IT认证电子书

质量更高　　服务更好

半年免费升级服务

http://www.itrenzheng.com

Exam : **Professional Cloud Network Engineer**

Title : Professional Cloud Network Engineer

Version : DEMO

1.Your organization uses a hub-and-spoke architecture with critical Compute Engine instances in your Virtual Private Clouds (VPCs). You are responsible for the design of Cloud DNS in Google Cloud. You need to be able to resolve Cloud DNS private zones from your on-premises data center and enable on-premises name resolution from your hub-and-spoke VPC design.
What should you do?
A. Configure a private DNS zone in the hub VPC, and configure DNS forwarding to the on-premises server.
Configure DNS peering from the spoke VPCs to the hub VPC.
B. Configure a DNS policy in the hub VPC to allow inbound query forwarding from the spoke VPCs.
Configure the spoke VPCs with a private zone, and set up DNS peering to the hub VPC.
C. Configure a DNS policy in the spoke VPCs, and configure your on-premises DNS as an alternate DNS server.
Configure the hub VPC with a private zone, and set up DNS peering to each of the spoke VPCs.
D. Configure a DNS policy in the hub VPC, and configure the on-premises DNS as an alternate DNS server.
Configure the spoke VPCs with a private zone, and set up DNS peering to the hub VPC.
Answer: C

2.You recently noticed a recurring daily spike in network usage in your Google Cloud project. You need to identify the virtual machine (VM) instances and type of traffic causing the spike in traffic utilization while minimizing the cost and management overhead required.
What should you do?
A. Enable VPC Flow Logs and send the output to BigQuery for analysis.
B. Enable Firewall Rules Logging for all allowed traffic and send the output to BigQuery for analysis.
C. Configure Packet Mirroring to send all traffic to a VM. Use Wireshark on the VM to identity traffic utilization for each VM in the VPC.
D. Deploy a third-party network appliance and configure it as the default gateway. Use the third-party network appliance to identify users with high network traffic.
Answer: C

3.You are the network administrator responsible for hybrid connectivity at your organization. Your developer team wants to use Cloud SQL in the us-west1 region in your Shared VPC. You configured a Dedicated Interconnect connection and a Cloud Router in us-west1, and the connectivity between your Shared VPC and on-premises data center is working as expected. You just created the private services access connection required for Cloud SQL using the reserved IP address range and default settings. However, your developers cannot access the Cloud SQL instance from on-premises. You want to resolve the issue.
What should you do?
A. Modify the VPC Network Peering connection used for Cloud SQL, and enable the import and export of routes.
Create a custom route advertisement in your Cloud Router to advertise the Cloud SQL IP address range.
B. Change the VPC routing mode to global.
Create a custom route advertisement in your Cloud Router to advertise the Cloud SQL IP address range.
C. Create an additional Cloud Router in us-west2.

Create a new Border Gateway Protocol (BGP) peering connection to your on-premises data center.
Modify the VPC Network Peering connection used for Cloud SQL, and enable the import and export of routes.
D. Change the VPC routing mode to global.
Modify the VPC Network Peering connection used for Cloud SQL, and enable the import and export of routes.
Answer: A

4.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

5.Your company has a Virtual Private Cloud (VPC) with two Dedicated Interconnect connections in two different regions: us-west1 and us-east1. Each Dedicated Interconnect connection is attached to a Cloud Router in its respective region by a VLAN attachment. You need to configure a high availability failover path. By default, all ingress traffic from the on-premises environment should flow to the VPC using the us-west1 connection. If us-west1 is unavailable, you want traffic to be rerouted to us-east1.
How should you configure the multi-exit discriminator (MED) values to enable this failover path?
A. Use regional routing. Set the us-east1 Cloud Router to a base priority of 100, and set the us-west1 Cloud Router to a base priority of 1
B. Use global routing. Set the us-east1 Cloud Router to a base priority of 100, and set the us-west1 Cloud Router to a base priority of 1
C. Use regional routing. Set the us-east1 Cloud Router to a base priority of 1000, and set the us-west1 Cloud Router to a base priority of 1
D. Use global routing. Set the us-east1 Cloud Router to a base priority of 1000, and set the us-west1 Cloud Router to a base priority of 1
Answer: A