-0	10.1.0.254	172.16.0.254	16551

Answer: C

NEW QUESTION 32
Your company has defined a resource hierarchy that includes a parent folder with subfolders for each department. Each department defines their respective project and VPC in the assigned folder and has the appropriate permissions to create Google Cloud firewall rules. The VPCs should not allow traffic to flow between them. You need to block all traffic from any source, including other VPCs, and delegate only the intra-VPC firewall rules to the respective departments. What should you do?

A. Create a VPC firewall rule in each VPC to block traffic from any source, with priority 0.
B. Create a VPC firewall rule in each VPC to block traffic from any source, with priority 1000.
C. Create two hierarchical firewall policies per department's folder with two rules in each: a high-priority rule that matches traffic from the private CIDRs assigned to

the respective VPC and sets the action to allow, and another lower-priority rule that blocks traffic from any other source.
D. Create two hierarchical firewall policies per department's folder with two rules in each: a high-priority rule that matches traffic from the private CIDRs assigned to the respective VPC and sets the action to goto_next, and another lower-priority rule that blocks traffic from any other source.

Answer: B

NEW QUESTION 34
You are configuring a new HTTP application that will be exposed externally behind both IPv4 and IPv6 virtual IP addresses, using ports 80, 8080, and 443. You will have backends in two regions: us-west1 and
us-east1. You want to serve the content with the lowest-possible latency while ensuring high availability and autoscaling, and create native content-based rules using the HTTP hostname and request path. The IP addresses of the clients that connect to the load balancer need to be visible to the backends. Which configuration should you use?

A. Use Network Load Balancing
B. Use TCP Proxy Load Balancing with PROXY protocol enabled
C. Use External HTTP(S) Load Balancing with URL Maps and custom headers
D. Use External HTTP(S) Load Balancing with URL Maps and an X-Forwarded-For header

Answer: D

NEW QUESTION 35
Your company is working with a partner to provide a solution for a customer. Both your company and the partner organization are using GCP. There are applications in the partner's network that need access to some resources in your company's VPC. There is no CIDR overlap between the VPCs.
Which two solutions can you implement to achieve the desired results without compromising the security? (Choose two.)

A. VPC peering
B. Shared VPC
C. Cloud VPN
D. Dedicated Interconnect
E. Cloud NAT

Answer: AC

Explanation:
Google Cloud VPC Network Peering allows internal IP address connectivity across two Virtual Private Cloud (VPC) networks regardless of whether they belong to the same project or the same organization.

NEW QUESTION 39
All the instances in your project are configured with the custom metadata enable-oslogin value set to FALSE and to block project-wide SSH keys. None of the instances are set with any SSH key, and no project-wide SSH keys have been configured. Firewall rules are set up to allow SSH sessions from any IP address range. You want to SSH into one instance.
What should you do?

A. Open the Cloud Shell SSH into the instance using gcloud compute ssh.
B. Set the custom metadata enable-oslogin to TRUE, and SSH into the instance using a third-party tool like putty or ssh.
C. Generate a new SSH key pai
D. Verify the format of the private key and add it to the instanc
E. SSH into the instance using a third-party tool like putty or ssh.
F. Generate a new SSH key pai
G. Verify the format of the public key and add it to the projec
H. SSH into the instance using a third-party tool like putty or ssh.

Answer: A

NEW QUESTION 42
Your company has a single Virtual Private Cloud (VPC) network deployed in Google Cloud with access from your on-premises network using Cloud Interconnect. You must configure access only to Google APIs and services that are supported by VPC Service Controls through hybrid connectivity with a service level agreement (SLA) in place. What should you do?

A. Configure the existing Cloud Routers to advertise the Google API's public virtual IP addresses.
B. Use Private Google Access for on-premises hosts with restricted.googleapis.com virtual IP addresses.
C. Configure the existing Cloud Routers to advertise a default route, and use Cloud NAT to translate traffic from your on-premises network.
D. Add Direct Peering links, and use them for connectivity to Google APIs that use public virtual IP addresses.

Answer: B

NEW QUESTION 45
You are responsible for enabling Private Google Access for the virtual machine (VM) instances in your Virtual Private Cloud (VPC) to access Google APIs. All VM instances have only a private IP address and need to access Cloud Storage. You need to ensure that all VM traffic is routed back to your on-premises data center for traffic scrubbing via your existing Cloud Interconnect connection. However, VM traffic to Google APIs should remain in the VPC. What should you do?

