Google

Exam Questions Professional-Cloud-Network-Engineer

Google Cloud Certified - Professional Cloud Network Engineer

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
You are trying to update firewall rules in a shared VPC for which you have been assigned only Network Admin permissions. You cannot modify the firewall rules.
Your organization requires using the least privilege necessary.
Which level of permissions should you request?

A. Security Admin privileges from the Shared VPC Admin.
B. Service Project Admin privileges from the Shared VPC Admin.
C. Shared VPC Admin privileges from the Organization Admin.
D. Organization Admin privileges from the Organization Admin.

Answer: A

Explanation:
A Shared VPC Admin can define a Security Admin by granting an IAM member the Security Admin (compute.securityAdmin) role to the host project. Security Admins manage firewall rules and SSL certificates.

NEW QUESTION 2
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 3
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 4
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 5
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 6
You need to define an address plan for a future new Google Kubernetes Engine (GKE) cluster in your Virtual Private Cloud (VPC). This will be a VPC-native cluster, and the default Pod IP range allocation will be used. You must pre-provision all the needed VPC subnets and their respective IP address ranges before cluster creation. The cluster will initially have a single node, but it will be scaled to a maximum of three nodes if necessary. You want to allocate the minimum number of Pod IP addresses. Which subnet mask should you use for the Pod IP address range?

A. /21
B. /22
C. /23
D. /25

Answer: A

NEW QUESTION 7
You created a new VPC network named Dev with a single subnet. You added a firewall rule for the network Dev to allow HTTP traffic only and enabled logging. When you try to log in to an instance in the subnet via Remote Desktop Protocol, the login fails. You look for the Firewall rules logs in Stackdriver Logging, but you do not see any entries for blocked traffic. You want to see the logs for blocked traffic.
What should you do?

A. Check the VPC flow logs for the instance.
B. Try connecting to the instance via SSH, and check the logs.
C. Create a new firewall rule to allow traffic from port 22, and enable logs.
D. Create a new firewall rule with priority 65500 to deny all traffic, and enable logs.

Answer: D

Explanation:
Ingress packets in VPC Flow Logs are sampled after ingress firewall rules. If an ingress firewall rule denies inbound packets, those packets are not sampled by VPC Flow Logs. We want to see the logs for blocked traffic so we have to look for them in firewall logs.
https://cloud.google.com/vpc/docs/flow-logs#key_properties

NEW QUESTION 8
You recently deployed two network virtual appliances in us-central1. Your network appliances provide connectivity to your on-premises network, 10.0.0.0/8. You need to configure the routing for your Virtual Private Cloud (VPC). Your design must meet the following requirements:
All access to your on-premises network must go through the network virtual appliances. Allow on-premises access in the event of a single network virtual appliance failure.
Both network virtual appliances must be used simultaneously. Which method should you use to accomplish this?

A. Configure two routes for 10.0.0.0/8 with different priorities, each pointing to separate network virtual appliances.
B. Configure an internal HTTP(S) load balancer with the two network virtual appliances as backends.Configure a route for 10.0.0.0/8 with the internal HTTP(S) load balancer as the next hop.
C. Configure a network load balancer for the two network virtual appliance
D. Configure a route for 10.0.0.0/8 with the network load balancer as the next hop.
E. Configure an internal TCP/UDP load balancer with the two network virtual appliances as backends.Configure a route for 10.0.0.0/8 with the internal load balancer as the next hop.

Answer: B

NEW QUESTION 9
Your organization has Compute Engine instances in us-east1, us-west2, and us-central1. Your organization also has an existing Cloud Interconnect physical connection in the East Coast of the United States with a single VLAN attachment and Cloud Router in us-east1. You need to provide a design with high availability and ensure that if a region goes down, you still have access to all your other Virtual Private Cloud (VPC) subnets. You need to accomplish this in the most cost-effective manner possible. What should you do?

A. Configure your VPC routing in regional mode.Add an additional Cloud Interconnect VLAN attachment in the us-east1 region, and configure a Cloud Router in us-east1.
B. Configure your VPC routing in global mode.Add an additional Cloud Interconnect VLAN attachment in the us-east1 region, and configure a Cloud Router in us-east1.
C. Configure your VPC routing in global mode.Add an additional Cloud Interconnect VLAN attachment in the us-west2 region, and configure a Cloud Router in us-west2.
D. Configure your VPC routing in regional mode.Add additional Cloud Interconnect VLAN attachments in the us-west2 and us-central1 regions, and configure Cloud Routers in us-west2 and us-central1.

