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 4 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 4
Topic #: 1
[All Professional Cloud Security Engineer Questions]

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.

Show Suggested Answer

by xhova at *April 2, 2020, 4:25 a.m.*

Comments

Type your comment...

Submit

droogie Highly Voted 4 years, 6 months ago

Answer. is A. B is just the method of authentication, all the heavy lifting is done in A

upvoted 30 times

upvoted 30 times

johnsm Highly Voted 3 years, 11 months ago

Correct Answer is A as explained here https://www.udemy.com/course/google-security-engineer-certification/?referralCode=E90E3FF49D9DE15E2855

"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."

upvoted 10 times

goat112 Most Recent 7 months ago

Selected Answer: A

Explanation:

Cloud Directory Sync (CDS) is the crucial first step. It's the mechanism that synchronizes your on-premises Active Directory groups with your Google Cloud environment. This allows GCP to recognize and utilize the group structures already defined in your AD.

Once the groups are synced, you can then:

Create IAM roles with the appropriate permissions for your GCP resources.
Grant those IAM roles to the synced AD groups. This effectively ties your existing AD group structure directly to the authorization levels within your GCP environment.
Why SAML 2.0 SSO alone is insufficient:

While SAML 2.0 SSO is essential for single sign-on capabilities (allowing users to access GCP with their existing AD credentials), it doesn't directly address the core requirement: managing GCP IAM permissions based on existing AD group memberships.

upvoted 2 times

ManuelY 9 months ago

Selected Answer: B

Answer is B. "Centrally manage from their ...", so, SAML and manage in the on-premise AD

upvoted 1 times

PleeO 9 months ago

the correct answer is indeed A as Cloud directory sync is the best approach

upvoted 1 times

cloud_monk 10 months, 4 weeks ago

Selected Answer: A

Cloud directory sync is for this purpose.

upvoted 1 times

K3rber0s 1 year, 1 month ago

Correct Answer is A. The keyword is on-prem AD groups which can be synced using Google Dir Sync which then you can apply IAM roles in it.. Without Google Dir Sync, how can you pull the on-prem AD groups? Without it, SSO solution will not work.

upvoted 3 times

f1veo 1 year, 7 months ago

Selected Answer: A

Correct answer is A.

upvoted 1 times

ejlp 1 year, 8 months ago

answer is A

upvoted 1 times

Pachuco 1 year, 11 months ago

Answer is A. GCP Cloud Skills Boost has an exact example on this using the fictitious bank called Cymbal Bank, and clearly call out the GCDS process to push Microsoft AD/LDAP into established Users and Groups in your GCP identity domain

upvoted 2 times

DevXr 2 years, 1 month ago

Selected Answer: B

Using third-party IDP connectors for sync
Many identity management vendors (such as Ping and Okta) provide a connector for G Suite and Cloud Identity Global Directory, which sync changes to users via the Admin SDK Directory API.

The identity providers control usernames, passwords and other information used to identify, authenticate and authorize users for web applications that Google hosts—in this context, it's the GCP console. There are a number of existing open source and commercial identity provider solutions that can help you implement SSO with Google. (Read more about SAML-based federated SSO if you're interested in using Google as the identity provider.)

upvoted 1 times

shayke 2 years, 1 month ago

Selected Answer: A

A will do

upvoted 1 times

Meyucho 2 years, 2 months ago

Selected Answer: A

With A the user and groups management is done in AD as it's asked.

upvoted 1 times

Premumar 2 years, 3 months ago

Selected Answer: A

The question clearly states that, centrally manage. So, Cloud Sync is correct one.

upvoted 1 times

thoadmin 2 years, 4 months ago

Selected Answer: A

A is correct for me

upvoted 2 times

Meyucho 2 years, 4 months ago

Selected Answer: A

SSO will only validate identity, that doesn't sync the groups! Answer is A

upvoted 2 times

GCP72 2 years, 5 months ago

Selected Answer: A

The correct answer is A

upvoted 1 times

Load full discussion...