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 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
Your company just completed the acquisition of Altostrat (a current GCP customer). Each company has a separate organization in GCP and has implemented a custom DNS solution. Each organization will retain its current domain and host names until after a full transition and architectural review is done in one year. These are the assumptions for both GCP environments.
• Each organization has enabled full connectivity between all of its projects by using Shared VPC.
• Both organizations strictly use the 10.0.0.0/8 address space for their instances, except for bastion hosts (for accessing the instances) and load balancers for serving web traffic.
• There are no prefix overlaps between the two organizations.
• Both organizations already have firewall rules that allow all inbound and outbound traffic from the 10.0.0.0/8 address space.
• Neither organization has Interconnects to their on-premises environment.
You want to integrate networking and DNS infrastructure of both organizations as quickly as possible and with minimal downtime.
Which two steps should you take? (Choose two.)

A. Provision Cloud Interconnect to connect both organizations together.
B. Set up some variant of DNS forwarding and zone transfers in each organization.
C. Connect VPCs in both organizations using Cloud VPN together with Cloud Router.
D. Use Cloud DNS to create A records of all VMs and resources across all projects in both organizations.
E. Create a third organization with a new host project, and attach all projects from your company and Altostrat to it using shared VPC.

Answer: BC

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

NEW QUESTION 4
You have an application that is running in a managed instance group. Your development team has released an updated instance template which contains a new feature which was not heavily tested. You want to minimize impact to users if there is a bug in the new template.
How should you update your instances?

A. Manually patch some of the instances, and then perform a rolling restart on the instance group.
B. Using the new instance template, perform a rolling update across all instances in the instance group.Verify the new feature once the rollout completes.
C. Deploy a new instance group and canary the updated template in that grou
D. Verify the new feature in the new canary instance group, and then update the original instance group.
E. Perform a canary update by starting a rolling update and specifying a target size for your instances to receive the new templat
F. Verify the new feature on the canary instances, and then roll forward to the rest of the instances.

Answer: D

Explanation:
https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups#startin https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups

NEW QUESTION 5
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 6
You converted an auto mode VPC network to custom mode. Since the conversion, some of your Cloud Deployment Manager templates are no longer working.
You want to resolve the problem.
What should you do?

A. Apply an additional IAM role to the Google API's service account to allow custom mode networks.
B. Update the VPC firewall to allow the Cloud Deployment Manager to access the custom mode networks.
C. Explicitly reference the custom mode networks in the Cloud Armor whitelist.
D. Explicitly reference the custom mode networks in the Deployment Manager templates.

Answer: D

NEW QUESTION 7
You are responsible for configuring firewall policies for your company in Google Cloud. Your security team has a strict set of requirements that must be met to configure firewall rules.
Always allow Secure Shell (SSH) from your corporate IP address. Restrict SSH access from all other IP addresses.
There are multiple projects and VPCs in your Google Cloud organization. You need to ensure that other VPC firewall rules cannot bypass the security team's requirements. What should you do?

A. Configure a hierarchical firewall policy to the organization node to allow TCP port 22 for your corporate IP address with priority 0.Configure a hierarchical firewall policy to the organization node to deny TCP port 22 for all IP addresses with priority 1.
B. Configure a VPC firewall rule to allow TCP port 22 for your corporate IP address with priority 0.Configure a VPC firewall rule to deny TCP port 22 for all IP addresses with priority 1.
C. Configure a VPC firewall rule to allow TCP port 22 for your corporate IP address with priority 1.Configure a VPC firewall rule to deny TCP port 22 for all IP addresses with priority 0.
D. Configure a hierarchical firewall policy to the organization node to allow TCP port 22 for your corporate IP address with priority 1Configure a hierarchical firewall policy to the organization node to deny TCP port 22 for all IP addresses with priority 0.

Answer: A

NEW QUESTION 8
You have enabled HTTP(S) load balancing for your application, and your application developers have reported that HTTP(S) requests are not being distributed correctly to your Compute Engine Virtual Machine instances. You want to find data about how the request are being distributed.
Which two methods can accomplish this? (Choose two.)

