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 112 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 112
Topic #: 1
[All Professional Cloud Security Engineer Questions]

Your company has been creating users manually in Cloud Identity to provide access to Google Cloud resources. Due to continued growth of the environment, you want to authorize the Google Cloud Directory Sync (GCDS) instance and integrate it with your on-premises LDAP server to onboard hundreds of users. You are required to:

- Replicate user and group lifecycle changes from the on-premises LDAP server in Cloud Identity.
- Disable any manually created users in Cloud Identity.

You have already configured the LDAP search attributes to include the users and security groups in scope for Google Cloud. What should you do next to complete this solution?

A. 1. Configure the option to suspend domain users not found in LDAP. 2. Set up a recurring GCDS task.

B. 1. Configure the option to delete domain users not found in LDAP. 2. Run GCDS after user and group lifecycle changes.

C. 1. Configure the LDAP search attributes to exclude manually created Cloud Identity users not found in LDAP. 2. Set up a recurring GCDS task.

D. 1. Configure the LDAP search attributes to exclude manually created Cloud Identity users not found in LDAP. 2. Run GCDS after user and group lifecycle changes.

Show Suggested Answer

by Tabayashi at *April 29, 2022, 3:17 a.m.*

Comments

Type your comment...

Submit

mT3 Highly Voted 2 years, 2 months ago

Selected Answer: A

Answer is (A).
To achieve the requirement "Disable any manually created users in Cloud Identity", configure GCDS to suspend rather than delete accounts if user accounts are not found in the LDAP directory in GCDS.
Ref: https://support.google.com/a/answer/7177267

upvoted 15 times

AzureDP900 1 year, 8 months ago

A is right

upvoted 1 times

alleinallein 1 year, 3 months ago

Why not C?

upvoted 1 times

GCBC Most Recent 11 months ago

Selected Answer: A

Ref: https://support.google.com/a/answer/7177267

upvoted 1 times

AwesomeGCP 1 year, 8 months ago

Selected Answer: A

A. 1. Configure the option to suspend domain users not found in LDAP. 2. Set up a recurring GCDS task.

upvoted 2 times

tangac 1 year, 10 months ago

Selected Answer: A

clearly A

upvoted 2 times

KillerGoogle 2 years, 2 months ago

C. 1. Configure the LDAP search attributes to exclude manually created Cloud Identity users not found in LDAP. 2. Set up a recurring GCDS task.

upvoted 3 times

Tabayashi 2 years, 3 months ago

I think the answer is (A).

When using Shared VPC, a service perimeter that includes projects that belong to a Shared VPC network must also include the project that hosts the network. When projects that belong to a Shared VPC network are not in the same perimeter as the host project, services might not work as expected or might be blocked entirely.
Ensure that the Shared VPC network host is in the same service perimeter as the projects connected to the network.
https://cloud.google.com/vpc-service-controls/docs/troubleshooting#shared_vpc

upvoted 3 times

Tabayashi 2 years, 3 months ago

Sorry, this answer is question 113.

upvoted 2 times