Exam Questions Professional-Cloud-Network-Engineer

Google Cloud Certified - Professional Cloud Network Engineer

https://www.2passeasy.com/dumps/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 built a web application with several containerized microservices. You want to run those microservices on Cloud Run. You must also ensure that the services are highly available to your customers with low latency. What should you do?

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

Answer: B

NEW QUESTION 3
You are designing a hybrid cloud environment. Your Google Cloud environment is interconnected with your on-premises network using HA VPN and Cloud Router in a central transit hub VPC. The Cloud Router is configured with the default settings. Your on-premises DNS server is located at 192.168.20.88. You need to ensure that your Compute Engine resources in multiple spoke VPCs can resolve on-premises private hostnames using the domain corp.altostrat.com while also resolving Google Cloud hostnames. You want to follow Google-recommended practices. What should you do?

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

Answer: A

NEW QUESTION 4
You have a Cloud Storage bucket in Google Cloud project XYZ. The bucket contains sensitive data. You need to design a solution to ensure that only instances belonging to VPCs under project XYZ can access the data stored in this Cloud Storage bucket. What should you do?

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

Answer: C

NEW QUESTION 5
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 6
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 7
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 8
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 9
You need to centralize the Identity and Access Management permissions and email distribution for the WebServices Team as efficiently as possible.
What should you do?

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

Answer: A

NEW QUESTION 10
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 10
You have configured a service on Google Cloud that connects to an on-premises service via a Dedicated Interconnect. Users are reporting recent connectivity issues. You need to determine whether the traffic is being dropped because of firewall rules or a routing decision. What should you do?

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

Answer: B

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

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

Answer: C

NEW QUESTION 19
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 24
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 26
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 30
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 35
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 39
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 43
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 VP
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 VP
E. Create one OpenVPN Access Server in each region of your partner's VP
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 VP
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 VP
J. Connect your VPN gateways to the partner's gateways with a pair of tunnel
K. Enable global dynamic routing in each VPC.

Answer: A

NEW QUESTION 45
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 50
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 55
You are creating an instance group and need to create a new health check for HTTP(s) load balancing. Which two methods can you use to accomplish this? (Choose two.)

A. Create a new health check using the gcloud command line tool.
B. Create a new health check using the VPC Network section in the GCP Console.
C. Create a new health check, or select an existing one, when you complete the load balancer's backend configuration in the GCP Console.
D. Create a new legacy health check using the gcloud command line tool.
E. Create a new legacy health check using the Health checks section in the GCP Console.

Answer: AC

Explanation:
https://cloud.google.com/load-balancing/docs/health-checks#creating_and_modifying_health_checks

NEW QUESTION 58
Your company has just launched a new critical revenue-generating web application. You deployed the application for scalability using managed instance groups, autoscaling, and a network load balancer as frontend. One day, you notice severe bursty traffic that the caused autoscaling to reach the maximum number of instances, and users of your application cannot complete transactions. After an investigation, you think it as a DDOS attack. You want to quickly restore user access to your application and allow successful transactions while minimizing cost.
Which two steps should you take? (Choose two.)

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

Answer: BE

NEW QUESTION 62
Your on-premises data center has 2 routers connected to your GCP 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 the same 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.
•The VPN logs have no-proposal-chosen lines when the VPNs are connecting.
•BGP session is not established between one on-premises router and the Cloud Router. What is the most likely cause of this problem?

A. One of the VPN sessions is configured incorrectly.
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. BGP sessions are not established between both on-premises routers and the Cloud Router.

Answer: A

Explanation:
If the VPN logs show a no-proposal-chosen error, this error indicates that Cloud VPN and your peer VPN gateway were unable to agree on a set of ciphers. For IKEv1, the set of ciphers must match exactly. For IKEv2, there must be at least one common cipher proposed by each gateway. Make sure that you use supported ciphers to configure your peer VPN gateway.
https://cloud.google.com/network-connectivity/docs/vpn/support/troubleshooting#:~:text=If%20the%20VPN%2

NEW QUESTION 66
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 69
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 70
You are configuring a new HTTP application that will be exposed externally behind both IPv4 and IPv6 virtual IP addresses, using ports 80, 8080, and 443. You will have backends in two regions: us-west1 and
us-east1. You want to serve the content with the lowest-possible latency while ensuring high availability and autoscaling, and create native content-based rules using the HTTP hostname and request path. The IP addresses of the clients that connect to the load balancer need to be visible to the backends. Which configuration should you use?

