Google

Exam Questions Professional-Cloud-Network-Engineer

Google Cloud Certified - Professional Cloud Network Engineer

NEW QUESTION 1
You built a web application with several containerized microservices. You want to run those microservices on Cloud Run. You must also ensure that the services are highly available to your customers with low latency. What should you do?

A. Deploy the Cloud Run services to multiple availability zone
B. Create a global TCP load balance
C. Addthe Cloud Run endpoints to its backend service.
D. Deploy the Cloud Run services to multiple region
E. Create serverless network endpoint groups (NEGs) that point to the service
F. Create a global HTTPS load balancer, and attach the serverless NEGs as backend services of the load balancer.
G. Deploy the Cloud Run services to multiple availability zone
H. Create Cloud Endpoints that point to the service
I. Create a global HTTPS load balancer, and attach the Cloud Endpoints to its backend
J. Deploy the Cloud Run services to multiple region
K. Configure a round-robin A record in Cloud DNS.

Answer: B

NEW QUESTION 2
You have a Cloud Storage bucket in Google Cloud project XYZ. The bucket contains sensitive data. You need to design a solution to ensure that only instances belonging to VPCs under project XYZ can access the data stored in this Cloud Storage bucket. What should you do?

A. Configure Private Google Access to privately access the Cloud Storage service using private IP addresses.
B. Configure a VPC Service Controls perimeter around project XYZ, and include storage.googleapis.com as a restricted service in the service perimeter.
C. Configure Cloud Storage with projectPrivate Access Control List (ACL) that gives permission to the project team based on their roles.
D. Configure Private Service Connect to privately access Cloud Storage from all VPCs under project XYZ.

Answer: C

NEW QUESTION 3
You have just deployed your infrastructure on Google Cloud. You now need to configure the DNS to meet the following requirements:
Your on-premises resources should resolve your Google Cloud zones. Your Google Cloud resources should resolve your on-premises zones.
You need the ability to resolve ".internal" zones provisioned by Google Cloud. What should you do?

A. Configure an outbound server policy, and set your alternative name server to be your on-premises DNS resolve
B. Configure your on-premises DNS resolver to forward Google Cloud zone queries to Google's public DNS 8.8.8.8.
C. Configure both an inbound server policy and outbound DNS forwarding zones with the target as the on-premises DNS resolve
D. Configure your on-premises DNS resolver to forward Google Cloud zone queries to Google Cloud's DNS resolver.
E. Configure an outbound DNS server policy, and set your alternative name server to be your on-premises DNS resolve
F. Configure your on-premises DNS resolver to forward Google Cloud zone queries to Google Cloud's DNS resolver.
G. Configure Cloud DNS to DNS peer with your on-premises DNS resolve
H. Configure your on-premises DNS resolver to forward Google Cloud zone queries to Google's public DNS 8.8.8.8.

Answer: A

NEW QUESTION 4
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 5
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 6

You have configured a service on Google Cloud that connects to an on-premises service via a Dedicated Interconnect. Users are reporting recent connectivity issues. You need to determine whether the traffic is being dropped because of firewall rules or a routing decision. What should you do?

A. Use the Network Intelligence Center Connectivity Tests to test the connectivity between the VPC and the on-premises network.
B. Use Network Intelligence Center Network Topology to check the traffic flow, and replay the traffic from the time period when the connectivity issue occurred.
C. Configure VPC Flow Log
D. Review the logs by filtering on the source and destination.
E. Configure a Compute Engine instance on the same VPC as the service running on Google Cloud to run a traceroute targeted at the on-premises service.

Answer: B

NEW QUESTION 7
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 8
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 9
Your company has provisioned 2000 virtual machines (VMs) in the private subnet of your Virtual Private Cloud (VPC) in the us-east1 region. You need to configure each VM to have a minimum of 128 TCP connections to a public repository so that users can download software updates and packages over the internet. You need to implement a Cloud NAT gateway so that the VMs are able to perform outbound NAT to the internet. You must ensure that all VMs can simultaneously connect to the public repository and download software updates and packages. Which two methods can you use to accomplish this? (Choose two.)

