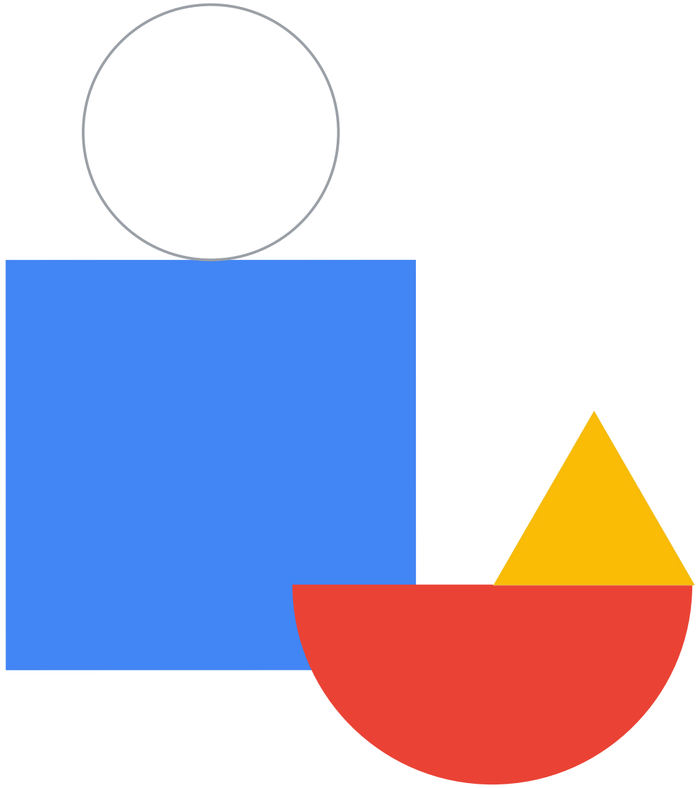
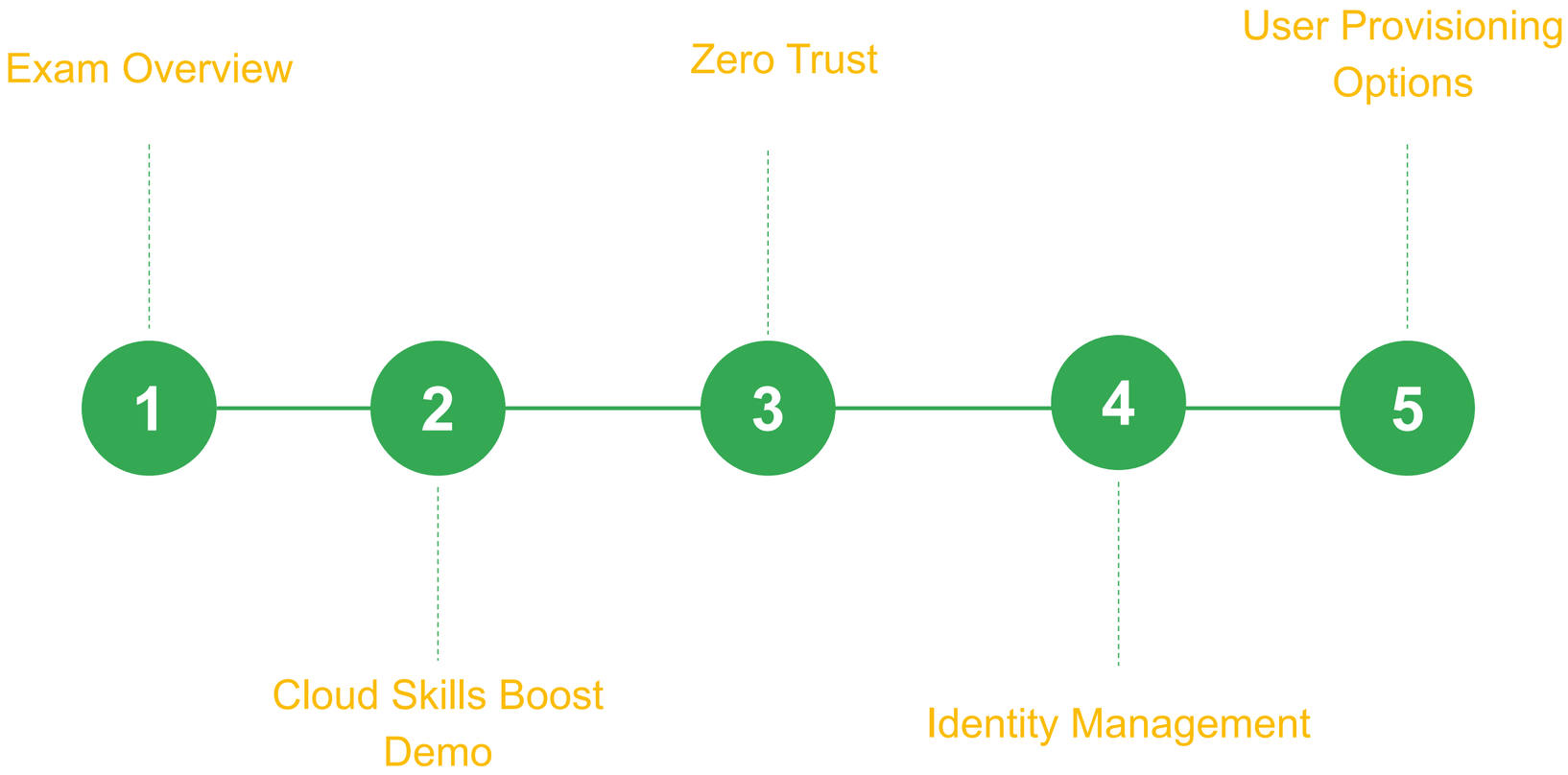
Google Cloud