Answer: B

NEW QUESTION 10
You are using a 10-Gbps direct peering connection to Google together with the gsutil tool to upload files to Cloud Storage buckets from on-premises servers. The on-premises servers are 100 milliseconds away from the Google peering point. You notice that your uploads are not using the full 10-Gbps bandwidth available to you. You want to optimize the bandwidth utilization of the connection.
What should you do on your on-premises servers?

A. Tune TCP parameters on the on-premises servers.
B. Compress files using utilities like tar to reduce the size of data being sent.
C. Remove the -m flag from the gsutil command to enable single-threaded transfers.
D. Use the perfdiag parameter in your gsutil command to enable faster performance: gsutil perfdiag gs://[BUCKET NAME].

Answer: A

Explanation:
https://cloud.google.com/solutions/tcp-optimization-for-network-performance-in-gcp-and-hybrid https://cloud.google.com/solutions/tcp-optimization-for-network-performance-in-gcp-and-hybrid
https://cloud.google.com/blog/products/gcp/5-steps-to-better-gcp-network-performance?hl=ml

NEW QUESTION 10
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 12
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 14
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 19
You are maintaining a Shared VPC in a host project. Several departments within your company have infrastructure in different service projects attached to the Shared VPC and use Identity and Access Management (IAM) permissions to manage the cloud resources in those projects. VPC Network Peering is also set up between the Shared VPC and a common services VPC that is not in a service project. Several users are experiencing failed connectivity between certain instances in different Shared VPC service projects and between certain instances and the internet. You need to validate the network configuration to identify whether a misconfiguration is the root cause of the problem. What should you do?

A. Review the VPC audit logs in Cloud Logging for the affected instances.
B. Use Secure Shell (SSH) to connect to the affected Compute Engine instances, and run a series of PING tests to the other affected endpoints and the 8.8.8.8 IPv4 address.
C. Run Connectivity Tests from Network Intelligence Center to check connectivity between the affected endpoints in your network and the internet.
D. Enable VPC Flow Logs for all VPCs, and review the logs in Cloud Logging for the affected instances.

Answer: C

NEW QUESTION 22
You need to restrict access to your Google Cloud load-balanced application so that only specific IP addresses can connect.
What should you do?

A. Create a secure perimeter using the Access Context Manager feature of VPC Service Controls and restrict access to the source IP range of the allowed clients and Google health check IP ranges.
B. Create a secure perimeter using VPC Service Controls, and mark the load balancer as a service restricted to the source IP range of the allowed clients and Google health check IP ranges.
C. Tag the backend instances "application," and create a firewall rule with target tag "application" and the source IP range of the allowed clients and Google health check IP ranges.
D. Label the backend instances "application," and create a firewall rule with the target label "application" and the source IP range of the allowed clients and Google health check IP ranges.

Answer: C

Explanation:
https://cloud.google.com/load-balancing/docs/https/setting-up-https#sendtraffic

NEW QUESTION 23
You have a storage bucket that contains the following objects:
- folder-a/image-a-1.jpg
- folder-a/image-a-2.jpg
- folder-b/image-b-1.jpg
- folder-b/image-b-2.jpg
Cloud CDN is enabled on the storage bucket, and all four objects have been successfully cached. You want to remove the cached copies of all the objects with the prefix folder-a, using the minimum number of commands.
What should you do?

A. Add an appropriate lifecycle rule on the storage bucket.
B. Issue a cache invalidation command with pattern /folder-a/*.
C. Make sure that all the objects with prefix folder-a are not shared publicly.
D. Disable Cloud CDN on the storage bucke
E. Wait 90 second
F. Re-enable Cloud CDN on the storage bucket.

Answer: B

Explanation:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Invalidation.html

NEW QUESTION 24
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 26
You created a VPC network named Retail in auto mode. You want to create a VPC network named Distribution and peer it with the Retail VPC.
How should you configure the Distribution VPC?