A. Delete the default route in your VPC.Create a private Cloud DNS zone for googleapis.com, create a CNAME for *.googleapis.com to restricted googleapis.com, and create an A record for restricted googleapis com that resolves to the addresses in 199.36.153.4/30.Create a static route in your VPC for the range 199.36.153.4/30 with the default internet gateway as the next hop.
B. Delete the default route in your VPC and configure your on-premises router to advertise 0.0.0.0/0 via Border Gateway Protocol (BGP).Create a public Cloud DNS zone with a CNAME for *.google.com to private googleapis com, create a CNAME for * googleapis.com to private googleapis com, and create an A record for Private googleapis.com that resolves to the addresses in 199.36.153 8/30.Create a static route in your VPC for the range 199 .36.153.8/30 with the default internet gateway as the next hop.

C. Configure your on-premises router to advertise 0.0.0.0/0 via Border Gateway Protocol (BGP) with a lower priority (MED) than the default VPC route.Create a private Cloud DNS zone for googleapis.com, create a CNAME for * googieapis.com to private googleapis com, and create an A record for private.googleapis.com that resolves to the addresses in 199.36.153.8/30.Create a static route in your VPC for the range 199.36. 153.8/30 with the default internet gateway as the next hop.
D. Delete the default route in your VPC and configure your on-premises router to advertise 0.0.0.0/0 via Border Gateway Protocol (BGP).Create a private Cloud DNS zone for googleapis.com, create a CNAME for * googieapis.com to Private googleapis.com, and create an A record for private.googleapis.com that resolves to the addresses in 199.36.153.8/30.Create a static route in your VPC for the range 199.36.153.8/30 with the default internet gateway as the next hop.

Answer: C

NEW QUESTION 50
You need to create the network infrastructure to deploy a highly available web application in the us-east1 and us-west1 regions. The application runs on Compute Engine instances, and it does not require the use of a database. You want to follow Google-recommended practices. What should you do?

A. Create one VPC with one subnet in each region.Create a regional network load balancer in each region with a static IP addres
B. Enable Cloud CDN on the load balancers.Create an A record in Cloud DNS with both IP addresses for the load balancers.
C. Create one VPC with one subnet in each region.Create a global load balancer with a static IP address.Enable Cloud CDN and Google Cloud Armor on the load balancer.Create an A record using the IP address of the load balancer in Cloud DNS.
D. Create one VPC in each region, and peer both VPCs.Create a global load balancer.Enable Cloud CDN on the load balancer.Create a CNAME for the load balancer in Cloud DNS.
E. Create one VPC with one subnet in each region.Create an HTTP(S) load balancer with a static IP address.Choose the standard tier for the networ
F. Enable Cloud CDN on the load balancer.Create a CNAME record using the load balancer's IP address in Cloud DNS.

Answer: C

NEW QUESTION 55
After a network change window one of your company's applications stops working. The application uses an on-premises database server that no longer receives any traffic from the application. The database server IP address is 10.2.1.25. You examine the change request, and the only change is that 3 additional VPC subnets were created. The new VPC subnets created are 10.1.0.0/16, 10.2.0.0/16, and 10.3.1.0/24/ The on-premises router is advertising 10.0.0.0/8.
What is the most likely cause of this problem?

A. The less specific VPC subnet route is taking priority.
B. The more specific VPC subnet route is taking priority.
C. The on-premises router is not advertising a route for the database server.
D. A cloud firewall rule that blocks traffic to the on-premises database server was created during the change.

Answer: B

NEW QUESTION 60
You work for a multinational enterprise that is moving to GCP. These are the cloud requirements:
• An on-premises data center located in the United States in Oregon and New York with Dedicated Interconnects connected to Cloud regions us-west1 (primary HQ) and us-east4 (backup)
• Multiple regional offices in Europe and APAC
• Regional data processing is required in europe-west1 and australia-southeast1
• Centralized Network Administration Team
Your security and compliance team requires a virtual inline security appliance to perform L7 inspection for URL filtering. You want to deploy the appliance in us-west1.
What should you do?

