

🔗 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 156 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 156

Topic #: 1

[\[All Professional Cloud Security Engineer Questions\]](#)

Your company plans to move most of its IT infrastructure to Google Cloud. They want to leverage their existing on-premises Active Directory as an identity provider for Google Cloud. Which two steps should you take to integrate the company's on-premises Active Directory with Google Cloud and configure access management? (Choose two.)

- A. Use Identity Platform to provision users and groups to Google Cloud.
- B. Use Cloud Identity SAML integration to provision users and groups to Google Cloud.
- C. Install Google Cloud Directory Sync and connect it to Active Directory and Cloud Identity.
- D. Create Identity and Access Management (IAM) roles with permissions corresponding to each Active Directory group.
- E. Create Identity and Access Management (IAM) groups with permissions corresponding to each Active Directory group.

Show Suggested Answer

by [GHOST1985](#) at *Sept. 12, 2022, 12:44 p.m.*

### Comments

Type your comment...

Submit



🗨️ [GHOST1985](#) Highly Voted 2 years, 10 months ago

**Selected Answer: CE**

<https://cloud.google.com/architecture/identity/federating-gcp-with-active-directory-synchronizing-user-accounts?hl=en>

[https://cloud.google.com/architecture/identity/federating-gcp-with-active-directory-synchronizing-user-accounts?hl=en#deciding\\_where\\_to\\_deploy\\_gcds](https://cloud.google.com/architecture/identity/federating-gcp-with-active-directory-synchronizing-user-accounts?hl=en#deciding_where_to_deploy_gcds)

   upvoted 9 times


  **Test114** 2 years, 10 months ago

How about BE?

<https://cloud.google.com/architecture/identity/federating-gcp-with-active-directory-introduction>


"Single sign-on: Whenever a user needs to authenticate, Google Cloud delegates the authentication to Active Directory by using the Security Assertion Markup Language (SAML) protocol."

   upvoted 1 times

  **zellick** 2 years, 10 months ago




SAML is used for authentication, not provisioning.

   upvoted 4 times

  **AzureDP900** 2 years, 8 months ago

CE sounds good

   upvoted 2 times

  **AwesomeGCP** **Highly Voted**  2 years, 9 months ago

**Selected Answer: CE**

C. Install Google Cloud Directory Sync and connect it to Active Directory and Cloud Identity.

E. Create Identity and Access Management (IAM) groups with permissions corresponding to each Active Directory group.

   upvoted 7 times

  **1209apl** **Most Recent**  3 months ago

**Selected Answer: CE**

Agree: C & E.

   upvoted 1 times

  **BPzen** 8 months ago

**Selected Answer: CE**

Google Cloud Directory Sync (GCDS):

Synchronizes user and group data from on-premises Active Directory to Cloud Identity, which is essential for enabling Active Directory as an identity provider.

IAM Groups:

Google Cloud IAM groups allow permissions to be managed collectively for a group of users.

By aligning IAM groups with Active Directory groups, you can streamline access management across Google Cloud resources.

   upvoted 2 times

  **BPzen** 8 months ago

**Selected Answer: CE**

To integrate on-premises Active Directory with Google Cloud for identity and access management, you need to synchronize your Active Directory users and groups with Google Cloud and map them to appropriate IAM permissions.

C. Install Google Cloud Directory Sync and connect it to Active Directory and Cloud Identity.

Google Cloud Directory Sync (GCDS) is used to synchronize users and groups from an on-premises Active Directory to Cloud Identity or Google Workspace.

This ensures that user accounts and group memberships in Google Cloud mirror the structure of your Active Directory.

E. Create Identity and Access Management (IAM) groups with permissions corresponding to each Active Directory group. After synchronizing groups from Active Directory to Google Cloud, you create IAM groups in Google Cloud and assign the appropriate permissions.

Using IAM groups simplifies access control by allowing permissions to be managed at the group level instead of the user level.

   upvoted 1 times

  **Roro\_Brother** 1 year, 2 months ago

**Selected Answer: CD**

GCDS is already creating the groups automatically. We need to create the IAM roles to assign to those groups. So D, not E

   upvoted 2 times



  **Betotoxicity** 1 year, 3 months ago

**Selected Answer: CD**

CD

Why not E?: IAM groups in Google Cloud are separate entities from IAM roles. While you could create IAM groups that mirror Active Directory groups, directly mapping permissions to IAM roles based on the corresponding Active Directory groups offers a more efficient and granular approach to access control.


   upvoted 2 times

  **glb2** 1 year, 4 months ago

**Selected Answer: CD**

Answer is C and D.

   upvoted 2 times

  **PTC231** 1 year, 4 months ago

ANSWER C and E

C. Install Google Cloud Directory Sync and connect it to Active Directory and Cloud Identity: Google Cloud Directory Sync (GCDS) is used to synchronize user and group information from on-premises Active Directory to Google Cloud Identity. This step ensures that user and group information is consistent across both environments.

E. Create Identity and Access Management (IAM) groups with permissions corresponding to each Active Directory group: Once the synchronization is set up, you can create IAM groups in Google Cloud that mirror the Active Directory groups. Assign permissions to these IAM groups based on the roles and access levels required for each group. This approach simplifies access management by aligning Google Cloud permissions with existing Active Directory groups.



   upvoted 2 times

  **PhuocT** 1 year, 5 months ago

**Selected Answer: CD**

C and D I think, we don't need to create group, as it will be synced from AD, we only need to focus on creating the role for the group.



   upvoted 3 times

  **desertlotus1211** 1 year, 5 months ago

Answers: B & C...

There is NO such thing as IAM groups in GCP



   upvoted 1 times

  **mjcts** 1 year, 5 months ago

**Selected Answer: CD**

GCDS is already creating the groups automatically. We need to create the IAM roles to assign to those groups. So D, not E

   upvoted 3 times

  **aygitci** 1 year, 9 months ago

**Selected Answer: CD**

Not Ek as the groups are already synced and retrieved, so roles will be attached to them

   upvoted 6 times

  **gkarthik1919** 1 year, 10 months ago

CE are seems to be coorrect. B is required only for SSO. GCDS would also provision user and group.



   upvoted 1 times

  **Mithung30** 1 year, 11 months ago

**Selected Answer: CD**

CD is correct

   upvoted 4 times

  **a190d62** 1 year, 12 months ago

**Selected Answer: CD**

There is a possibility to synchronize groups between AD and Google Cloud so why not to use it and focus on creating roles

[https://cloud.google.com/architecture/identity/federating-gcp-with-active-directory-introduction?hl=en#mapping\\_groups](https://cloud.google.com/architecture/identity/federating-gcp-with-active-directory-introduction?hl=en#mapping_groups)

   upvoted 3 times

  **tauseef71** 2 years, 4 months ago

CD is the right answer. C> sync with AD user and groups ; D> give users and groups the roles in IAM.

   upvoted 4 times

[Load full discussion...](#)



## Platform

---

> [Home](#)

> [Examtopics PRO](#)

> [All Exams](#)

> [Training Courses](#)