A. Create the Distribution VPC in auto mod
B. Peer both the VPCs via network peering.
C. Create the Distribution VPC in custom mod
D. Use the CIDR range 10.0.0.0/9. Create the necessary subnets, and then peer them via network peering.
E. Create the Distribution VPC in custom mod
F. Use the CIDR range 10.128.0.0/9. Create the necessary subnets, and then peer them via network peering.
G. Rename the default VPC as "Distribution" and peer it via network peering.

Answer: B

Explanation:
https://cloud.google.com/vpc/docs/vpc#ip-ranges

NEW QUESTION 31
You created a new VPC for your development team. You want to allow access to the resources in this VPC via SSH only.
How should you configure your firewall rules?

A. Create two firewall rules: one to block all traffic with priority 0, and another to allow port 22 with priority 1000.

B. Create two firewall rules: one to block all traffic with priority 65536, and another to allow port 3389 with priority 1000.
C. Create a single firewall rule to allow port 22 with priority 1000.
D. Create a single firewall rule to allow port 3389 with priority 1000.

Answer: C

NEW QUESTION 33
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 35
Your company is running out of network capacity to run a critical application in the on-premises data center. You want to migrate the application to GCP. You also want to ensure that the Security team does not lose their ability to monitor traffic to and from Compute Engine instances.
Which two products should you incorporate into the solution? (Choose two.)

A. VPC flow logs
B. Firewall logs
C. Cloud Audit logs
D. Stackdriver Trace
E. Compute Engine instance system logs

Answer: AB

Explanation:
A: Using VPC Flow Logs VPC Flow Logs records a sample of network flows sent from and received by VM instances, including instances used as GKE nodes. These logs can be used for network monitoring, forensics, real-time security analysis, and expense optimization. https://cloud.google.com/vpc/docs/using-flow-logs
(B): Firewall Rules Logging overview Firewall Rules Logging allows you to audit, verify, and analyze the effects of your firewall rules. For example, you can determine if a firewall rule designed to deny traffic is functioning
as intended. Firewall Rules Logging is also useful if you need to determine how many connections are affected by a given firewall rule. You enable Firewall Rules Logging individually for each firewall rule whose connections you need to log. Firewall Rules Logging is an option for any firewall rule, regardless of the action (allow or deny) or direction (ingress or egress) of the rule.
https://cloud.google.com/vpc/docs/firewall-rules-logging

NEW QUESTION 39
Your company offers a popular gaming service. Your instances are deployed with private IP addresses, and external access is granted through a global load balancer. You believe you have identified a potential malicious actor, but aren't certain you have the correct client IP address. You want to identify this actor while minimizing disruption to your legitimate users.
What should you do?

A. Create a Cloud Armor Policy rule that denies traffic and review necessary logs.
B. Create a Cloud Armor Policy rule that denies traffic, enable preview mode, and review necessary logs.
C. Create a VPC Firewall rule that denies traffic, enable logging and set enforcement to disabled, and review necessary logs.
D. Create a VPC Firewall rule that denies traffic, enable logging and set enforcement to enabled, and review necessary logs.

Answer: B

Explanation:
https://cloud.google.com/armor/docs/security-policy-concepts#preview_mode

NEW QUESTION 42
You are responsible for designing a new connectivity solution for your organization's enterprise network to access and use Google Workspace. You have an existing Shared VPC with Compute Engine instances in us-west1. Currently, you access Google Workspace via your service provider's internet access. You want to set up a direct connection between your network and Google. What should you do?

A. Order a Dedicated Interconnect connection in the same metropolitan are
B. Create a VLAN attachment, a Cloud Router in us-west1, and a Border Gateway Protocol (BGP) session between your Cloud Router and your router.
C. Order a Direct Peering connection in the same metropolitan are
D. Configure a Border Gateway Protocol (BGP) session between Google and your router.
E. Configure HA VPN in us-west1. Configure a Border Gateway Protocol (BGP) session between your Cloud Router and your on-premises data center.
F. Order a Carrier Peering connection in the same metropolitan are
G. Configure a Border Gateway Protocol (BGP) session between Google and your router.

