PROFESSIONAL-CLOUD-SECURITY-ENGINEER^{Q&As}

Professional Cloud Security Engineer

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

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

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

100% Passing Guarantee
100% Money Back Assurance

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

Latest PROFESSIONAL-CLOUD-SECURITY-ENGINEER Dumps |
PROFESSIONAL-CLOUD-SECURITY-ENGINEER PDF Dumps |
PROFESSIONAL-CLOUD-SECURITY-ENGINEER Exam Questions

1 / 6

Latest PROFESSIONAL-CLOUD-SECURITY-ENGINEER Dumps |
PROFESSIONAL-CLOUD-SECURITY-ENGINEER PDF Dumps |
PROFESSIONAL-CLOUD-SECURITY-ENGINEER Exam Questions

2 / 6

QUESTION 1

Your team sets up a Shared VPC Network where project co-vpc-prod is the host project. Your team has configured the firewall rules, subnets, and VPN gateway on the host project. They need to enable Engineering Group A to attach a Compute Engine instance to only the 10.1.1.0/24 subnet.

What should your team grant to Engineering Group A to meet this requirement?

A. Compute Network User Role at the host project level.

B. Compute Network User Role at the subnet level.

C. Compute Shared VPC Admin Role at the host project level.

D. Compute Shared VPC Admin Role at the service project level.

Correct Answer: B

https://cloud.google.com/vpc/docs/shared-vpc#svc_proj_admins

QUESTION 2

You need to connect your organization\\'s on-premises network with an existing Google Cloud environment that includes one Shared VPC with two subnets named Production and Non-Production. You are required

to:

Use a private transport link.

Configure access to Google Cloud APIs through private API endpoints originating from on-premises environments.

Ensure that Google Cloud APIs are only consumed via VPC Service Controls.

What should you do?

A. 1. Set up a Cloud VPN link between the on-premises environment and Google Cloud.

2. Configure private access using the restricted googleapis.com domains in on-premises DNS configurations.

B. 1. Set up a Partner Interconnect link between the on-premises environment and Google Cloud.

2. Configure private access using the private.googleapis.com domains in on-premises DNS configurations.

C. 1. Set up a Direct Peering link between the on-premises environment and Google Cloud.

2. Configure private access for both VPC subnets.

D. 1. Set up a Dedicated Interconnect link between the on-premises environment and Google Cloud.

2. Configure private access using the restricted.googleapis.com domains in on-premises DNS configurations.

Correct Answer: D

Latest PROFESSIONAL-CLOUD-SECURITY-ENGINEER Dumps |
PROFESSIONAL-CLOUD-SECURITY-ENGINEER PDF Dumps |
PROFESSIONAL-CLOUD-SECURITY-ENGINEER Exam Questions

3 / 6

restricted.googleapis.com (199.36.153.4/30) only provides access to Cloud and Developer APIs that support VPC
Service Controls. VPC Service Controls are enforced for these services https://cloud.google.com/vpc/docs/configure-
privategoogle-access-hybrid

QUESTION 3

A large financial institution is moving its Big Data analytics to Google Cloud Platform. They want to have maximum
control over the encryption process of data stored at rest in BigQuery.

What technique should the institution use?

A. Use Cloud Storage as a federated Data Source.

B. Use a Cloud Hardware Security Module (Cloud HSM).

C. Customer-managed encryption keys (CMEK).

D. Customer-supplied encryption keys (CSEK).

Correct Answer: C

If you want to manage the key encryption keys used for your data at rest, instead of having Google manage the keys,
use Cloud Key Management Service to manage your keys. This scenario is known as customer-managed encryption
keys (CMEK). https://cloud.google.com/bigquery/docs/encryption-at-rest

Reference: https://cloud.google.com/bigquery/docs/encryption-at-rest

QUESTION 4

Your company uses Google Cloud and has publicly exposed network assets. You want to discover the assets and
perform a security audit on these assets by using a software tool in the least amount of time.

What should you do?

A. Run a platform security scanner on all instances in the organization.

B. Notify Google about the pending audit and wait for confirmation before performing the scan.

C. Contact a Google approved security vendor to perform the audit.

D. Identify all external assets by using Cloud Asset Inventory and then run a network security scanner against them.

Correct Answer: D

QUESTION 5

Your organization is using Active Directory and wants to configure Security Assertion Markup Language (SAML). You
must set up and enforce single sign-on (SSO) for all users.

What should you do?

Latest PROFESSIONAL-CLOUD-SECURITY-ENGINEER Dumps |
PROFESSIONAL-CLOUD-SECURITY-ENGINEER PDF Dumps |
PROFESSIONAL-CLOUD-SECURITY-ENGINEER Exam Questions

4 / 6

A. 1. Create a new SAML profile.

2.

 Populate the sign-in and sign-out page URLs.

3.

 Upload the X.509 certificate.

4.

 Configure Entity ID and ACS URL in your IdP.

B. 1. Configure prerequisites for OpenID Connect (OIDC) in your Active Directory (AD) tenant.

2.

 Verify the AD domain.

3.

 Decide which users should use SAML.

4.

 Assign the pre-configured profile to the select organizational units (OUs) and groups.

C. 1. Create a new SAML profile.

2.

 Upload the X.509 certificate.

3.

 Enable the change password URL.

4.

 Configure Entity ID and ACS URL in your IdP.

D. 1. Manage SAML profile assignments.

2.

 Enable OpenID Connect (OIDC) in your Active Directory (AD) tenant.

3.

 Verify the domain.

Correct Answer: A

When configuring SAML-based Single Sign-On (SSO) in an organization that\'s using Active Directory, the general
steps would involve setting up a SAML profile, specifying the necessary URLs for sign-in and sign- out processes,
uploading an X.509 certificate for secure communication, and setting up the Entity ID and Assertion Consumer Service

Latest PROFESSIONAL-CLOUD-SECURITY-ENGINEER Dumps |
PROFESSIONAL-CLOUD-SECURITY-ENGINEER PDF Dumps |
PROFESSIONAL-CLOUD-SECURITY-ENGINEER Exam Questions

5 / 6

(ACS) URL in the Identity Provider (which in this case would be Active Directory).

A. Create a new SAML profile, populate URLs, upload X.509 certificate, configure Entity ID and ACS URL: This option comprehensively covers the steps necessary for setting up SAML-based SSO.

Latest PROFESSIONAL-CLOUD-SECURITY-ENGINEER Dumps | PROFESSIONAL-CLOUD-SECURITY-ENGINEER PDF Dumps | PROFESSIONAL-CLOUD-SECURITY-ENGINEER Exam Questions

6 / 6