A. Configure the NAT gateway in manual allocation mode, allocate 2 NAT IP addresses, and update the minimum number of ports per VM to 256.
B. Create a second Cloud NAT gateway with the default minimum number of ports configured per VM to 64.
C. Use the default Cloud NAT gateway's NAT proxy to dynamically scale using a single NAT IP address.
D. Use the default Cloud NAT gateway to automatically scale to the required number of NAT IP addresses, and update the minimum number of ports per VM to 128.
E. Configure the NAT gateway in manual allocation mode, allocate 4 NAT IP addresses, and update the minimum number of ports per VM to 128.

Answer: AB

NEW QUESTION 10
Your organization's security policy requires that all internet-bound traffic return to your on-premises data center through HA VPN tunnels before egressing to the internet, while allowing virtual machines (VMs) to leverage private Google APIs using private virtual IP addresses 199.36.153.4/30. You need to configure the routes to enable these traffic flows. What should you do?

A. Configure a custom route 0.0.0.0/0 with a priority of 500 whose next hop is the default internet gateway.Configure another custom route 199.36.153.4/30 with priority of 1000 whose next hop is the VPN tunnel back to the on-premises data center.
B. Configure a custom route 0.0.0.0/0 with a priority of 1000 whose next hop is the internet gateway.Configure another custom route 199.36.153.4/30 with a priority of 500 whose next hop is the VPN tunnel back to the on-premises data center.
C. Announce a 0.0.0.0/0 route from your on-premises router with a MED of 1000. Configure a custom route 199.36.153.4/30 with a priority of 1000 whose next hop is the default internet gateway.
D. Announce a 0.0.0.0/0 route from your on-premises router with a MED of 500. Configure another custom route 199.36.153.4/30 with a priority of 1000 whose next hop is the VPN tunnel back to the onpremises data center.

Answer: A

NEW QUESTION 10
You work for a university that is migrating to Google Cloud.
These are the cloud requirements:
On-premises connectivity with 10 Gbps Lowest latency access to the cloud Centralized Networking Administration Team
New departments are asking for on-premises connectivity to their projects. You want to deploy the most cost-efficient interconnect solution for connecting the campus to Google Cloud.
What should you do?

A. Use Shared VPC, and deploy the VLAN attachments and Dedicated Interconnect in the host project.
B. Use Shared VPC, and deploy the VLAN attachments in the service project
C. Connect the VLAN attachment to the Shared VPC's host project.
D. Use standalone projects, and deploy the VLAN attachments in the individual project
E. Connect the VLAN attachment to the standalone projects' Dedicated Interconnects.
F. Use standalone projects and deploy the VLAN attachments and Dedicated Interconnects in each of the individual projects.

Answer: A

NEW QUESTION 14
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 18
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 19
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 20
You are migrating to Cloud DNS and want to import your BIND zone file. Which command should you use?

A. gcloud dns record-sets import ZONE_FILE --zone MANAGED_ZONE
B. gcloud dns record-sets import ZONE_FILE --replace-origin-ns --zone MANAGED_ZONE
C. gcloud dns record-sets import ZONE_FILE --zone-file-format --zone MANAGED_ZONE
D. gcloud dns record-sets import ZONE_FILE --delete-all-existing --zone MANAGED ZONE

Answer: C

Explanation:

https://cloud.google.com/sdk/gcloud/reference/dns/record-sets/import

NEW QUESTION 25
Your company has just launched a new critical revenue-generating web application. You deployed the application for scalability using managed instance groups, autoscaling, and a network load balancer as frontend. One day, you notice severe bursty traffic that the caused autoscaling to reach the maximum number of instances, and users of your application cannot complete transactions. After an investigation, you think it as a DDOS attack. You want to quickly restore user access to your application and allow successful transactions while minimizing cost.
Which two steps should you take? (Choose two.)