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

Answer: D

NEW QUESTION 74
You suspect that one of the virtual machines (VMs) in your default Virtual Private Cloud (VPC) is under a denial-of-service attack. You need to analyze the incoming traffic for the VM to understand where the traffic is coming from. What should you do?

A. Enable Data Access audit logs of the VP
B. Analyze the logs and get the source IP addresses from the subnetworks.get field.
C. Enable VPC Flow Logs for the subne
D. Analyze the logs and get the source IP addresses from the connection field.
E. Enable VPC Flow Logs for the VP
F. Analyze the logs and get the source IP addresses from the src_location field.
G. Enable Data Access audit logs of the subne
H. Analyze the logs and get the source IP addresses from the networks.get field.

Answer: B

NEW QUESTION 78
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 83
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 85
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 89
You need to establish network connectivity between three Virtual Private Cloud networks, Sales, Marketing, and Finance, so that users can access resources in all three VPCs. You configure VPC peering between the Sales VPC and the Finance VPC. You also configure VPC peering between the Marketing VPC and the Finance VPC. After you complete the configuration, some users cannot connect to resources in the Sales VPC and the Marketing VPC. You want to resolve the problem.
What should you do?

A. Configure VPC peering in a full mesh.
B. Alter the routing table to resolve the asymmetric route.
C. Create network tags to allow connectivity between all three VPCs.
D. Delete the legacy network and recreate it to allow transitive peering.

Answer: A

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

NEW QUESTION 94
You are responsible for enabling Private Google Access for the virtual machine (VM) instances in your Virtual Private Cloud (VPC) to access Google APIs. All VM instances have only a private IP address and need to access Cloud Storage. You need to ensure that all VM traffic is routed back to your on-premises data center for traffic scrubbing via your existing Cloud Interconnect connection. However, VM traffic to Google APIs should remain in the VPC. What should you do?

A. Delete the default route in your VPC.Create a private Cloud DNS zone for googleapis.com, create a CNAME for *.googleapis.com to restricted googleapis.com, and create an A record for restricted googleapis com that resolves to the addresses in 199.36.153.4/30.Create a static route in your VPC for the range 199.36.153.4/30 with the default internet gateway as the next hop.
B. Delete the default route in your VPC and configure your on-premises router to advertise 0.0.0.0/0 via Border Gateway Protocol (BGP).Create a public Cloud DNS zone with a CNAME for *.google.com to private googleapis com, create a CNAME for * googleapis.com to private googleapis com, and create an A record for Private googleapis.com that resolves to the addresses in 199.36.153 8/30.Create a static route in your VPC for the range 199 .36.153.8/30 with the default internet gateway as the next hop.
C. Configure your on-premises router to advertise 0.0.0.0/0 via Border Gateway Protocol (BGP) with a lower priority (MED) than the default VPC route.Create a private Cloud DNS zone for googleapis.com, create a CNAME for * googieapis.com to private googleapis com, and create an A record for private.googleapis.com that resolves to the addresses in 199.36.153.8/30.Create a static route in your VPC for the range 199.36. 153.8/30 with the default internet gateway as the next hop.
D. Delete the default route in your VPC and configure your on-premises router to advertise 0.0.0.0/0 via Border Gateway Protocol (BGP).Create a private Cloud DNS zone for googleapis.com, create a CNAME for * googieapis.com to Private googleapis.com, and create an A record for private.googleapis.com that resolves to the addresses in 199.36.153.8/30.Create a static route in your VPC for the range 199.36.153.8/30 with the default internet gateway as the next hop.