Answer: B

NEW QUESTION 45
Your organization is deploying a single project for 3 separate departments. Two of these departments require network connectivity between each other, but the third department should remain in isolation. Your design should create separate network administrative domains between these departments. You want to

minimize operational overhead.
How should you design the topology?

A. Create a Shared VPC Host Project and the respective Service Projects for each of the 3 separate departments.
B. Create 3 separate VPCs, and use Cloud VPN to establish connectivity between the two appropriate VPCs.
C. Create 3 separate VPCs, and use VPC peering to establish connectivity between the two appropriate VPCs.
D. Create a single project, and deploy specific firewall rule
E. Use network tags to isolate access between the departments.

Answer: C

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

NEW QUESTION 50
Your end users are located in close proximity to us-east1 and europe-west1. Their workloads need to communicate with each other. You want to minimize cost and increase network efficiency.
How should you design this topology?

A. Create 2 VPCs, each with their own regions and individual subnet
B. Create 2 VPN gateways to establish connectivity between these regions.
C. Create 2 VPCs, each with their own region and individual subnet
D. Use external IP addresses on the instances to establish connectivity between these regions.
E. Create 1 VPC with 2 regional subnet
F. Create a global load balancer to establish connectivity between the regions.
G. Create 1 VPC with 2 regional subnet
H. Deploy workloads in these subnets and have them communicate using private RFC1918 IP addresses.

Answer: D

Explanation:
https://cloud.google.com/vpc/docs/using-vpc#create-auto-network
We create one VPC network in auto mode that creates one subnet in each Google Cloud region automatically. So, region us-east1 and europe-west1 are in the same network and they can communicate using their internal IP address even though they are in different Regions. They take advantage of Google's global fiber network.

NEW QUESTION 54
You have configured Cloud CDN using HTTP(S) load balancing as the origin for cacheable content. Compression is configured on the web servers, but responses served by Cloud CDN are not compressed.
What is the most likely cause of the problem?

A. You have not configured compression in Cloud CDN.
B. You have configured the web servers and Cloud CDN with different compression types.
C. The web servers behind the load balancer are configured with different compression types.
D. You have to configure the web servers to compress responses even if the request has a Via header.

Answer: D

Explanation:
If responses served by Cloud CDN are not compressed but should be, check that the web server software running on your instances is configured to compress responses. By default, some web server software will automatically disable compression for requests that include a Via header. The presence of a Via header indicates the request was forwarded by a proxy. HTTP proxies such as HTTP(S) load balancing add a Via header to each request as required by the HTTP specification. To enable compression, you may have to override your web server's default configuration to tell it to compress responses even if the request had a Via header.

NEW QUESTION 58
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 61
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 62
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 63
You are configuring an HA VPN connection between your Virtual Private Cloud (VPC) and on-premises network. The VPN gateway is named VPN_GATEWAY_1. You need to restrict VPN tunnels created in the project to only connect to your on-premises VPN public IP address: 203.0.113.1/32. What should you do?

A. Configure a firewall rule accepting 203.0.113.1/32, and set a target tag equal to VPN_GATEWAY_1.
B. Configure the Resource Manager constraint constraints/compute.restrictVpnPeerIPs to use an allowList consisting of only the 203.0.113.1/32 address.
C. Configure a Google Cloud Armor security policy, and create a policy rule to allow 203.0.113.1/32.
D. Configure an access control list on the peer VPN gateway to deny all traffic except 203.0.113.1/32, and attach it to the primary external interface.

Answer: B

NEW QUESTION 66
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 71
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 72
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 77
You are migrating a three-tier application architecture from on-premises to Google Cloud. As a first step in the migration, you want to create a new Virtual Private Cloud (VPC) with an external HTTP(S) load balancer. This load balancer will forward traffic back to the on-premises compute resources that run the presentation tier. You need to stop malicious traffic from entering your VPC and consuming resources at the edge, so you must configure this policy to filter IP addresses and stop cross-site scripting (XSS) attacks. What should you do?

A. Create a Google Cloud Armor policy, and apply it to a backend service that uses an unmanaged instance group backend.
B. Create a hierarchical firewall ruleset, and apply it to the VPC's parent organization resource node.
C. Create a Google Cloud Armor policy, and apply it to a backend service that uses an internet network endpoint group (NEG) backend.
D. Create a VPC firewall ruleset, and apply it to all instances in unmanaged instance groups.