A. • Create 2 VPCs in a Shared VPC Host Project.• Configure a 2-NIC instance in zone us-west1-a in the Host Project.• Attach NIC0 in VPC #1 us-west1 subnet of the Host Project.• Attach NIC1 in VPC #2 us-west1 subnet of the Host Project.• Deploy the instance.• Configure the necessary routes and firewall rules to pass traffic through the instance.
B. • Create 2 VPCs in a Shared VPC Host Project.• Configure a 2-NIC instance in zone us-west1-a in the Service Project.• Attach NIC0 in VPC #1 us-west1 subnet of the Host Project.• Attach NIC1 in VPC #2 us-west1 subnet of the Host Project.• Deploy the instance.• Configure the necessary routes and firewall rules to pass traffic through the instance.
C. • Create 1 VPC in a Shared VPC Host Project.• Configure a 2-NIC instance in zone us-west1-a in the Host Project.• Attach NIC0 in us-west1 subnet of the Host Project.• Attach NIC1 in us-west1 subnet of the Host Project• Deploy the instance.• Configure the necessary routes and firewall rules to pass traffic through the instance.
D. • Create 1 VPC in a Shared VPC Service Project.• Configure a 2-NIC instance in zone us-west1-a in the Service Project.• Attach NIC0 in us-west1 subnet of the Service Project.• Attach NIC1 in us-west1 subnet of the Service Project• Deploy the instance.• Configure the necessary routes and firewall rules to pass traffic through the instance.

Answer: B

Explanation:
https://cloud.google.com/vpc/docs/shared-vpc

NEW QUESTION 61
You deployed a hub-and-spoke architecture in your Google Cloud environment that uses VPC Network Peering to connect the spokes to the hub. For security reasons, you deployed a private Google Kubernetes
Engine (GKE) cluster in one of the spoke projects with a private endpoint for the control plane. You configured authorized networks to be the subnet range where the GKE nodes are deployed. When you attempt to reach the GKE control plane from a different spoke project, you cannot access it. You need to allow access to the GKE control plane from the other spoke projects. What should you do?

A. Add a firewall rule that allows port 443 from the other spoke projects.
B. Enable Private Google Access on the subnet where the GKE nodes are deployed.
C. Configure the authorized networks to be the subnet ranges of the other spoke projects.
D. Deploy a proxy in the spoke project where the GKE nodes are deployed and connect to the control plane through the proxy.

Answer: C

NEW QUESTION 64
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.

Answer: A

NEW QUESTION 69
You are configuring load balancing for a standard three-tier (web, application, and database) application. You have configured an external HTTP(S) load balancer for the web servers. You need to configure load balancing for the application tier of servers. What should you do?

A. Configure a forwarding rule on the existing load balancer for the application tier.
B. Configure equal cost multi-path routing on the application servers.
C. Configure a new internal HTTP(S) load balancer for the application tier.
D. Configure a URL map on the existing load balancer to route traffic to the application tier.

Answer: A

NEW QUESTION 72
You configured Cloud VPN with dynamic routing via Border Gateway Protocol (BGP). You added a custom route to advertise a network that is reachable over the VPN tunnel. However, the on-premises clients still cannot reach the network over the VPN tunnel. You need to examine the logs in Cloud Logging to confirm that the appropriate routers are being advertised over the VPN tunnel. Which filter should you use in Cloud Logging to examine the logs?

A. resource.type= “gce_router”
B. resource.type= “gce_network_region”
C. resource.type= “vpn_tunnel”
D. resource.type= “vpn_gateway”

Answer: C

NEW QUESTION 75
You are using the gcloud command line tool to create a new custom role in a project by coping a predefined role. You receive this error message:
INVALID_ARGUMENT: Permission resourcemanager.projects.list is not valid What should you do?

A. Add the resourcemanager.projects.get permission, and try again.
B. Try again with a different role with a new name but the same permissions.
C. Remove the resourcemanager.projects.list permission, and try again.
D. Add the resourcemanager.projects.setIamPolicy permission, and try again.

Answer: C

NEW QUESTION 79
You want to implement an IPSec tunnel between your on-premises network and a VPC via Cloud VPN. You need to restrict reachability over the tunnel to specific local subnets, and you do not have a device capable of speaking Border Gateway Protocol (BGP).
Which routing option should you choose?