A. On the Load Balancer details page of the GCP Console, click on the Monitoring tab, select your backend service, and look at the graphs.
B. In Stackdriver Error Reporting, look for any unacknowledged errors for the Cloud Load Balancers service.
C. In Stackdriver Monitoring, select Resources > Metrics Explorer and search for https/request_bytes_count metric.
D. In Stackdriver Monitoring, select Resources > Google Cloud Load Balancers and review the Key Metrics graphs in the dashboard.
E. In Stackdriver Monitoring, create a new dashboard and track the https/backend_request_count metric for the load balancer.

Answer: AE

NEW QUESTION 9
You need to enable Private Google Access for use by some subnets within your Virtual Private Cloud (VPC). Your security team set up the VPC to send all internet-bound traffic back to the on- premises data center for inspection before egressing to the internet, and is also implementing VPC Service Controls in the environment for API-level security control. You have already enabled the subnets for Private Google Access. What configuration changes should you make to enable Private Google Access while adhering to your security team's requirements?

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

Answer: C

NEW QUESTION 10
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 10
You need to configure a Google Kubernetes Engine (GKE) cluster. The initial deployment should have 5 nodes with the potential to scale to 10 nodes. The maximum number of Pods per node is 8. The number of services could grow from 100 to up to 1024. How should you design the IP schema to optimally meet this requirement?

A. Configure a /28 primary IP address range for the node IP addresse
B. Configure a (25 secondary IP range for the Pod
C. Configure a /22 secondary IP range for the Services.
D. Configure a /28 primary IP address range for the node IP addresse
E. Configure a /25 secondary IP range for the Pod
F. Configure a /21 secondary IP range for the Services.
G. Configure a /28 primary IP address range for the node IP addresse
H. Configure a /28 secondary IP range for the Pod
I. Configure a /21 secondary IP range for the Services.
J. Configure a /28 primary IP address range for the node IP addresse
K. Configure a /24 secondary IP range for the Pad
L. Configure a /22 secondary IP range for the Services.

Answer: A

NEW QUESTION 13
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 15
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 19
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 20
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 23
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 28
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 33
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 34
You recently deployed Compute Engine instances in regions us-west1 and us-east1 in a Virtual Private Cloud (VPC) with default routing configurations. Your company security policy mandates that virtual machines (VMs) must not have public IP addresses attached to them. You need to allow your instances to fetch updates from the internet while preventing external access. What should you do?

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

Answer: A

NEW QUESTION 35
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 36
Your organization uses a Shared VPC architecture with a host project and three service projects. You have Compute Engine instances that reside in the service projects. You have critical workloads in your on-premises data center. You need to ensure that the Google Cloud instances can resolve on-premises hostnames via the Dedicated Interconnect you deployed to establish hybrid connectivity. What should you do?

A. Create a Cloud DNS private forwarding zone in the host project of the Shared VPC that forwards the private zone to the on-premises DNS servers.In your Cloud Router, add a custom route advertisement for the IP 35.199.192.0/19 to the on-premises environment.
B. Create a Cloud DNS private forwarding zone in the host project of the Shared VPC that forwards the Private zone to the on-premises DNS servers.In your Cloud Router, add a custom route advertisement for the IP 169.254 169.254 to the on-premisesenvironment.
C. Configure a Cloud DNS private zone in the host project of the Shared VPC.Set up DNS forwarding to your Google Cloud private zone on your on-premises DNS servers to point to the inbound forwarder IP address in your host projectIn your Cloud Router, add a custom route advertisement for the IP 169.254 169 254 to the on-premises environment.
D. Configure a Cloud DNS private zone in the host project of the Shared VPC.Set up DNS forwarding to your Google Cloud private zone on your on-premises DNS servers to point to the inbound forwarder IP address in your host project.Configure a DNS policy in the Shared VPC to allow inbound query forwarding with your on-premises DNS server as the alternative DNS server.

Answer: D

NEW QUESTION 41
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 43
You want to use Cloud Interconnect to connect your on-premises network to a GCP VPC. You cannot meet Google at one of its point-of-presence (POP) locations, and your on-premises router cannot run a Border Gateway Protocol (BGP) configuration.
Which connectivity model should you use?