Answer: C

NEW QUESTION 99
Your company has a single Virtual Private Cloud (VPC) network deployed in Google Cloud with on-premises connectivity already in place. You are deploying a new application using Google Kubernetes Engine (GKE), which must be accessible only from the same VPC network and on-premises locations. You must ensure that the GKE control plane is exposed to a predefined list of on-premises subnets through private connectivity only. What should you do?

A. Create a GKE private cluster with a private endpoint for the control plan
B. Configure VPC Networking Peering export/import routes and custom route advertisements on the Cloud Router
C. Configure authorized networks to specify the desired on-premises subnets.
D. Create a GKE private cluster with a public endpoint for the control plan
E. Configure VPC Networking Peering export/import routes and custom route advertisements on the Cloud Routers.
F. Create a GKE private cluster with a private endpoint for the control plan

G. Configure authorized networks to specify the desired on-premises subnets.
H. Create a GKE public cluste
I. Configure authorized networks to specify the desired on-premises subnets.

Answer: C

NEW QUESTION 100
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 networr
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 102
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 104
You deployed a hub-and-spoke architecture in your Google Cloud environment that uses VPC Network Peering to connect the spokes to the hub. For security reasons, you deployed a private Google Kubernetes
Engine (GKE) cluster in one of the spoke projects with a private endpoint for the control plane. You configured authorized networks to be the subnet range where the GKE nodes are deployed. When you attempt to reach the GKE control plane from a different spoke project, you cannot access it. You need to allow access to the GKE control plane from the other spoke projects. What should you do?

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

Answer: C

NEW QUESTION 108
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 112
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 115
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 116
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 121
You are configuring load balancing for a standard three-tier (web, application, and database) application. You have configured an external HTTP(S) load balancer for the web servers. You need to configure load balancing for the application tier of servers. What should you do?

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

Answer: A

NEW QUESTION 123
Your organization is implementing a new security policy to control how firewall rules are applied to control flows between virtual machines (VMs). Using Google-recommended practices, you need to set up a firewall rule to enforce strict control of traffic between VM A and VM B. You must ensure that communications flow only from VM A to VM B within the VPC, and no other communication paths are allowed. No other firewall rules exist in the VPC. Which firewall rule should you configure to allow only this communication path?

A. Firewall rule direction: ingress Action: allowTarget: VM B service accountSource ranges: VM A service account Priority: 1000
B. Firewall rule direction: ingress Action: allowTarget: specific VM B tagSource ranges: VM A tag and VM A source IP address Priority: 1000
C. Firewall rule direction: ingress Action: allowTarget: VM A service accountSource ranges: VM B service account and VM B source IP address Priority: 100
D. Firewall rule direction: ingress Action: allowTarget: specific VM A tagSource ranges: VM B tag and VM B source IP address Priority: 100

Answer: D

NEW QUESTION 127
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 129

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 131
You want to implement an IPSec tunnel between your on-premises network and a VPC via Cloud VPN. You need to restrict reachability over the tunnel to specific local subnets, and you do not have a device capable of speaking Border Gateway Protocol (BGP).
Which routing option should you choose?

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

Answer: C

NEW QUESTION 136
You recently configured Google Cloud Armor security policies to manage traffic to your application. You discover that Google Cloud Armor is incorrectly blocking some traffic to your application. You need to identity the web application firewall (WAF) rule that is incorrectly blocking traffic. What should you do?

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

Answer: A

NEW QUESTION 141
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 145
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 148
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 149
Your company has recently expanded their EMEA-based operations into APAC. Globally distributed users report that their SMTP and IMAP services are slow. Your company requires end-to-end encryption, but you do not have access to the SSL certificates.
Which Google Cloud load balancer should you use?

