Google Discussions

EXAM CLOUD DIGITAL LEADER TOPIC 1 QUESTION 15 DISCUSSION

Actual exam question from Google's Cloud Digital Leader

Question #: 15

Topic #: 1

[All Cloud Digital Leader Questions]

Your organization uses Active Directory to authenticate users. Users' Google account access must be removed when their Active Directory account is terminated.

How should your organization meet this requirement?

A. Configure two-factor authentication in the Google domain

B. Remove the Google account from all IAM policies

C. Configure BeyondCorp and Identity-Aware Proxy in the Google domain

D. Configure single sign-on in the Google domain

Show Suggested Answer

by JCE at *Jan. 7, 2022, 4:41 a.m.*

Comments

Type your comment...

Submit

⊟ JCE Highly Voted 2 years, 9 months ago

D seems correct
https://cloud.google.com/architecture/identity/federating-gcp-with-active-directory-configuring-single-sign-on

upvoted 8 times

cookieMr Highly Voted 1 year, 4 months ago

Selected Answer: D

SSO allows for centralized user management, where user accounts and access permissions are managed in a single identity provider (such as Active Directory). When a user's Active Directory account is terminated, SSO provides a centralized point to revoke access across multiple applications and services, including Google accounts.

upvoted 7 times

moncherie Most Recent 3 months ago

Selected Answer: D

of course the answer is D

upvoted 1 times

joe03 3 months, 2 weeks ago

Selected Answer: D

When you use SSO, you are redirected to an external Identity Provider. In this question, it is Microsoft AD. SAML assertion is sent to Google Cloud once the user is authenticated.

upvoted 1 times

Surek 10 months ago

Answer is D

upvoted 1 times

chai_gpt 11 months, 3 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

__rajan__ 1 year ago

Selected Answer: D

SSO is correct as deletion of AD account will remove access from GCP as well.

upvoted 1 times

mdsarfraz69 1 year, 1 month ago

Selected Answer: D

D is correct

upvoted 1 times

star2anand 1 year, 7 months ago

D. Configure single sign-on in the Google domain

upvoted 1 times

KanikaA 1 year, 8 months ago

Selected Answer: D

Using SSO would help in removing access once the account is no longer active.

upvoted 1 times

ucsdmiami2020 1 year, 10 months ago

Selected Answer: D

Per Google Docs article, Federating Google Cloud with Active Directory. "This article describes how you can configure Cloud Identity or Google Workspace to use Active Directory as IdP and authoritative source.

The article compares the logical structure of Active Directory with the structure used by Cloud Identity and Google Workspace and describes how you can map Active Directory forests, domains, users, and groups. The article also provides a flowchart that helps you determine the best mapping approach for your scenario."
https://cloud.google.com/architecture/identity/federating-gcp-with-active-directory-introduction

upvoted 6 times

Pou1ze 1 year, 10 months ago

Selected Answer: D

D is correct

upvoted 1 times

ronieto 1 year, 11 months ago

Selected Answer: D

SSO means federation between AD and Cloud ID, so is the correct answer

SSO means federation between AD and Cloud ID, so is the correct answer

upvoted 3 times

SimonIt73 1 year, 11 months ago

The correct answer should be "Setting up federation between Active Directory and Cloud Identity or Google Workspace". To do that, you have to enable automatic users provisioning and SSO.

upvoted 3 times

rikininetysix 2 years ago

Selected Answer: C

The question asked to provide a solution to remove users' Google account access when their Active Directory account is terminated. So, option 'C' should be correct as BeyondCorp and Identity Aware Proxy are focused solutions to mage Identity and implement a Zero trust model.

upvoted 2 times

> **hogtrough** 2 years ago
>
> The correct answer is D. If you have SSO configured, once a user's AD account is terminated, their access is removed from all services using AD.
>
> upvoted 3 times

haroldbenites 2 years, 4 months ago

Go for D

upvoted 2 times

Monicaarg 2 years, 5 months ago

Selected Answer: D

Your organization uses Active Directory to authenticate users.
Then you need to use Single sign-on (SSO) is an authentication scheme that allows a user to log in with a single ID and password to different systems and software.
SSO allows IT departments to administrator a single identity that can access many machines and cloud services.

upvoted 4 times

Load full discussion...

We are the biggest and most updated IT certification exam material website.

Using our own resources, we strive to strengthen the IT professionals community for free.

ExamTopics doesn't offer Real Microsoft Exam Questions. ExamTopics doesn't offer Real Amazon Exam Questions. ExamTopics Materials do not contain actual questions and answers from Cisco's Certification Exams.

CFA Institute does not endorse, promote or warrant the accuracy or quality of ExamTopics. CFA® and Chartered Financial Analyst® are registered trademarks owned by CFA Institute.