A. Dynamic routing using Cloud Router
B. Route-based routing using default traffic selectors
C. Policy-based routing using a custom local traffic selector
D. Policy-based routing using the default local traffic selector

Answer: C

NEW QUESTION 83
You recently configured Google Cloud Armor security policies to manage traffic to your application. You discover that Google Cloud Armor is incorrectly blocking some traffic to your application. You need to identity the web application firewall (WAF) rule that is incorrectly blocking traffic. What should you do?

A. Enable firewall logs, and view the logs in Firewall Insights.
B. Enable HTTP(S) Load Balancing logging with sampling rate equal to 1, and view the logs in Cloud Logging.
C. Enable VPC Flow Logs, and view the logs in Cloud Logging.
D. Enable Google Cloud Armor audit logs, and view the logs on the Activity page in the Google CloudConsole.

Answer: A

NEW QUESTION 87
You are adding steps to a working automation that uses a service account to authenticate. You need to drive the automation the ability to retrieve files from a Cloud Storage bucket. Your organization requires using the least privilege possible.
What should you do?

A. Grant the compute.instanceAdmin to your user account.
B. Grant the iam.serviceAccountUser to your user account.
C. Grant the read-only privilege to the service account for the Cloud Storage bucket.
D. Grant the cloud-platform privilege to the service account for the Cloud Storage bucket.

Answer: C

NEW QUESTION 92
You recently deployed your application in Google Cloud. You need to verify your Google Cloud network configuration before deploying your on-premises workloads. You want to confirm that your Google Cloud network configuration allows traffic to flow from your cloud resources to your on- premises network. This validation should also analyze and diagnose potential failure points in your Google Cloud network configurations without sending any data plane test traffic. What should you do?

A. Use Network Intelligence Center's Connectivity Tests.
B. Enable Packet Mirroring on your application and send test traffic.
C. Use Network Intelligence Center's Network Topology visualizations.
D. Enable VPC Flow Logs and send test traffic.

Answer: C

NEW QUESTION 97
You have the following firewall ruleset applied to all instances in your Virtual Private Cloud (VPC):

Direction	Action	Address range	Port	Priority
egress	deny	192.0.2.0/24	80	100
egress	deny	198.51.100.0/24	80	200
ingress	allow	203.0.113.0/24	80	300

You need to update the firewall rule to add the following rule to the ruleset:

Direction	Action	Address range	Port	Logging
egress	deny	192.0.2.42/32	80	true

You are using a new user account. You must assign the appropriate identity and Access Management (IAM) user roles to this new user account before updating the firewall rule. The new user account must be able to apply the update and view firewall logs. What should you do?

A. Assign the compute.securityAdmin and logging.viewer rule to the new user accoun
B. Apply the new firewall rule with a priority of 50.
C. Assign the compute.securityAdmin and logging.bucketWriter role to the new user accoun
D. Apply the new firewall rule with a priority of 150.
E. Assign the compute.orgSecurityPolicyAdmin and logging.viewer role to the new user accoun
F. Apply the new firewall rule with a priority of 50.
G. Assign the compute.orgSecurityPolicyAdmin and logging.bucketWriter role to the new user account.Apply the new firewall rule with a priority of 150.

Answer: A

NEW QUESTION 102
You have a storage bucket that contains two objects. Cloud CDN is enabled on the bucket, and both objects have been successfully cached. Now you want to make sure that one of the two objects will not be cached anymore, and will always be served to the internet directly from the origin.
What should you do?

A. Ensure that the object you don’t want to be cached anymore is not shared publicly.
B. Create a new storage bucket, and move the object you don’t want to be checked anymore inside i
C. Then edit the bucket setting and enable the private attribute.
D. Add an appropriate lifecycle rule on the storage bucket containing the two objects.
E. Add a Cache-Control entry with value private to the metadata of the object you don’t want to be cached anymor
F. Invalidate all the previously cached copies.

Answer: D

Explanation:
https://cloud.google.com/cdn/docs/invalidating-cached-content

NEW QUESTION 103
In your project my-project, you have two subnets in a Virtual Private Cloud (VPC): subnet-a with IP range 10.128.0.0/20 and subnet-b with IP range 172.16.0.0/24. You need to deploy database servers in subnet-a. You will also deploy the application servers and web servers in subnet-b. You want to configure firewall rules that only allow database traffic from the application servers to the database servers. What should you do?

