

Google

Exam Questions Professional-Cloud-Network-Engineer

Google Cloud Certified - Professional Cloud Network Engineer



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 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. 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 hub VPC.

Answer: A

NEW QUESTION 3

You are designing a new application that has backends internally exposed on port 800. The application will be exposed externally using both IPv4 and IPv6 via TCP on port 700. You want to ensure high availability for this application. What should you do?

- A. Create a network load balancer that used backend services containing one instance group with two instances.
- B. Create a network load balancer that uses a target pool backend with two instances.
- C. Create a TCP proxy that uses a zonal network endpoint group containing one instance.
- D. Create a TCP proxy that uses backend services containing an instance group with two instances.

Answer: D

NEW QUESTION 4

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 manually distribute 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 5

You want to use Partner Interconnect to connect your on-premises network with your VPC. You already have an Interconnect partner. What should you first?

- A. Log in to your partner's portal and request the VLAN attachment there.
- B. Ask your Interconnect partner to provision a physical connection to Google.
- C. Create a Partner Interconnect type VLAN attachment in the GCP Console and retrieve the pairing key.
- D. Run `gcloud compute interconnect attachments partner update <attachment> / -- region <region> --admin-enabled`.

Answer: B

Explanation:

<https://cloud.google.com/network-connectivity/docs/interconnect/concepts/partner-overview?hl=En#provisionin> "To provision a Partner Interconnect connection with a service provider, you start by connecting your on-premises network to a supported service provider. Work with the service provider to establish connectivity.

NEW QUESTION 6

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 7

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

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

Answer: B

NEW QUESTION 8

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 9

You have created an HTTP(S) load balanced service. You need to verify that your backend instances are responding properly. How should you configure the health check?

- A. Set request-path to a specific URL used for health checking, and set proxy-header to PROXY_V1.
- B. Set request-path to a specific URL used for health checking, and set host to include a custom host header that identifies the health check.
- C. Set request-path to a specific URL used for health checking, and set response to a string that the backend service will always return in the response body.
- D. Set proxy-header to the default value, and set host to include a custom host header that identifies the health check.

Answer: C

Explanation:

https://cloud.google.com/load-balancing/docs/health-check-concepts#content-based_health_checks

NEW QUESTION 10

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 10

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 bucket.
- E. Wait 90 seconds.
- F. Re-enable Cloud CDN on the storage bucket.

Answer: B

Explanation:

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

NEW QUESTION 15

You want to deploy a VPN Gateway to connect your on-premises network to GCP. You are using a non BGP-capable on-premises VPN device. You want to minimize downtime and operational overhead when your network grows. The device supports only IKEv2, and you want to follow Google-recommended practices.

What should you do?

- A. • Create a Cloud VPN instance. • Create a policy-based VPN tunnel per subnet. • Configure the appropriate local and remote traffic selectors to match your local and remote networks. • Create the appropriate static routes.
- B. • Create a Cloud VPN instance. • Create a policy-based VPN tunnel. • Configure the appropriate local and remote traffic selectors to match your local and remote networks. • Configure the appropriate static routes.
- C. • Create a Cloud VPN instance. • Create a route-based VPN tunnel. • Configure the appropriate local and remote traffic selectors to match your local and remote networks. • Configure the appropriate static routes.
- D. • Create a Cloud VPN instance. • Create a route-based VPN tunnel. • Configure the appropriate local and remote traffic selectors to 0.0.0.0/0. • Configure the appropriate static routes.

Answer: B

Explanation:

https://cloud.google.com/network-connectivity/docs/vpn/how-to/creating-static-vpns#creating_a_gateway_and_

NEW QUESTION 18

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 21

You have applications running in the us-west1 and us-east1 regions. You want to build a highly available VPN that provides 99.99% availability to connect your applications from your project to the cloud services provided by your partner's project while minimizing the amount of infrastructure required. Your partner's services are also in the us-west1 and us-east1 regions. You want to implement the simplest solution. What should you do?