A. Direct Peering
B. Dedicated Interconnect
C. Partner Interconnect with a layer 2 partner
D. Partner Interconnect with a layer 3 partner

Answer: D

Explanation:
https://cloud.google.com/network-connectivity/docs/interconnect/concepts/partner-overview
For Layer 3 connections, your service provider establishes a BGP session between your Cloud Routers and their edge routers for each VLAN attachment. You don't need to configure BGP on your on-premises router. Google and your service provider automatically set the correct configurations.
https://cloud.google.com/network-connectivity/docs/interconnect/concepts/partner-overview#connectivity-type

NEW QUESTION 47
You have created a firewall with rules that only allow traffic over HTTP, HTTPS, and SSH ports. While testing, you specifically try to reach the server over multiple ports and protocols; however, you do not see any denied connections in the firewall logs. You want to resolve the issue.
What should you do?

A. Enable logging on the default Deny Any Firewall Rule.
B. Enable logging on the VM Instances that receive traffic.
C. Create a logging sink forwarding all firewall logs with no filters.
D. Create an explicit Deny Any rule and enable logging on the new rule.

Answer: D

Explanation:
https://cloud.google.com/vpc/docs/firewall-rules-logging#egress_deny_example
You can only enable Firewall Rules Logging for rules in a Virtual Private Cloud (VPC) network. Legacy networks are not supported. Firewall Rules Logging only records TCP and UDP connections. Although you can create a firewall rule applicable to other protocols, you cannot log their connections. You cannot enable Firewall Rules Logging for the implied deny ingress and implied allow egress rules. Log entries are written from the perspective of virtual machine (VM) instances. Log entries are only created if a firewall rule has logging enabled and if the rule applies to traffic sent to or from the VM. Entries are created according to the connection logging limits on a best effort basis. The number of connections that can be logged in a given interval is based on the machine type. Changes to firewall rules can be viewed in VPC audit logs. https://cloud.google.com/vpc/docs/firewall-rules-logging#specifications

NEW QUESTION 51
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 54
Your company has a security team that manages firewalls and SSL certificates. It also has a networking team that manages the networking resources. The networking team needs to be able to read firewall rules, but should not be able to create, modify, or delete them.
How should you set up permissions for the networking team?

A. Assign members of the networking team the compute.networkUser role.
B. Assign members of the networking team the compute.networkAdmin role.
C. Assign members of the networking team a custom role with only the compute.networks.* and the compute.firewalls.list permissions.
D. Assign members of the networking team the compute.networkViewer role, and add the compute.networks.use permission.

Answer: B

NEW QUESTION 57
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 60
Your company has a Virtual Private Cloud (VPC) with two Dedicated Interconnect connections in two different regions: us-west1 and us-east1. Each Dedicated Interconnect connection is attached to a Cloud Router in its respective region by a VLAN attachment. You need to configure a high availability failover path. By default, all ingress traffic from the on-premises environment should flow to the VPC using the us-west1 connection. If us-west1 is unavailable, you want traffic to be rerouted to us-east1. How should you configure the multi-exit discriminator (MED) values to enable this failover path?

A. Use regional routin
B. Set the us-east1 Cloud Router to a base priority of 100, and set the us-west1 CloudRouter to a base priority of 1
C. Use global routin
D. Set the us-east1 Cloud Router to a base priority of 100, and set the us-west1 Cloud Router to a base priority of 1
E. Use regional routin
F. Set the us-east1 Cloud Router to a base priority of 1000, and set the us-west1 Cloud Router to a base priority of 1
G. Use global routin
H. Set the us-east1 Cloud Router to a base priority of 1000, and set the us-west1 Cloud Router to a base priority of 1

Answer: A

NEW QUESTION 61
In your Google Cloud organization, you have two folders: Dev and Prod. You want a scalable and consistent way to enforce the following firewall rules for all virtual machines (VMs) with minimal cost:
Port 8080 should always be open for VMs in the projects in the Dev folder.
Any traffic to port 8080 should be denied for all VMs in your projects in the Prod folder. What should you do?