A. Create network tag app-server and service account sa-db@my-project.iam.gserviceaccount.co
B. Add the tag to the application servers, and associate the service account with the database server
C. Run the following command:gcloud compute firewall-rules create app-db-firewall-rule \--action allow \--direction ingress \--rules top:3306 \--source-tags app-server \--target-service-accounts sa-db@my- project.iam.gserviceaccount.com
D. Create service accounts sa-app@my-project.iam.gserviceaccount.com andsa-db@my-project.iam.gserviceaccount.co
E. Associate service account sa-app with the application servers, and associate theservice account sa-db with the database server
F. Run the following command: gcloud compute firewall-rules create app-db-firewall-ru--allow TCP:3306 \--source-service-accounts sa-app@democloud-idp-demo.iam.gserviceaccount.com \--target-service-accounts sa-db@my- project.iam.gserviceaccount.com
G. Create service accounts sa-app@my-project.iam.gserviceaccount.com andsa-db@my-project.iam.gserviceaccount.co

H. Associate the service account sa-app with the application servers, and associatethe service account sa-db with the database server
I. Run the following command: gcloud compute firewall-rules create app-db-firewall-ru--allow TCP:3306 \--source-ranges 10.128.0.0/20 \--source-service-accounts sa-app@my- project.iam.gserviceaccount.com \--target-service-accounts sa-db@my- project.iam.gserviceaccount.com
J. Create network tags app-server and db-serve
K. Add the app-server tag to the application servers, and add the db-server tag to the database server
L. Run the following command:gcloud compute firewall-rules create app-db-firewall-rule \--action allow \--direction ingress \--rules tcp:3306 \--source-ranges 10.128.0.0/20 \--source-tags app-server \--target-tags db-server

Answer: D

NEW QUESTION 107
You need to create a new VPC network that allows instances to have IP addresses in both the 10.1.1.0/24 network and the 172.16.45.0/24 network.
What should you do?

A. Configure global load balancing to point 172.16.45.0/24 to the correct instance.
B. Create unique DNS records for each service that sends traffic to the desired IP address.
C. Configure an alias-IP range of 172.16.45.0/24 on the virtual instances within the VPC subnet of 10.1.1.0/24.
D. Use VPC peering to allow traffic to route between the 10.1.0.0/24 network and the 172.16.45.0/24network.

Answer: C

NEW QUESTION 112
Your company's Google Cloud-deployed, streaming application supports multiple languages. The application development team has asked you how they should support splitting audio and video traffic to different backend Google Cloud storage buckets. They want to use URL maps and minimize operational overhead. They are currently using the following directory structure:
/fr/video
/en/video
/es/video
/../video
/fr/audio
/en/audio
/es/audio
/../audio
Which solution should you recommend?

A. Rearrange the directory structure, create a URL map and leverage a path rule such as /video/* and/audio/*.
B. Rearrange the directory structure, create DNS hostname entries for video and audio and leverage a path rule such as /video/* and /audio/*.
C. Leave the directory structure as-is, create a URL map and leverage a path rule such as \/[a-z]{2}\/video and \/[a-z]{2}\/audio.
D. Leave the directory structure as-is, create a URL map and leverage a path rule such as /*/video and /*/ audio.

Answer: A

Explanation:
https://cloud.google.com/load-balancing/docs/url-map#configuring_url_maps
Path matcher constraints Path matchers and path rules have the following constraints: A path rule can only include a wildcard character (*) after a forward slash character (/). For example, /videos/* and /videos/hd/* are valid for path rules, but /videos* and /videos/hd* are not. Path rules do not use regular expression or substring matching. For example, path rules for either /videos/hd or /videos/hd/* do not apply to a URL with the path /video/hd-abcd. However, a path rule for /video/* does apply to that path. https://cloud.google.com/load-balancing/docs/url-map-concepts#pm-constraints

NEW QUESTION 117
In your company, two departments with separate GCP projects (code-dev and data-dev) in the same organization need to allow full cross-communication between all of their virtual machines in GCP. Each department has one VPC in its project and wants full control over their network. Neither department intends to recreate its existing computing resources. You want to implement a solution that minimizes cost.
Which two steps should you take? (Choose two.)

A. Connect both projects using Cloud VPN.
B. Connect the VPCs in project code-dev and data-dev using VPC Network Peering.
C. Enable Shared VPC in one project (
D. g., code-dev), and make the second project (
E. g., data-dev) a service project.
F. Enable firewall rules to allow all ingress traffic from all subnets of project code-dev to all instances in project data-dev, and vice versa.
G. Create a route in the code-dev project to the destination prefixes in project data-dev and use nexthop as the default gateway, and vice versa.