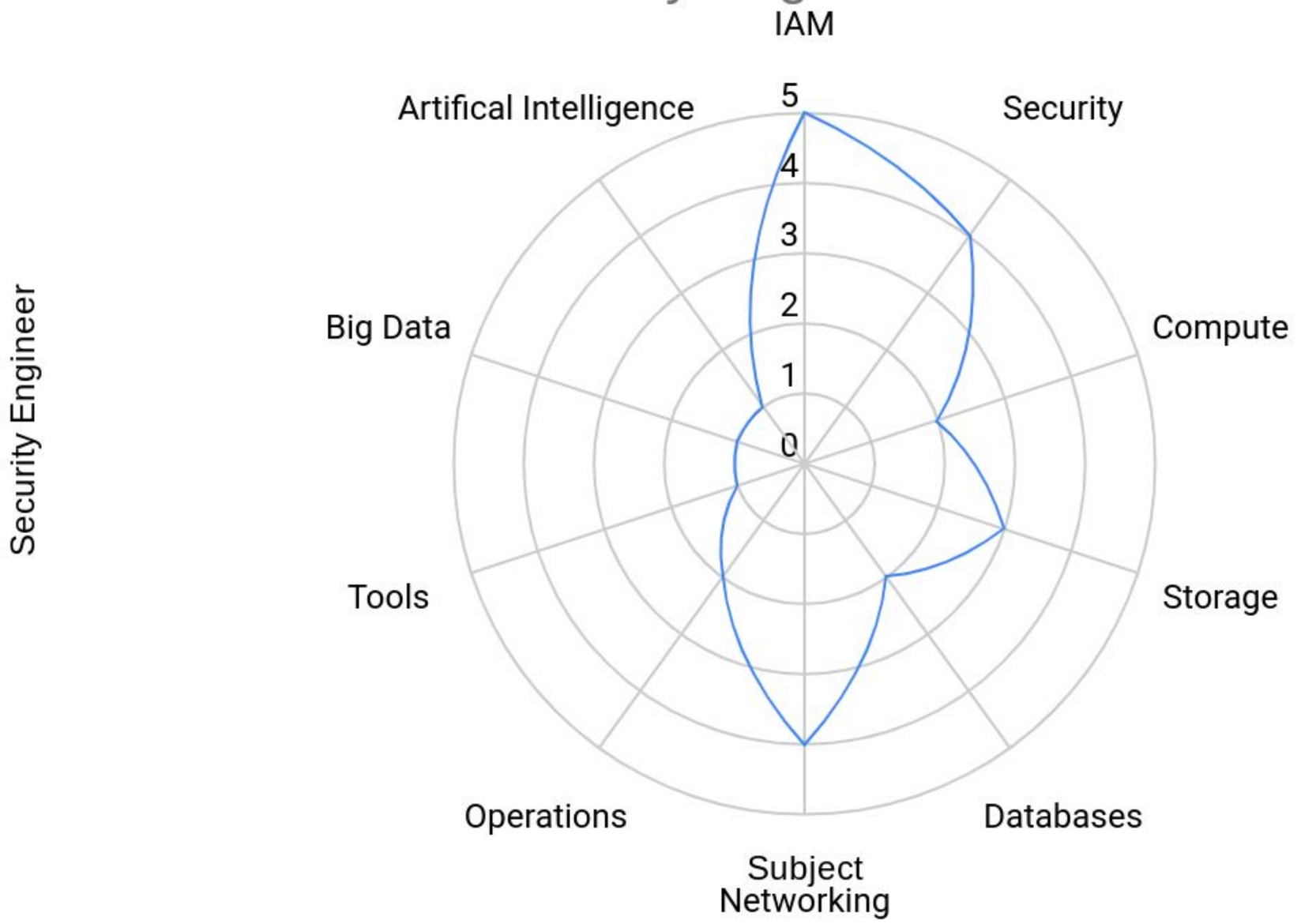
Preparing for your Professional Cloud Security Engineer Journey

Who am I and what's my role here?

