PROFESSIONAL-CLOUD-NETWORK-ENGINEER Q&As

Professional Cloud Network Engineer

Pass Google PROFESSIONAL-CLOUD-NETWORK-ENGINEER Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/professional-cloud-network-engineer.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Google Official Exam Center

QUESTION 1

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

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

How should you create the GKE cluster?

A. Create a private cluster that uses VPC advanced routes. Set the pod and service ranges as /24. Set up a network proxy to access the master.

B. Create a VPC-native GKE cluster using GKE-managed IP ranges. Set the pod IP range as /21 and service IP range as /24. Set up a network proxy to access the master.

C. Create a VPC-native GKE cluster using user-managed IP ranges. Enable a GKE cluster network policy, set the pod and service ranges as /24. Eet up a network proxy to access the master. Enable master authorized networks.

D. Create a VPC-native GKE cluster using user-managed IP ranges. Enable privateEndpoint on the cluster master. Set the pod and service ranges as /24. Set up a network proxy to access the master. Enable master authorized networks.

Correct Answer: D

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

QUESTION 2

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

A. Enable Firewall Rules Logging inside the third project.

B. Modify the existing VPC Service Controls policy to include the new project in dry run mode.

C. Monitor the Resource Manager audit logs inside the perimeter.

D. Enable VPC Flow Logs inside the third project, and monitor the logs for negative impact.

Correct Answer: B

QUESTION 3

You have deployed a new internal application that provides HTTP and TFTP services to on-premises hosts. You want to be able to distribute traffic across multiple Compute Engine instances, but need to ensure that clients are sticky to a particular instance across both services.

Which session affinity should you choose?

A. None

B. Client IP

C. Client IP and protocol

D. Client IP, port and protocol

Correct Answer: B

QUESTION 4

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.

Correct Answer: C

Reference: https://geekflare.com/gcp-firewall-configuration/

QUESTION 5

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

A. Configure your VPC routing in regional mode. Add an additional Cloud Interconnect VLAN attachment in the us-east1 region, and configure a Cloud Router in us-east1.

B. Configure your VPC routing in global mode. Add an additional Cloud Interconnect VLAN attachment in the us-east1 region, and configure a Cloud Router in us-east1.

C. Configure your VPC routing in global mode. Add an additional Cloud Interconnect VLAN attachment in the us-west2 region, and configure a Cloud Router in us-west2.

D. Configure your VPC routing in regional mode. Add additional Cloud Interconnect VLAN attachments in the us-west2

and us-central1 regions, and configure Cloud Routers in us-west2 and us-central1.

Correct Answer: B