A. Create and associate a firewall policy with the Dev folder with a rule to open port 8080. Create and associate a firewall policy with the Prod folder with a rule to deny traffic to port 8080.
B. Create a Shared VPC for the Dev projects and a Shared VPC for the Prod project
C. Create a VPC firewall rule to open port 8080 in the Shared VPC for De
D. Create a firewall rule to deny traffic to port 8080 in the Shared VPC for Pro
E. Deploy VMs to those Shared VPCs.
F. In all VPCs for the Dev projects, create a VPC firewall rule to open port 8080. In all VPCs for the Prod projects, create a VPC firewall rule to deny traffic to port

8080.
G. Use Anthos Config Connector to enforce a security policy to open port 8080 on the Dev VMs and deny traffic to port 8080 on the Prod VMs.

Answer: A

NEW QUESTION 64
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 68
You have provisioned a Partner Interconnect connection to extend connectivity from your on-premises data center to Google Cloud. You need to configure a Cloud Router and create a VLAN attachment to connect to resources inside your VPC. You need to configure an Autonomous System number (ASN) to use with the associated Cloud Router and create the VLAN attachment.
What should you do?

A. Use a 4-byte private ASN 4200000000-4294967294.
B. Use a 2-byte private ASN 64512-65535.
C. Use a public Google ASN 15169.
D. Use a public Google ASN 16550.

Answer: B

NEW QUESTION 72
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 77
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 81
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 84
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 88
You are configuring your Google Cloud environment to connect to your on-premises network. Your configuration must be able to reach Cloud Storage APIs and your Google Kubernetes Engine nodes across your private Cloud Interconnect network. You have already configured a Cloud Router with your Interconnect VLAN attachments. You now need to set up the appropriate router advertisement configuration on the Cloud Router. What should you do?

A. Configure the route advertisement to the default setting.
B. On the on-premises router, configure a static route for the storage API virtual IP address which points to the Cloud Router's link-local IP address.
C. Configure the route advertisement to the custom setting, and manually add prefix 199.36.153.8/30 to the list of advertisement
D. Leave all other options as their default settings.
E. Configure the route advertisement to the custom setting, and manually add prefix 199.36.153.8/30 to the list of advertisement
F. Advertise all visible subnets to the Cloud Router.

Answer: C

NEW QUESTION 91
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 95
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 100
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 101
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 102
Your company has a single Virtual Private Cloud (VPC) network deployed in Google Cloud with access from your on-premises network using Cloud Interconnect. You must configure access only to Google APIs and services that are supported by VPC Service Controls through hybrid connectivity with a service level agreement (SLA) in place. What should you do?

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

Answer: B

NEW QUESTION 104
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 have recently engaged a traffic-scrubbing service and want to restrict your origin to allow connections only from the traffic-scrubbing service.
What should you do?

A. Create a Cloud Armor Security Policy that blocks all traffic except for the traffic-scrubbing service.
B. Create a VPC Firewall rule that blocks all traffic except for the traffic-scrubbing service.
C. Create a VPC Service Control Perimeter that blocks all traffic except for the traffic-scrubbing service.
D. Create IPTables firewall rules that block all traffic except for the traffic-scrubbing service.

Answer: A

Explanation:
Global load balancer will proxy the connection . thus no trace of session origin IP. you should use Cloud Armor to geofence your service.
https://cloud.google.com/load-balancing/docs/https

NEW QUESTION 106
You have the following private Google Kubernetes Engine (GKE) cluster deployment:

```
gcloud container clusters describe customer-1-cluster --zone us-central1-c

...

clusterIpv4Cidr: 192.168.36.0/24
endpoint: 192.168.38.2
ipAllocationPolicy:
  clusterIpv4Cidr: 192.168.36.0/24
  clusterIpv4CidrBlock: 192.168.36.0/24
  clusterSecondaryRangeName: customer-1-pods
  servicesIpv4Cidr: 192.168.37.0/24
  servicesIp4CidrBlock: 192.168.37.0/24
  servicesSecondaryRangeName: customer-1-svc
  useIpAliases: true

...

masterAuthorizedNetworksConfig:

...

privateClusterConfig:
  enablePrivateEndpoint: true
  enablePrivateNodes: true
  masterIpv4CidrBlock: 192.168.38.0/28
  privateEndpoint: 192.168.38.2
  publicEndpoint: 35.224.37.17

...

servicesIpv4Cidr: 192.162.37.0/24

...

subnetwork: customer-1-nodes
zone: us-central1-c
```

You have a virtual machine (VM) deployed in the same VPC in the subnetwork kubernetes-management with internal IP address 192.168.40 2/24 and no external IP address assigned. You need to communicate with the cluster master using kubectl. What should you do?