Week 1 topics



Professional Cloud Security Engineer



PCSE Exam High-level Overview

- 80h-150h+ to complete. Consistency is the key! 2-3 hours a day, starting from now...
- Exam structure:
  - Get a feeling by doing a sample test.
  - ~50 questions / 2h for the exam. *Exam tip: Handle the easier questions first (aim at ~1.5 min per question), mark the rest for review. Also, don't leave any questions unanswered (no negative points).*
  - Multiple-choice theoretical questions, but asking about "real-world" challenges. Most with a single correct answer, some with more (you will know how many).
  - In a lot of cases, you will need to choose BEST answer from 2-4 which are technically correct.
  - *Exam tip: Start by eliminating the most obvious wrong choices.*
  - NO labs, NO hands-on exercises (but essential when preparing!), NO case-studies on the exam.
  - English language only (no additional time for non-native speakers).
- It's not clear what is the percentage needed to pass (aim at 85+% accuracy for practise questions).
- Can be taken online or at a testing center.
- Certificate is valid for 2 years.
- If you fail, retake policy is: 14 days / 60 days / 1 year (separate voucher needed for each attempt)
- 20-min video on how to prep for PCSE and PCNE exam

Exam question - example

Notice the business context

Sample quiz

A Cloud Development team needs to use service accounts extensively in their local environment. You need to provide the team with the keys for these service accounts. You want to follow Google-recommended practices.
What should you do?

A. Implement a daily key rotation process that generates a new key and commits it to the source code repository every day.

B. Implement a daily key rotation process, and provide developers with a Cloud Storage bucket from which they can download the new key every day.

C. Create a Google Group with all developers. Assign the group the IAM role of Service Account User, and have developers generate and download their own keys.

D. Create a Google Group with all developers. Assign the group the IAM role of Service Account Admin, and have developers generate and download their own keys.

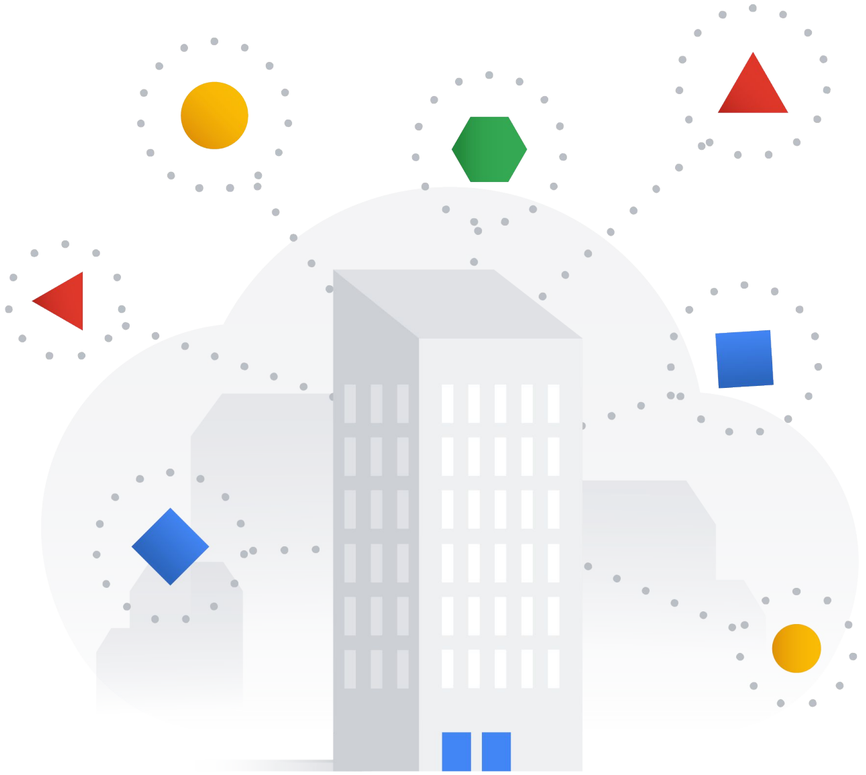
Understand the scope of the exam based on the Professional Cloud Security Engineer Exam Guide.

cloud.google.com/certification/guides/cloud-security-engineer

What is the role of a Professional Cloud Security Engineer?

