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.leads4pass.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

QUESTION 1

Your organization uses Google Workspace Enterprise Edition tor authentication. You are concerned about employees leaving their laptops unattended for extended periods of time after authenticating into Google Cloud. You must prevent malicious people from using an employee\\'s unattended laptop to modify their environment.

What should you do?

A. Create a policy that requires employees to not leave their sessions open for long durations.

B. Review and disable unnecessary Google Cloud APIs.

C. Require strong passwords and 2SV through a security token or Google authenticate.

D. Set the session length timeout for Google Cloud services to a shorter duration.

Correct Answer: D

QUESTION 2

Your company operates an application instance group that is currently deployed behind a Google Cloud load balancer in us-central-1 and is configured to use the Standard Tier network. The infrastructure team wants to expand to a second Google Cloud region, us-east-2. You need to set up a single external IP address to distribute new requests to the instance groups in both regions.

What should you do?

A. Change the load balancer backend configuration to use network endpoint groups instead of instance groups.

B. Change the load balancer frontend configuration to use the Premium Tier network, and add the new instance group.

C. Create a new load balancer in us-east-2 using the Standard Tier network, and assign a static external IP address.

D. Create a Cloud VPN connection between the two regions, and enable Google Private Access.

Correct Answer: B

https://cloud.google.com/load-balancing/docs/choosing-load-balancer#global-regional

QUESTION 3

While migrating your organization\\'s infrastructure to GCP, a large number of users will need to access GCP Console. The Identity Management team already has a well-established way to manage your users and want to keep using your existing Active Directory or LDAP server along with the existing SSO password.

What should you do?

A. Manually synchronize the data in Google domain with your existing Active Directory or LDAP server.

B. Use Google Cloud Directory Sync to synchronize the data in Google domain with your existing Active Directory or LDAP server.

C. Users sign in directly to the GCP Console using the credentials from your on-premises Kerberos compliant identity provider.

D. Users sign in using OpenID (OIDC) compatible IdP, receive an authentication token, then use that token to log in to the GCP Console.

Correct Answer: B

https://cloud.google.com/architecture/identity/federating-gcp-with-active-directory-configuring-single-sign- on https://cloud.google.com/blog/products/identity-security/using-your-existing-identity-management-system- with-google-cloud-platform

QUESTION 4

Your organization recently deployed a new application on Google Kubernetes Engine. You need to deploy a solution to protect the application. The solution has the following requirements: Scans must run at least once per week Must be able to detect cross-site scripting vulnerabilities Must be able to authenticate using Google accounts Which solution should you use?

A. Google Cloud Armor

B. Web Security Scanner

C. Security Health Analytics

D. Container Threat Detection

Correct Answer: B

Reference: https://cloud.google.com/security-command-center/docs/concepts-web-security-scanner- overview

Web Security Scanner identifies security vulnerabilities in your App Engine, Google Kubernetes Engine (GKE), and Compute Engine web applications. https://cloud.google.com/security-command-center/docs/concepts-web-security-scanner-overview

QUESTION 5

A customer wants to deploy a large number of 3-tier web applications on Compute Engine.

How should the customer ensure authenticated network separation between the different tiers of the application?

A. Run each tier in its own Project, and segregate using Project labels.

B. Run each tier with a different Service Account (SA), and use SA-based firewall rules.

C. Run each tier in its own subnet, and use subnet-based firewall rules.

D. Run each tier with its own VM tags, and use tag-based firewall rules.

Correct Answer: B

"Isolate VMs using service accounts when possible" "even though it is possible to uses tags for target filtering in this manner, we recommend that you use service accounts where possible. Target tags are not access-controlled and can

be changed by someone with the instanceAdmin role while VMs are in service. Service accounts are access-controlled, meaning that a specific user must be explicitly authorized to use a service account. There can only be one service account per instance, whereas there can be multiple tags. Also, service accounts assigned to a VM can only be changed when the VM is stopped." https://cloud.google.com/solutions/best-practices-vpc-design#isolate-vms-service-accounts