A. Add the network 192.168.40.0/24 to the masterAuthorizedNetworksConfi
B. Configure kubectl tocommunicate with the endpoint 192.168.38.2.
C. Add the network 192.168.38.0/28 to the masterAuthorizedNetworksConfi
D. Configure kubectl to communicate with the endpoint 192.168.38.2
E. Add the network 192.168.36.0/24 to the masterAuthorizedNetworksConfi
F. Configure kubectl to communicate with the endpoint 192.168.38.2
G. Add an external IP address to the VM, and add this IP address in the masterAuthorizedNetworksConfig.Configure kubectl to communicate with the endpoint 35.224.37.17.

Answer: A

NEW QUESTION 111
You need to create the network infrastructure to deploy a highly available web application in the us-east1 and us-west1 regions. The application runs on Compute Engine instances, and it does not require the use of a database. You want to follow Google-recommended practices. What should you do?

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

Answer: C

NEW QUESTION 116
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 120
You want to configure a NAT to perform address translation between your on-premises network blocks and GCP.
Which NAT solution should you use?

A. Cloud NAT
B. An instance with IP forwarding enabled
C. An instance configured with iptables DNAT rules
D. An instance configured with iptables SNAT rules

Answer: A

NEW QUESTION 123
You want to create a service in GCP using IPv6. What should you do?

A. Create the instance with the designated IPv6 address.
B. Configure a TCP Proxy with the designated IPv6 address.
C. Configure a global load balancer with the designated IPv6 address.
D. Configure an internal load balancer with the designated IPv6 address.

Answer: C

Explanation:
https://cloud.google.com/load-balancing/docs/load-balancing-overview mentions to use global load balancer for IPv6 termination.

NEW QUESTION 127
You have an HA VPN connection with two tunnels running in active/passive mode between your Virtual Private Cloud (VPC) and on-premises network. Traffic over the connection has recently increased from 1 gigabit per second (Gbps) to 4 Gbps, and you notice that packets are being dropped. You need to configure your VPN connection to Google Cloud to support 4 Gbps. What should you do?

A. Configure the remote autonomous system number (ASN) to 4096.
B. Configure a second Cloud Router to scale bandwidth in and out of the VPC.
C. Configure the maximum transmission unit (MTU) to its highest supported value.
D. Configure a second set of active/passive VPN tunnels.

Answer: D

NEW QUESTION 129
One instance in your VPC is configured to run with a private IP address only. You want to ensure that even if this instance is deleted, its current private IP address will not be automatically assigned to a different instance.
In the GCP Console, what should you do?

A. Assign a public IP address to the instance.
B. Assign a new reserved internal IP address to the instance.
C. Change the instance’s current internal IP address to static.
D. Add custom metadata to the instance with key internal-address and value reserved.

Answer: C

Explanation:
https://cloud.google.com/compute/docs/ip-addresses/reserve-static-internal-ip-address#reservenewip Since here https://cloud.google.com/compute/docs/ip-addresses/reserve-static-internal-ip-address#reservenewip it is written that "automatically allocated or an unused address from an existing subnet".

NEW QUESTION 131
You configured Cloud VPN with dynamic routing via Border Gateway Protocol (BGP). You added a custom route to advertise a network that is reachable over the VPN tunnel. However, the on-premises clients still cannot reach the network over the VPN tunnel. You need to examine the logs in Cloud Logging to confirm that the appropriate routers are being advertised over the VPN tunnel. Which filter should you use in Cloud Logging to examine the logs?

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

Answer: C

NEW QUESTION 135
In order to provide subnet level isolation, you want to force instance-A in one subnet to route through a security appliance, called instance-B, in another subnet. What should you do?