A. Use Cloud Armor to blacklist the attacker's IP addresses.
B. Increase the maximum autoscaling backend to accommodate the severe bursty traffic.
C. Create a global HTTP(s) load balancer and move your application backend to this load balancer.
D. Shut down the entire application in GCP for a few hour
E. The attack will stop when the application is offline.
F. SSH into the backend compute engine instances, and view the auth logs and syslogs to further understand the nature of the attack.

Answer: BE

NEW QUESTION 29
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 31
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 32
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 37
You are designing a hub-and-spoke network architecture for your company's cloud-based environment. You need to make sure that all spokes are peered with the hub. The spokes must use the hub's virtual appliance for internet access.
The virtual appliance is configured in high-availability mode with two instances using an internal load balancer with IP address 10.0.0.5. What should you do?

A. Create a default route in the hub VPC that points to IP address 10.0.0.5.Delete the default internet gateway route in the hub VPC, and create a new higher-priority route that is tagged only to the appliances with a next hop of the default internet gateway.Export the custom routes in the hu
B. Import the custom routes in the spokes.
C. Create a default route in the hub VPC that points to IP address 10.0.0.5.Delete the default internet gateway route in the hub VPC, and create a new higher-priority route that is tagged only to the appliances with a next hop of the default internet gateway.Export the custom routes in the hu
D. Import the custom routes in the spoke

E. Delete the default internet gateway route of the spokes.
F. Create two default routes in the hub VPC that point to the next hop instances of the virtual appliances.Delete the default internet gateway route in the hub VPC, and create a new higher-priority route that is tagged only to the appliances with a next hop of the default internet gateway.Export the custom routes in the hu
G. Import the custom routes in the spokes.
H. Create a default route in the hub VPC that points to IP address 10.0.0.5.Delete the default internet gateway route in the hub VPC, and create a new higher-priority route that is tagged only to the appliances with a next hop of the default internet gateway.Create a new route in the spoke VPC that points to IP address 10.0.0.5.

Answer: B

NEW QUESTION 39
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 41
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 43
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 47
You create multiple Compute Engine virtual machine instances to be used as TFTP servers. Which type of load balancer should you use?

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

Answer: D

Explanation:
"TFTP is a UDP-based protocol. Servers listen on port 69 for the initial client-to-server packet to establish the TFTP session, then use a port above 1023 for all further packets during that session. Clients use ports above 1023" https://docstore.mik.ua/orelly/networking_2ndEd/fire/ch17_02.htm Besides, Google Cloud external TCP/UDP Network Load Balancing (after this referred to as Network Load Balancing) is a regional,
non-proxied load balancer. Network Load Balancing distributes traffic among virtual machine (VM) instances in the same region in a Virtual Private Cloud (VPC)

netw

NEW QUESTION 49
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 51
You successfully provisioned a single Dedicated Interconnect. The physical connection is at a colocation facility closest to us-west2. Seventy-five percent of your workloads are in us-east4, and the remaining twenty-five percent of your workloads are in us-central1. All workloads have the same network traffic profile. You need to minimize data transfer costs when deploying VLAN attachments. What should you do?

A. Keep the existing Dedicated interconnec
B. Deploy a VLAN attachment to a Cloud Router in us-west2, and use VPC global routing to access workloads in us-east4 and us-central1.
C. Keep the existing Dedicated Interconnec
D. Deploy a VLAN attachment to a Cloud Router in us-east4, and deploy another VLAN attachment to a Cloud Router in us-central1.
E. Order a new Dedicated Interconnect for a colocation facility closest to us-east4, and use VPC globalrouting to access workloads in us-central1.
F. Order a new Dedicated Interconnect for a colocation facility closest to us-central1, and use VPC global routing to access workloads in us-east4.

Answer: C

NEW QUESTION 54
Your company has 10 separate Virtual Private Cloud (VPC) networks, with one VPC per project in a single region in Google Cloud. Your security team requires each VPC network to have private connectivity to the main on-premises location via a Partner Interconnect connection in the same region. To optimize cost and operations, the same connectivity must be shared with all projects. You must ensure that all traffic between different projects, on-premises locations, and the internet can be inspected using the same third-party appliances. What should you do?