A. SSL proxy load balancer
B. Network load balancer
C. HTTPS load balancer
D. TCP proxy load balancer

Answer: D

Explanation:
https://cloud.google.com/security/encryption-in-transit/ Automatic encryption between GFEs and backends For the following load balancer types, Google automatically encrypts traffic between Google Front Ends (GFEs) and your backends that reside within Google Cloud VPC networks: HTTP(S) Load Balancing TCP Proxy Load Balancing SSL Proxy Load Balancing

NEW QUESTION 154
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 155
In your project my-project, you have two subnets in a Virtual Private Cloud (VPC): subnet-a with IP range 10.128.0.0/20 and subnet-b with IP range 172.16.0.0/24. You need to deploy database servers in subnet-a. You will also deploy the application servers and web servers in subnet-b. You want to configure firewall rules that only allow database traffic from the application servers to the database servers. What should you do?

A. Create network tag app-server and service account sa-db@my-project.iam.gserviceaccount.co
B. Add the tag to the application servers, and associate the service account with the database server
C. Run the following command:gcloud compute firewall-rules create app-db-firewall-rule \--action allow \--direction ingress \--rules top:3306 \--source-tags app-server \--target-service-accounts sa-db@my- project.iam.gserviceaccount.com
D. Create service accounts sa-app@my-project.iam.gserviceaccount.com andsa-db@my-project.iam.gserviceaccount.co
E. Associate service account sa-app with the application servers, and associate theservice account sa-db with the database server
F. Run the following command: gcloud compute firewall-rules create app-db-firewall-ru--allow TCP:3306 \--source-service-accounts sa-app@democloud-idp-demo.iam.gserviceaccount.com \--target-service-accounts sa-db@my- project.iam.gserviceaccount.com
G. Create service accounts sa-app@my-project.iam.gserviceaccount.com andsa-db@my-project.iam.gserviceaccount.co
H. Associate the service account sa-app with the application servers, and associatethe service account sa-db with the database server
I. Run the following command: gcloud compute firewall-rules create app-db-firewall-ru--allow TCP:3306 \--source-ranges 10.128.0.0/20 \--source-service-accounts sa-app@my- project.iam.gserviceaccount.com \--target-service-accounts sa-db@my- project.iam.gserviceaccount.com
J. Create network tags app-server and db-serve
K. Add the app-server tag to the application servers, and add the db-server tag to the database server

L. Run the following command:gcloud compute firewall-rules create app-db-firewall-rule \--action allow \--direction ingress \--rules tcp:3306 \--source-ranges 10.128.0.0/20 \--source-tags app-server \--target-tags db-server

Answer: D

NEW QUESTION 160
You are designing the network architecture for your organization. Your organization has three developer teams: Web, App, and Database. All of the developer teams require access to Compute Engine instances to perform their critical tasks. You are part of a small network and security team that needs to provide network access to the developers. You need to maintain centralized control over network resources, including subnets, routes, and firewalls. You want to minimize operational overhead. How should you design this topology?

A. Configure a host project with a Shared VP
B. Create service projects for Web, App, and Database.
C. Configure one VPC for Web, one VPC for App, and one VPC for Databas
D. Configure HA VPN between each VPC.
E. Configure three Shared VPC host projects, each with a service project: one for Web, one for App, and one for Database.
F. Configure one VPC for Web, one VPC for App, and one VPC for Databas
G. Use VPC Network Peering to connect all VPCs in a full mesh.

Answer: C

NEW QUESTION 162
Your company's on-premises network is connected to a VPC using a Cloud VPN tunnel. You have a static route of 0.0.0.0/0 with the VPN tunnel as its next hop defined in the VPC. All internet bound traffic currently passes through the on-premises network. You configured Cloud NAT to translate the primary IP addresses of Compute Engine instances in one region. Traffic from those instances will now reach the internet directly from their VPC and not from the on-premises network. Traffic from the virtual machines (VMs) is not translating addresses as expected. What should you do?

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

Answer: A

NEW QUESTION 163
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 165
You need to ensure your personal SSH key works on every instance in your project. You want to accomplish this as efficiently as possible.
What should you do?

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

Answer: A

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

NEW QUESTION 169
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual Professional-Cloud-Network-Engineer Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the Professional-Cloud-Network-Engineer Product From:

https://www.2passeasy.com/dumps/Professional-Cloud-Network-Engineer/

Money Back Guarantee

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