- A. Create one Cloud Router and one HA VPN gateway in each region of your VPC and your partner's VPC.
- B. Connect your VPN gateways to the partner's gateway.
- C. Enable global dynamic routing in each VPC.
- D. Create one Cloud Router and one HA VPN gateway in the us-west1 region of your VPC.
- E. Create one OpenVPN Access Server in each region of your partner's VPC.
- F. Connect your VPN gateway to your partner's servers.
- G. Create one OpenVPN Access Server in each region of your VPC and your partner's VPC.
- H. Connect your servers to the partner's servers.
- I. Create one Cloud Router and one HA VPN gateway in the us-west1 region of your VPC and your partner's VPC.
- J. Connect your VPN gateways to the partner's gateways with a pair of tunnels.
- K. Enable global dynamic routing in each VPC.

Answer: A

NEW QUESTION 25

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 29

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 30

You need to give each member of your network operations team least-privilege access to create, modify, and delete Cloud Interconnect VLAN attachments. What should you do?

- A. Assign each user the editor role.
- B. Assign each user the compute.networkAdmin role.
- C. Give each user the following permissions only: compute.interconnectAttachments.create, compute.interconnectAttachments.get.
- D. Give each user the following permissions only: compute.interconnectAttachments.create, compute.interconnectAttachments.get, compute.routers.create, compute.routers.get, compute.routers.update.

Answer: D

Explanation:

<https://cloud.google.com/interconnect/docs/how-to/dedicated/creating-vlan-attachments>

NEW QUESTION 34

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

- A. Delete the default route in your VPC. Create a private Cloud DNS zone for googleapis.com, create a CNAME for *.googleapis.com to restricted googleapis.com, and create an A record for restricted googleapis.com that resolves to the addresses in 199.36.153.4/30. Create a static route in your VPC for the range 199.36.153.4/30 with the default internet gateway as the next hop.
- B. Delete the default route in your VPC and configure your on-premises router to advertise 0.0.0.0/0 via Border Gateway Protocol (BGP). Create a public Cloud DNS zone with a CNAME for *.google.com to private googleapis.com, create a CNAME for * googleapis.com to private googleapis.com, and create an A record for Private googleapis.com that resolves to the addresses in 199.36.153.8/30. Create a static route in your VPC for the range 199.36.153.8/30 with the default internet gateway as the next hop.
- C. Configure your on-premises router to advertise 0.0.0.0/0 via Border Gateway Protocol (BGP) with a lower priority (MED) than the default VPC route. Create a private Cloud DNS zone for googleapis.com, create a CNAME for * googleapis.com to private googleapis.com, and create an A record for private.googleapis.com that resolves to the addresses in 199.36.153.8/30. Create a static route in your VPC for the range 199.36.153.8/30 with the default internet gateway as the next hop.
- D. Delete the default route in your VPC and configure your on-premises router to advertise 0.0.0.0/0 via Border Gateway Protocol (BGP). Create a private Cloud DNS zone for googleapis.com, create a CNAME for * googleapis.com to Private googleapis.com, and create an A record for private.googleapis.com that resolves to the addresses in 199.36.153.8/30. Create a static route in your VPC for the range 199.36.153.8/30 with the default internet gateway as the next hop.

Answer: C

NEW QUESTION 38

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 40

You are designing a shared VPC architecture. Your network and security team has strict controls over which routes are exposed between departments. Your Production and Staging departments can communicate with each other, but only via specific networks. You want to follow Google-recommended practices. How should you design this topology?

- A. Create 2 shared VPCs within the shared VPC Host Project, and enable VPC peering between the
- B. Use firewall rules to filter access between the specific networks.
- C. Create 2 shared VPCs within the shared VPC Host Project, and create a Cloud VPN/Cloud Router between the
- D. Use Flexible Route Advertisement (FRA) to filter access between the specific networks.
- E. Create 2 shared VPCs within the shared VPC Service Project, and create a Cloud VPN/Cloud Router between the
- F. Use Flexible Route Advertisement (FRA) to filter access between the specific networks.
- G. Create 1 VPC within the shared VPC Host Project, and share individual subnets with the Service Projects to filter access between the specific networks.