A. Configure the third-party appliances with multiple interfaces and specific Partner Interconnect VLAN attachments per projec
B. Create the relevant routes on the third-party appliances and VPC networks.
C. Configure the third-party appliances with multiple interfaces, with each interface connected to a separate VPC networ
D. Create separate VPC networks for on- premises and internet connectivit
E. Create the relevant routes on the third-party appliances and VPC networks.
F. Consolidate all existing projects' subnetworks into a single VP
G. Create separate VPC networks for on-premises and internet connectivit
H. Configure the third-party appliances with multiple interfaces, with each interface connected to a separate VPC networ
I. Create the relevant routes on the third-party appliances and VPC networks.
J. Configure the third-party appliances with multiple interface
K. Create a hub VPC network for all projects, and create separate VPC networks for on-premises and internet connectivit
L. Create the relevant routes on the third-party appliances and VPC network
M. Use VPC Network Peering to connect all projects' VPC networks to the hub VP
N. Export custom routes from the hub VPC and import on all projects' VPC networks.

Answer: D

NEW QUESTION 56
You are in the early stages of planning a migration to GCP. You want to test the functionality of your hybrid cloud design before you start to implement it in production. The design includes services running on a Compute Engine Virtual Machine instance that need to communicate to on-premises servers using private IP addresses. The on-premises servers have connectivity to the internet, but you have not yet established any Cloud Interconnect connections. You want to choose the lowest cost method of enabling connectivity between your instance and on-premises servers and complete the test in 24 hours.
Which connectivity method should you choose?

A. Cloud VPN
B. 50-Mbps Partner VLAN attachment
C. Dedicated Interconnect with a single VLAN attachment
D. Dedicated Interconnect, but don't provision any VLAN attachments

Answer: A

NEW QUESTION 58
You are designing a Partner Interconnect hybrid cloud connectivity solution with geo-redundancy across two metropolitan areas. You want to follow Google-recommended practices to set up the following region/metro pairs:
(region 1/metro 1)
(region 2/metro 2) What should you do?

A. Create a Cloud Router in region 1 with two VLAN attachments connected to metro1-zone1-x.Create a Cloud Router in region 2 with two VLAN attachments connected to metro1-zone2-x.
B. Create a Cloud Router in region 1 with one VLAN attachment connected to metro1-zone1-x.Create a Cloud Router in region 2 with two VLAN attachments connected to metro2-zone2-x.
C. Create a Cloud Router in region 1 with one VLAN attachment connected to metro1-zone2-x.Create a Cloud Router in region 2 with one VLAN attachment connected to metro2-zone2-x.
D. Create a Cloud Router in region 1 with one VLAN attachment connected to metro1-zone1-x and one VLAN attachment connected to metro1-zone2-x.Create a Cloud Router in region 2 with one VLAN attachment connected to metro2-zone1-x and one VLAN attachment to metro2-zone2-x.

Answer: B

NEW QUESTION 62
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 65
You are creating a new application and require access to Cloud SQL from VPC instances without public IP addresses.
Which two actions should you take? (Choose two.)

A. Activate the Service Networking API in your project.
B. Activate the Cloud Datastore API in your project.
C. Create a private connection to a service producer.
D. Create a custom static route to allow the traffic to reach the Cloud SQL API.
E. Enable Private Google Access.

Answer: CE

Explanation:
https://cloud.google.com/sql/docs/mysql/configure-private-services-access#console_1
C: If you are using private IP for any of your Cloud SQL instances, you only need to configure private services access one time for every Google Cloud project that has or needs to connect to a Cloud SQL instance. If your Google Cloud project has a Cloud SQL instance, you can either configure it yourself or let Cloud SQL do it for you to use private IP. Cloud SQL configures private services access for you when all the conditions below are true:
https://cloud.google.com/sql/docs/postgres/configure-private-services-access#before_you_begin
E: You can enable Private Google access on a subnet level and any VMs on that subnet can access Google APIs by using their internal IP address.
https://cloud.google.com/vpc/docs/configure-private-google-access

NEW QUESTION 67
You have recently been put in charge of managing identity and access management for your organization. You have several projects and want to use scripting and automation wherever possible. You want to grant the editor role to a project member.
Which two methods can you use to accomplish this? (Choose two.)