Answer: BD

NEW QUESTION 119
Your on-premises data center has 2 routers connected to your Google Cloud environment through a VPN on each router. All applications are working correctly; however, all of the traffic is passing across a single VPN instead of being load-balanced across the 2 connections as desired.
During troubleshooting you find:
• Each on-premises router is configured with a unique ASN.
• Each on-premises router is configured with the same routes and priorities.
• Both on-premises routers are configured with a VPN connected to a single Cloud Router.
• BGP sessions are established between both on-premises routers and the Cloud Router.
• Only 1 of the on-premises router's routes are being added to the routing table. What is the most likely cause of this problem?

A. The on-premises routers are configured with the same routes.
B. A firewall is blocking the traffic across the second VPN connection.
C. You do not have a load balancer to load-balance the network traffic.
D. The ASNs being used on the on-premises routers are different.

Answer: D

Explanation:
https://cloud.google.com/network-connectivity/docs/router/support/troubleshooting#ecmp

NEW QUESTION 120
Your organization has a Google Cloud Virtual Private Cloud (VPC) with subnets in us-east1, us-west4, and europe-west4 that use the default VPC configuration. Employees in a branch office in Europe need to access the resources in the VPC using HA VPN. You configured the HA VPN associated with the Google Cloud VPC for your organization with a Cloud Router deployed in europe-west4. You need to ensure that the users in the branch office can quickly and easily access all resources in the VPC. What should you do?

A. Create custom advertised routes for each subnet.
B. Configure each subnet's VPN connections to use Cloud VPN to connect to the branch office.
C. Configure the VPC dynamic routing mode to Global.
D. Set the advertised routes to Global for the Cloud Router.

Answer: C

NEW QUESTION 124
You are using a third-party next-generation firewall to inspect traffic. You created a custom route of 0.0.0.0/0 to route egress traffic to the firewall. You want to allow your VPC instances without public IP addresses to access the BigQuery and Cloud Pub/Sub APIs, without sending the traffic through the firewall.
Which two actions should you take? (Choose two.)

A. Turn on Private Google Access at the subnet level.
B. Turn on Private Google Access at the VPC level.
C. Turn on Private Services Access at the VPC level.
D. Create a set of custom static routes to send traffic to the external IP addresses of Google APIs and services via the default internet gateway.
E. Create a set of custom static routes to send traffic to the internal IP addresses of Google APIs and services via the default internet gateway.

Answer: AD

Explanation:
https://cloud.google.com/vpc/docs/private-access-options#pga Private Google Access VM instances that only have internal IP addresses (no external IP addresses) can use Private Google Access. They can reach the_external IP addresses_ of Google APIs and services.

NEW QUESTION 128
You have provisioned a Dedicated Interconnect connection of 20 Gbps with a VLAN attachment of 10 Gbps. You recently noticed a steady increase in ingress traffic on the Interconnect connection from the on-premises data center. You need to ensure that your end users can achieve the full 20 Gbps throughput as quickly as possible. Which two methods can you use to accomplish this? (Choose two.)

A. Configure an additional VLAN attachment of 10 Gbps in another regio
B. Configure the on-premises router to advertise routes with the same multi-exit discriminator (MED).
C. Configure an additional VLAN attachment of 10 Gbps in the same regio
D. Configure the on-premises router to advertise routes with the same multi-exit discriminator (MED).
E. From the Google Cloud Console, modify the bandwidth of the VLAN attachment to 20 Gbps.
F. From the Google Cloud Console, request a new Dedicated Interconnect connection of 20 Gbps, and configure a VLAN attachment of 10 Gbps.
G. Configure Link Aggregation Control Protocol (LACP) on the on-premises router to use the 20-Gbps Dedicated Interconnect connection.

Answer: CE

NEW QUESTION 130
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

Professional-Cloud-Network-Engineer Practice Exam Features:

* Professional-Cloud-Network-Engineer Questions and Answers Updated Frequently

* Professional-Cloud-Network-Engineer Practice Questions Verified by Expert Senior Certified Staff

* Professional-Cloud-Network-Engineer Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* Professional-Cloud-Network-Engineer Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year