A. Create a more specific route than the system-generated subnet route, pointing the next hop to instance-B with no tag.
B. Create a more specific route than the system-generated subnet route, pointing the next hop to instance-B with a tag applied to instance-A.
C. Delete the system-generated subnet route and create a specific route to instance-B with a tag applied to instance-A.
D. Move instance-B to another VPC and, using multi-NIC, connect instance-B's interface to instance-A's networ
E. Configure the appropriate routes to force traffic through to instance-A.

Answer: B

NEW QUESTION 140
Your organization has a new security policy that requires you to monitor all egress traffic payloads from your virtual machines in region us-west2. You deployed an intrusion detection system (IDS) virtual appliance in the same region to meet the new policy. You now need to integrate the IDS into the environment to monitor all egress traffic payloads from us-west2. What should you do?

A. Enable firewall logging, and forward all filtered egress firewall logs to the IDS.
B. Enable VPC Flow Log
C. Create a sink in Cloud Logging to send filtered egress VPC Flow Logs to the IDS.
D. Create an internal TCP/UDP load balancer for Packet Mirroring, and add a packet mirroring policy filter for egress traffic.
E. Create an internal HTTP(S) load balancer for Packet Mirroring, and add a packet mirroring policy filter for egress traffic.

Answer: B

NEW QUESTION 144
You need to define an address plan for a future new GKE cluster in your 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: B

Explanation:
https://cloud.google.com/kubernetes-engine/docs/how-to/alias-ips#cluster_sizing_secondary_range_pods

NEW QUESTION 148
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 150
Your organization uses a hub-and-spoke architecture with critical Compute Engine instances in your Virtual Private Clouds (VPCs). You are responsible for the design of Cloud DNS in Google Cloud. You need to be able to resolve Cloud DNS private zones from your on-premises data center and enable on-premises name resolution from your hub-and-spoke VPC design. What should you do?

A. Configure a private DNS zone in the hub VPC, and configure DNS forwarding to the on-premises server.Configure DNS peering from the spoke VPCs to the hub VPC.
B. Configure a DNS policy in the hub VPC to allow inbound query forwarding from the spoke VPCs.Configure the spoke VPCs with a private zone, and set up DNS peering to the hub VPC.
C. Configure a DNS policy in the spoke VPCs, and configure your on-premises DNS as an alternate DNS server.Configure the hub VPC with a private zone, and set up DNS peering to each of the spoke VPCs.
D. Configure a DNS policy in the hub VPC, and configure the on-premises DNS as an alternate DNS server.Configure the spoke VPCs with a private zone, and set up DNS peering to the hub VPC.

Answer: C

NEW QUESTION 155
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 159
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 164
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 165
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 166
You want to set up two Cloud Routers so that one has an active Border Gateway Protocol (BGP) session, and the other one acts as a standby.
Which BGP attribute should you use on your on-premises router?

A. AS-Path
B. Community
C. Local Preference
D. Multi-exit Discriminator

Answer: D

NEW QUESTION 171
You recently deployed your application in Google Cloud. You need to verify your Google Cloud network configuration before deploying your on-premises workloads. You want to confirm that your Google Cloud network configuration allows traffic to flow from your cloud resources to your on- premises network. This validation should also analyze and diagnose potential failure points in your Google Cloud network configurations without sending any data plane test traffic. What should you do?

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

Answer: C

NEW QUESTION 173
You have several microservices running in a private subnet in an existing Virtual Private Cloud (VPC). You need to create additional serverless services that use Cloud Run and Cloud Functions to access the
microservices. The network traffic volume between your serverless services and private microservices is low. However, each serverless service must be able to communicate with any of your microservices. You want to implement a solution that minimizes cost. What should you do?

A. Deploy your serverless services to the serverless VP
B. Peer the serverless service VPC to the existing VP
C. Configure firewall rules to allow traffic between the serverless services and your existing microservices.
D. Create a serverless VPC access connector for each serverless servic
E. Configure the connectors to allow traffic between the serverless services and your existing microservices.
F. Deploy your serverless services to the existing VP
G. Configure firewall rules to allow traffic between the serverless services and your existing microservices.
H. Create a serverless VPC access connecto
I. Configure the serverless service to use the connector for communication to the microservices.

