

Passcert

Higher Quality, better service!



Q&A

[Http://www.passcert.com](http://www.passcert.com)

We offer free update service for one year.

Exam : **Professional Cloud
Security Engineer**

Title : Google Cloud Certified -
Professional Cloud Security
Engineer

Version : DEMO

1. Your team needs to make sure that a Compute Engine instance does not have access to the internet or to any Google APIs or services.

Which two settings must remain disabled to meet these requirements? (Choose two.)

- A. Public IP
- B. IP Forwarding
- C. Private Google Access
- D. Static routes
- E. IAM Network User Role

Answer: A,C

Explanation:

To ensure that a Compute Engine instance does not have access to the internet or to any Google APIs or services, you need to disable the following settings:

Public IP: Disabling the public IP address ensures that the instance does not have a direct connection to the internet. Without a public IP address, the instance cannot be accessed from or communicate with the internet directly.

Private Google Access: Disabling Private Google Access ensures that the instance does not have access to Google APIs and services through the internal Google network. Private Google Access allows instances without a public IP to reach Google APIs and services using private IP addresses, but disabling it will block this path.

Disabling these settings will effectively isolate the instance from both the public internet and Google's internal API services.

Reference

Google Cloud VPC Documentation - Overview

Configuring Private Google Access

Compute Engine Network Overview

2. Which two implied firewall rules are defined on a VPC network? (Choose two.)

- A. A rule that allows all outbound connections
- B. A rule that denies all inbound connections
- C. A rule that blocks all inbound port 25 connections
- D. A rule that blocks all outbound connections
- E. A rule that allows all inbound port 80 connections

Answer: A,B

Explanation:

Implied IPv4 allow egress rule. An egress rule whose action is allow, destination is 0.0.0.0/0, and priority is the lowest possible (65535) lets any instance send traffic to any destination. Implied IPv4 deny ingress rule. An ingress rule whose action is deny, source is 0.0.0.0/0, and priority is the lowest possible (65535) protects all instances by blocking incoming connections to them.

https://cloud.google.com/vpc/docs/firewalls?hl=en#default_firewall_rules

3. A customer needs an alternative to storing their plain text secrets in their source-code management (SCM) system.

How should the customer achieve this using Google Cloud Platform?

- A. Use Cloud Source Repositories, and store secrets in Cloud SQL.

- B. Encrypt the secrets with a Customer-Managed Encryption Key (CMEK), and store them in Cloud Storage.
- C. Run the Cloud Data Loss Prevention API to scan the secrets, and store them in Cloud SQL.
- D. Deploy the SCM to a Compute Engine VM with local SSDs, and enable preemptible VMs.

Answer: B

Explanation:

Storing secrets securely is crucial for maintaining the integrity and confidentiality of your applications. Here is how you can achieve this using Google Cloud Platform:

Encrypt the Secrets: Use Customer-Managed Encryption Keys (CMEK) to encrypt your secrets. CMEK allows you to have greater control over the encryption keys used to protect your data. This ensures that even if the storage medium is compromised, the secrets remain protected by strong encryption.

Store in Cloud Storage: Store the encrypted secrets in Google Cloud Storage. Cloud Storage is a secure and scalable object storage service. By using encrypted storage, you can ensure that the secrets are securely stored and can only be accessed by authorized entities.

This method provides a secure and managed way to store secrets, ensuring that they are not exposed in plain text within your source code management system.

Reference

Customer-Managed Encryption Keys (CMEK)

Google Cloud Storage Security

4. Your team wants to centrally manage GCP IAM permissions from their on-premises Active Directory Service. Your team wants to manage permissions by AD group membership.

What should your team do to meet these requirements?

- A. Set up Cloud Directory Sync to sync groups, and set IAM permissions on the groups.
- B. Set up SAML 2.0 Single Sign-On (SSO), and assign IAM permissions to the groups.
- C. Use the Cloud Identity and Access Management API to create groups and IAM permissions from Active Directory.
- D. Use the Admin SDK to create groups and assign IAM permissions from Active Directory.

Answer: A

Explanation:

"In order to be able to keep using the existing identity management system, identities need to be synchronized between AD and GCP IAM. To do so google provides a tool called Cloud Directory Sync. This tool will read all identities in AD and replicate those within GCP. Once the identities have been replicated then it's possible to apply IAM permissions on the groups. After that you will configure SAML so google can act as a service provider and either you ADFS or other third party tools like Ping or Okta will act as the identity provider. This way you effectively delegate the authentication from Google to something that is under your control."

5. When creating a secure container image, which two items should you incorporate into the build if possible? (Choose two.)

- A. Ensure that the app does not run as PID 1.
- B. Package a single app as a container.
- C. Remove any unnecessary tools not needed by the app.
- D. Use public container images as a base image for the app.

E. Use many container image layers to hide sensitive information.

Answer: B,C

Explanation:

When creating a secure container image, it is essential to follow best practices to minimize vulnerabilities and ensure the container operates as intended.

Here are the two key practices:

Package a Single App as a Container: By packaging only a single application within a container, you reduce complexity and potential attack surfaces. This practice aligns with the principle of single responsibility, ensuring each container has a clear and focused purpose.

Remove Any Unnecessary Tools: Any additional tools or software that are not required by the application should be removed from the container image. This minimizes the number of potential vulnerabilities and reduces the attack surface. A minimal container image also leads to smaller image sizes and faster deployment times.

These practices contribute to creating a more secure and efficient container image.

Reference

Container Security Best Practices

Securing Container Images