A. GetIamPolicy() via REST API
B. setIamPolicy() via REST API
C. gcloud pubsub add-iam-policy-binding Sprojectname --member user:Susername --role roles/editor
D. gcloud projects add-iam-policy-binding Sprojectname --member user:Susername --role roles/editor
E. Enter an email address in the Add members field, and select the desired role from the drop-down menu in the GCP Console.

Answer: DE

NEW QUESTION 69
Your company has a single Virtual Private Cloud (VPC) network deployed in Google Cloud with access from on-premises locations using Cloud Interconnect connections. Your company must be able to send traffic to Cloud Storage only through the Interconnect links while accessing other Google APIs and services over the public internet. What should you do?

A. Use the default public domains for all Google APIs and services.
B. Use Private Service Connect to access Cloud Storage, and use the default public domains for all other Google APIs and services.
C. Use Private Google Access, with restricted.googleapis.com virtual IP addresses for Cloud Storage and private.googleapis.com for all other Google APIs and services.
D. Use Private Google Access, with private.googleapis.com virtual IP addresses for Cloud Storage and restricted.googleapis.com virtual IP addresses for all other Google APIs and services.

Answer: B

NEW QUESTION 72
You are designing a Google Kubernetes Engine (GKE) cluster for your organization. The current cluster size is expected to host 10 nodes, with 20 Pods per node and 150 services. Because of the migration of new services over the next 2 years, there is a planned growth for 100 nodes, 200 Pods per node, and 1500 services. You want to use VPC-native clusters with alias IP ranges, while minimizing address consumption.
How should you design this topology?

A. Create a subnet of size/25 with 2 secondary ranges of: /17 for Pods and /21 for Service
B. Create a VPC-native cluster and specify those ranges.
C. Create a subnet of size/28 with 2 secondary ranges of: /24 for Pods and /24 for Service
D. Create a VPC-native cluster and specify those range
E. When the services are ready to be deployed, resize the subnets.
F. Use gcloud container clusters create [CLUSTER NAME]--enable-ip-alias to create a VPC-native cluster.
G. Use gcloud container clusters create [CLUSTER NAME] to create a VPC-native cluster.

Answer: A

Explanation:
The service range setting is permanent and cannot be changed. Please see
https://stackoverflow.com/questions/60957040/how-to-increase-the-service-address-range-of-a-gke-cluster I think the correc tanswer is A since: Grow is expected to up to 100 nodes (that would be /25), then up to 200 pods per node (100 times 200 = 20000 so /17 is 32768), then 1500 services in a /21 (up to 2048)
https://docs.netgate.com/pfsense/en/latest/book/network/understanding-cidr-subnet-mask-notation.html

NEW QUESTION 73
You are configuring a new instance of Cloud Router in your Organization's Google Cloud environment to allow connection across a new Dedicated Interconnect to your data center Sales, Marketing, and IT each have a service project attached to the Organization's host project.
Where should you create the Cloud Router instance?

A. VPC network in all projects
B. VPC network in the IT Project
C. VPC network in the Host Project
D. VPC network in the Sales, Marketing, and IT Projects

Answer: C

NEW QUESTION 78
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 83
You have two Google Cloud projects in a perimeter to prevent data exfiltration. You need to move a third project inside the perimeter; however, the move could negatively impact the existing environment. You need to validate the impact of the change. What should you do?

A. Enable Firewall Rules Logging inside the third project.
B. Modify the existing VPC Service Controls policy to include the new project in dry run mode.
C. Monitor the Resource Manager audit logs inside the perimeter.
D. Enable VPC Flow Logs inside the third project, and monitor the logs for negative impact.

Answer: B

NEW QUESTION 86
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 90
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 94
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 97
.....

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