Answer: C

NEW QUESTION 81
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 86
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 91
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 94
Your company has separate Virtual Private Cloud (VPC) networks in a single region for two departments: Sales and Finance. The Sales department's VPC network already has connectivity to on-premises locations using HA VPN, and you have confirmed that the subnet ranges do not overlap. You plan to peer both VPC networks to use the same HA tunnels for on-premises connectivity, while providing internet connectivity for the Google Cloud workloads through Cloud NAT. Internet access from the on-premises locations should not flow through Google Cloud. You need to propagate all routes between the Finance department and on-premises locations. What should you do?

A. Peer the two VPCs, and use the default configuration for the Cloud Routers.
B. Peer the two VPCs, and use Cloud Router's custom route advertisements to announce the peered VPC network ranges to the on-premises locations.
C. Peer the two VPC
D. Configure VPC Network Peering to export custom routes from Sales and import custom routes on Finance's VPC networ
E. Use Cloud Router's custom route advertisements to announce a default route to the on-premises locations.
F. Peer the two VPC
G. Configure VPC Network Peering to export custom routes from Sales and import custom routes on Finance's VPC networ
H. Use Cloud Router's custom route advertisements to announce the peered VPC network ranges to the on-premises locations.

Answer: A

NEW QUESTION 96
Your company has recently installed a Cloud VPN tunnel between your on-premises data center and your Google Cloud Virtual Private Cloud (VPC). You need to configure access to the Cloud Functions API for your on-premises servers. The configuration must meet the following requirements:
Certain data must stay in the project where it is stored and not be exfiltrated to other projects.
Traffic from servers in your data center with RFC 1918 addresses do not use the internet to access Google Cloud APIs.
All DNS resolution must be done on-premises.
The solution should only provide access to APIs that are compatible with VPC Service Controls. What should you do?

A. Create an A record for private.googleapis.com using the 199.36.153.8/30 address range.Create a CNAME record for *.googleapis.com that points to the A record.Configure your on-premises routers to use the Cloud VPN tunnel as the next hop for the addresses you used in the A record.Remove the default internet gateway from the VPC where your Cloud VPN tunnel terminates.
B. Create an A record for restricted.googleapis.com using the 199.36.153.4/30 address range.Create a CNAME record for *.googleapis.com that points to the A record.Configure your on-premises routers to use the Cloud VPN tunnel as the next hop for the addresses you used in the A record.Configure your on-premises firewalls to allow traffic to the restricted.googleapis.com addresses.
C. Create an A record for restricted.googleapis.com using the 199.36.153.4/30 address range.Create a CNAME record for *.googleapis.com that points to the A record.Configure your on-premises routers to use the Cloud VPN tunnel as the next hop for the addresses you used in the A record.Remove the default internet gateway from the VPC where your Cloud VPN tunnel terminates.
D. Create an A record for private.googleapis.com using the 199.36.153.8/30 address range.Create a CNAME record for *.googleapis.com that points to the A record.Configure your on-premises routers to use the Cloud VPN tunnel as the next hop for the addresses you used in the A record.Configure your on-premises firewalls to allow traffic to the private.googleapis.com addresses.

Answer: C

NEW QUESTION 101
Your software team is developing an on-premises web application that requires direct connectivity to Compute Engine Instances in GCP using the RFC 1918 address space. You want to choose a connectivity solution from your on-premises environment to GCP, given these specifications:

- Your ISP is a Google Partner Interconnect provider.
- Your on-premises VPN device's internet uplink and downlink speeds are 10 Gbps.
- A test VPN connection between your on-premises gateway and GCP is performing at a maximum speed of 500 Mbps due to packet losses.
- Most of the data transfer will be from GCP to the on-premises environment.
- The application can burst up to 1.5 Gbps during peak transfers over the Interconnect.
- Cost and the complexity of the solution should be minimal.

How should you provision the connectivity solution?

A. Provision a Partner Interconnect through your ISP.
B. Provision a Dedicated Interconnect instead of a VPN.
C. Create multiple VPN tunnels to account for the packet losses, and increase bandwidth using ECMP.
D. Use network compression over your VPN to increase the amount of data you can send over your VPN.