Answer: D

NEW QUESTION 43

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 46

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 47

You are using the gcloud command line tool to create a new custom role in a project by copying 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 48

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 project
- 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 network
- D. Create separate VPC networks for on-premises and internet connectivity
- E. Create the relevant routes on the third-party appliances and VPC networks.
- F. Consolidate all existing projects' subnetworks into a single VPC
- G. Create separate VPC networks for on-premises and internet connectivity
- H. Configure the third-party appliances with multiple interfaces, with each interface connected to a separate VPC network
- I. Create the relevant routes on the third-party appliances and VPC networks.
- J. Configure the third-party appliances with multiple interfaces
- K. Create a hub VPC network for all projects, and create separate VPC networks for on-premises and internet connectivity
- 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 VPC
- N. Export custom routes from the hub VPC and import on all projects' VPC networks.

Answer: D

NEW QUESTION 53

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 57

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 61

You work for a university that is migrating to GCP. 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 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' Interconnects.
- F. Use standalone projects and deploy the VLAN attachments and Interconnects in each of the individual projects.

Answer: A

Explanation:

<https://cloud.google.com/interconnect/docs/how-to/dedicated/using-interconnects-other-projects>

Using Cloud Interconnect with Shared VPC You can use Shared VPC to share your VLAN attachment in a project with other VPC networks. Choosing Shared VPC is preferable if you need to create many projects and would like to prevent individual project owners from managing their connectivity back to your on-premises network. In this scenario, the host project contains a common Shared VPC network usable by VMs in service projects. Because VMs in the service projects use this network, Service Project Admins don't need to create other VLAN attachments or Cloud Routers in the service projects. In this scenario, you must create VLAN attachments and Cloud Routers for a Cloud Interconnect connection only in the Shared VPC host project. The combination of a VLAN attachment and its associated Cloud Router are unique to a given Shared VPC network.

<https://cloud.google.com/network-connectivity/docs/interconnect/how-to/enabling-multiple-networks-access-sa>

<https://cloud.google.com/vpc/docs/shared-vpc>

NEW QUESTION 62

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

How should you design this topology?

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

Answer: A

Explanation:

The service range setting is permanent and cannot be changed. Please see

<https://stackoverflow.com/questions/60957040/how-to-increase-the-service-address-range-of-a-gke-cluster> I think the correct answer is A since: Grow is expected

to up to 100 nodes (that would be /25), then up to 200 pods per node (100 times 200 = 20000 so /17 is 32768), then 1500 services in a /21 (up to 2048)
<https://docs.netgate.com/pfsense/en/latest/book/network/understanding-cidr-subnet-mask-notation.html>

NEW QUESTION 66

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 71

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 and sa-db@my-project.iam.gserviceaccount.co
- E. Associate service account sa-app with the application servers, and associate the service account sa-db with the database server
- F. Run the following command: `gcloud compute firewall-rules create app-db-firewall-rule --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 and sa-db@my-project.iam.gserviceaccount.co
- H. Associate the service account sa-app with the application servers, and associate the service account sa-db with the database server
- I. Run the following command: `gcloud compute firewall-rules create app-db-firewall-rule --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-server
- 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 72

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 address
- 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 gateway
- 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 75

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 172.16.45.0/24 network.

Answer: C

NEW QUESTION 76

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 region
- 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 region
- 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 80

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

Professional-Cloud-Network-Engineer Practice Exam Features:

- * Professional-Cloud-Network-Engineer Questions and Answers Updated Frequently
- * Professional-Cloud-Network-Engineer Practice Questions Verified by Expert Senior Certified Staff
- * Professional-Cloud-Network-Engineer Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * Professional-Cloud-Network-Engineer Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The Professional-Cloud-Network-Engineer Practice Test Here](#)