Google Discussions

Exam Professional Cloud Security Engineer All Questions

View all questions & answers for the Professional Cloud Security Engineer exam

Go to Exam

EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 207 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 207
Topic #: 1
[All Professional Cloud Security Engineer Questions]

Your DevOps team uses Packer to build Compute Engine images by using this process:

1. Create an ephemeral Compute Engine VM.
2. Copy a binary from a Cloud Storage bucket to the VM's file system.
3. Update the VM's package manager.
4. Install external packages from the internet onto the VM.

Your security team just enabled the organizational policy, constraints/ compute.vmExternalIpAccess, to restrict the usage of public IP Addresses on VMs. In response, your DevOps team updated their scripts to remove public IP addresses on the Compute Engine VMs; however, the build pipeline is failing due to connectivity issues.

What should you do? (Choose two.)

A. Provision an HTTP load balancer with the VM in an unmanaged instance group to allow inbound connections from the internet to your VM.

B. Provision a Cloud NAT instance in the same VPC and region as the Compute Engine VM.

C. Enable Private Google Access on the subnet that the Compute Engine VM is deployed within.

D. Update the VPC routes to allow traffic to and from the internet.

E. Provision a Cloud VPN tunnel in the same VPC and region as the Compute Engine VM.

Show Suggested Answer

by K1SMM at *Aug. 4, 2023, 2:14 a.m.*

Comments

Type your comment...

Submit

Xoxoo 10 months, 1 week ago

Selected Answer: BC

Provision a Cloud NAT instance (Option B): Cloud NAT allows your Compute Engine instances without public IP addresses to access the internet while preserving the security restrictions imposed by your organizational policy. By provisioning a Cloud NAT instance in the same VPC and region as your Compute Engine VMs, you enable outbound connectivity for these VMs.

Enable Private Google Access (Option C): Enabling Private Google Access on the subnet where your Compute Engine VMs are deployed allows these instances to access Google Cloud services over the private IP address range. This can help with accessing external resources needed during the Packer image build process without exposing the VMs to the public internet.

upvoted 1 times

Xoxoo 10 months, 1 week ago

Options A, D, and E are not the most suitable solutions in this context:

A. Provisioning an HTTP load balancer with an unmanaged instance group would allow inbound connections from the internet, which is the opposite of what you want to achieve (restricting public IP addresses).

D. Updating VPC routes to allow traffic to and from the internet would also contradict the goal of restricting public IP addresses.

E. Provisioning a Cloud VPN tunnel is used for connecting on-premises networks to Google Cloud or for secure communication between different VPCs but is not necessary for addressing the issue of restricted public IP addresses for Packer image builds.

In summary, the most appropriate actions to address the connectivity issue while adhering to the policy constraint are options B and C. These solutions ensure that your Compute Engine VMs can access external resources and Google Cloud services without public IP addresses.

upvoted 1 times

anshad666 11 months ago

Selected Answer: BC

B- Cloud Nat for external connections
C- Cloud Storage private access from VM

upvoted 3 times

cyberpunk21 11 months, 1 week ago

Selected Answer: BC

BC looks good

upvoted 2 times

pfilourenco 11 months, 4 weeks ago

Selected Answer: BC

B & C make sense

upvoted 3 times

K1SMM 11 months, 4 weeks ago

BC I think
Cloud NAT to update em private access to cloud storage access

upvoted 1 times