Answer: D

NEW QUESTION 176
You have the following firewall ruleset applied to all instances in your Virtual Private Cloud (VPC):

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

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

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

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

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

Answer: A

NEW QUESTION 178
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 179
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 183
You are the Organization Admin for your company. One of your engineers is responsible for setting up multiple host projects across multiple folders and sharing subnets with service projects. You need to enable the engineer's Identity and Access Management (IAM) configuration to complete their task in the fewest number of steps. What should you do?

A. Set up the engineer with Compute Shared VPC Admin IAM role at the folder level.
B. Set up the engineer with Compute Shared VPC Admin IAM role at the organization level.
C. Set up the engineer with Compute Shared VPC Admin IAM role and Project IAM Admin role at the folder level.
D. Set up the engineer with Compute Shared VPC Admin IAM role and Project IAM Admin role at the organization level.

Answer: B

NEW QUESTION 187
Your company's security team wants to limit the type of inbound traffic that can reach your web servers to protect against security threats. You need to configure the firewall rules on the web servers within your Virtual Private Cloud (VPC) to handle HTTP and HTTPS web traffic for TCP only. What should you do?

A. Create an allow on match ingress firewall rule with the target tag "web-server" to allow all IP addresses for TCP port 80.
B. Create an allow on match egress firewall rule with the target tag "web-server" to allow all IP addresses for TCP port 80.
C. Create an allow on match ingress firewall rule with the target tag "web-server" to allow all IP addresses for TCP ports 80 and 443.
D. Create an allow on match egress firewall rule with the target tag "web-server" to allow web server IP addresses for TCP ports 60 and 443.

Answer: C

NEW QUESTION 188
You are developing an HTTP API hosted on a Compute Engine virtual machine instance that must be invoked only by multiple clients within the same Virtual Private Cloud (VPC). You want clients to be able to get the IP address of the service. What should you do?

A. Reserve a static external IP address and assign it to an HTTP(S) load balancing service's forwarding rul
B. Clients should use this IP address to connect to the service.
C. Ensure that clients use Compute Engine internal DNS by connecting to the instance name with the url https://[INSTANCE_NAME].[ZONE].c.[PROJECT_ID].internal/.
D. Reserve a static external IP address and assign it to an HTTP(S) load balancing service's forwardingrul
E. Then, define an A record in Cloud DN
F. Clients should use the name of the A record to connect to the service.
G. Ensure that clients use Compute Engine internal DNS by connecting to the instance name with the url https://[API_NAME]/[API_VERSION]/.

Answer: C

NEW QUESTION 189
You are increasing your usage of Cloud VPN between on-premises and GCP, and you want to support more traffic than a single tunnel can handle. You want to increase the available bandwidth using Cloud VPN.
What should you do?

A. Double the MTU on your on-premises VPN gateway from 1460 bytes to 2920 bytes.
B. Create two VPN tunnels on the same Cloud VPN gateway that point to the same destination VPN gateway IP address.
C. Add a second on-premises VPN gateway with a different public IP addres
D. Create a second tunnel on the existing Cloud VPN gateway that forwards the same IP range, but points at the new on-premises gateway IP.
E. Add a second Cloud VPN gateway in a different region than the existing VPN gatewa
F. Create a new tunnel on the second Cloud VPN gateway that forwards the same IP range, but points to the existing on-premises VPN gateway IP address.

Answer: C

Explanation:
https://cloud.google.com/network-connectivity/docs/vpn/concepts/classic-topologies#redundancy-options

NEW QUESTION 194

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

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

Answer: C

NEW QUESTION 198
Your on-premises data center has 2 routers connected to your Google Cloud environment through a VPN on each router. All applications are working correctly; however, all of the traffic is passing across a single VPN instead of being load-balanced across the 2 connections as desired.
During troubleshooting you find:
• Each on-premises router is configured with a unique ASN.
• Each on-premises router is configured with the same routes and priorities.
• Both on-premises routers are configured with a VPN connected to a single Cloud Router.
• BGP sessions are established between both on-premises routers and the Cloud Router.
• Only 1 of the on-premises router's routes are being added to the routing table. What is the most likely cause of this problem?

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

Answer: D

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

NEW QUESTION 202
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 203
.....

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/