Answer: A

Explanation:
Direct Interconnect will be too expensive and also an overkill for this requirement. Managing multiple tunnels that too with packet loss consideration is complex also. Whereas partner interconnect fits the bill with providing required bandwidth but not super expensive also once setup not too complex too manage.

NEW QUESTION 102
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 105
You need to create a GKE cluster in an existing VPC that is accessible from on-premises. You must meet the following requirements:

- IP ranges for pods and services must be as small as possible.
- The nodes and the master must not be reachable from the internet.
- You must be able to use kubectl commands from on-premises subnets to manage the cluster.

How should you create the GKE cluster?

A. • Create a private cluster that uses VPC advanced routes.•Set the pod and service ranges as /24.•Set up a network proxy to access the master.
B. • Create a VPC-native GKE cluster using GKE-managed IP ranges.•Set the pod IP range as /21 and service IP range as /24.•Set up a network proxy to access the master.
C. • Create a VPC-native GKE cluster using user-managed IP ranges.•Enable a GKE cluster network policy, set the pod and service ranges as /24.•Set up a network proxy to access the master.•Enable master authorized networks.
D. • Create a VPC-native GKE cluster using user-managed IP ranges.•Enable privateEndpoint on the cluster master.•Set the pod and service ranges as /24.•Set up a network proxy to access the master.•Enable master authorized networks.

Answer: D

Explanation:
Creating GKE private clusters with network proxies for controller access When you create a GKE private cluster with a private cluster controller endpoint, the cluster's controller node is inaccessible from the public internet, but it needs to be accessible for administration. By default, clusters can access the controller through its private endpoint, and authorized networks can be defined within the VPC network. To access the controller from on-premises or another VPC network, however, requires additional steps. This is because the VPC network that hosts the controller is owned by Google and cannot be accessed from resources connected through another VPC network peering connection, Cloud VPN or Cloud Interconnect. https://cloud.google.com/solutions/creating-kubernetes-engine-private-clusters-with-net-proxies

NEW QUESTION 108
Your company's on-premises network is connected to a VPC using a Cloud VPN tunnel. You have a static route of 0.0.0.0/0 with the VPN tunnel as its next hop defined in the VPC. All internet bound traffic currently passes through the on-premises network. You configured Cloud NAT to translate the primary IP addresses of Compute Engine instances in one region. Traffic from those instances will now reach the internet directly from their VPC and not from the on-premises network. Traffic from the virtual machines (VMs) is not translating addresses as expected. What should you do?

A. Lower the TCP Established Connection Idle Timeout for the NAT gateway.
B. Add firewall rules that allow ingress and egress of the external NAT IP address, have a target tag that is on the Compute Engine instances, and have a priority value higher than the priority value of the default route to the VPN gateway.
C. Add a default static route to the VPC with the default internet gateway as the next hop, the network tag associated with the Compute Engine instances, and a higher priority than the priority of the default route to the VPN tunnel.
D. Increase the default min-ports-per-vm setting for the Cloud NAT gateway.

Answer: A

NEW QUESTION 111
You need to ensure your personal SSH key works on every instance in your project. You want to accomplish this as efficiently as possible.
What should you do?

A. Upload your public ssh key to the project Metadata.
B. Upload your public ssh key to each instance Metadata.
C. Create a custom Google Compute Engine image with your public ssh key embedded.
D. Use gcloud compute ssh to automatically copy your public ssh key to the instance.

Answer: A

Explanation:
Overview By creating and managing SSH keys, you can let users access a Linux instance through third-party tools. An SSH key consists of the following files: A public SSH key file that is applied to instance-level metadata or project-wide metadata. A private SSH key file that the user stores on their local devices. If a user presents their private SSH key, they can use a third-party tool to connect to any instance that is configured with the matching public SSH key file, even if they aren't a member of your Google Cloud project. Therefore, you can control which instances a user can access by changing the public SSH key metadata for one or more instances. https://cloud.google.com/compute/docs/instances/adding-removing-ssh-keys#addkey

NEW QUESTION 112
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 113

.....

Relate Links

100% Pass Your Professional-Cloud-Network-Engineer Exam with Exambible Prep Materials

https://www.exambible.com/Professional-Cloud-Network-Engineer-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/