



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.pass4itsure.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



VCE & PDF

Pass4itSure.com

<https://www.pass4itsure.com/professional-cloud-network-engineer.html>

2024 Latest pass4itsure PROFESSIONAL-CLOUD-NETWORK-ENGINEER

PDF and VCE dumps Download

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



**QUESTION 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.

Correct Answer: C

QUESTION 2

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 identify 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 Cloud Console.

Correct Answer: A

QUESTION 3

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.

Correct Answer: C

Reference: <https://cloud.google.com/iam/docs/understanding-custom-roles>

QUESTION 4

Your organization's security policy requires that all internet-bound traffic return to your on-premises data center through HA VPN tunnels before egressing to the internet, while allowing virtual machines (VMs) to leverage private Google APIs

using private virtual IP addresses 199.36.153.4/30. You need to configure the routes to enable these traffic flows.

What should you do?

A. Configure a custom route 0.0.0.0/0 with a priority of 500 whose next hop is the default internet gateway. Configure another custom route 199.36.153.4/30 with priority of 1000 whose next hop is the VPN tunnel back to the on-premises data center.

B. Configure a custom route 0.0.0.0/0 with a priority of 1000 whose next hop is the internet gateway. Configure another custom route 199.36.153.4/30 with a priority of 500 whose next hop is the VPN tunnel back to the on-premises data center.

C. Announce a 0.0.0.0/0 route from your on-premises router with a MED of 1000. Configure a custom route 199.36.153.4/30 with a priority of 1000 whose next hop is the default internet gateway.

D. Announce a 0.0.0.0/0 route from your on-premises router with a MED of 500. Configure another custom route 199.36.153.4/30 with a priority of 1000 whose next hop is the VPN tunnel back to the on-premises data center.

Correct Answer: A

QUESTION 5

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.

Correct Answer: A



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.

[PROFESSIONAL-CLOUD-NETWORK-ENGINEER PDF Dumps](#)

[PROFESSIONAL-CLOUD-NETWORK-ENGINEER VCE Dumps](#)

[PROFESSIONAL-CLOUD-NETWORK-ENGINEER Practice Test](#)