- Should be proficient in:
  - Identity and access management
  - Defining organizational structure and policies
  - Using Google Cloud technologies to provide data protection
  - Configuring network security defenses
  - Collecting and analyzing Google Cloud logs
  - Managing incident responses
  - Applying dynamic regulatory considerations

- For more information, visit the Professional Cloud Security Engineer certification page

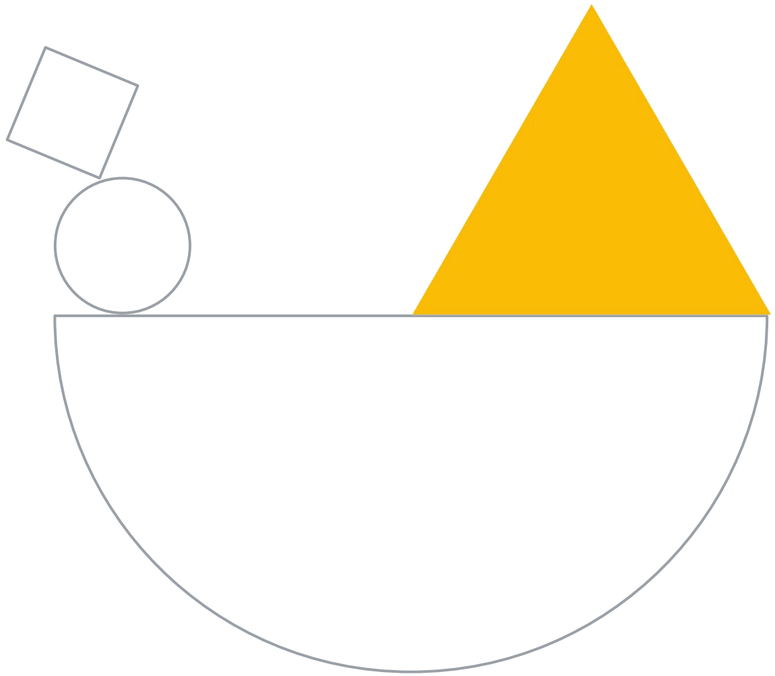


Cymbal Bank

Digitally Transforming

A nationally-recognized American retail bank founded in 1920 and acquired by Cymbal in 1975.

Resources to support your certification journey



See what others think…

Published	Title/Link	Author
2022/07	Preparing for the PCSE Exam	Ammett Williams
2021/10	My review on the PCSE Beta Exam	Antoni Tzavelas
2020/02	BeyondProd: A new approach to cloud-native security	Google
2019/11	Exam Study Guide	Mark Johnson
2019/11	Google Cloud Security Engineer Exam Notes	Travis Webb
2019/08	How to pass the Google Professional Cloud Security Engineer certification	Ivam Luz
2019/08	Google Cloud Security Exam Experience: RTFQ twice	Jaroslav Pantsjoha
2019/07	Exam Prep Sheet	Ammett Williams
2019/06	How to fail and then pass the Security Engineer Exam	Ammett Williams
2019/05	Google Professional Cloud Security Engineer Certification	John Hanley
2019/03	Google Professional Cloud Security Engineer—Beta exam review	Rakesh Sharma
2019/02	Notes from my beta Google Cloud Professional Security Engineer Certification Exam	Sathish VJ
2019/02	Google Professional Cloud Security Engineer Beta Exam walkthrough	Dmitri Lerko
2019/02	Google Cloud Professional Security Engineer Exam Guide	Darpan Shah
2018/03	Google Cloud Security Whitepapers	Google
	Path to Professional Security Engineer	Google

LINK

Additional resources - quizzes

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. 1 point

What should your team do to meet these requirements?

- ○ Set up Cloud Directory Sync to sync groups, and set IAM permissions on the groups.
- ○ Set up SAML 2.0 Single Sign-On (SSO), and assign IAM permissions to the groups.
- ○ Use the Cloud Identity and Access Management API to create groups and IAM permissions from Active Directory.
- ○ Use the Admin SDK to create groups and assign IAM permissions from Active Directory.

- Aim: validate **technical** knowledge (no business context)
- NOT as complex as questions on the exam

Pro tip: Make notes while you learn!!!

- Choose your favourite tool that handles text **and images**.
- Copy & paste from GCP documentation / course transcripts
- Copy & paste important slides / images / decision trees / tables
- Use colours / bold
- Paste difficult quiz questions from quizzes etc with explanations / links to solutions
- Remember about 2-year validity of GCP certificates -> notes will most probably be very useful next time.

Custom roles
https://cloud.google.com/iam/docs/creating-custom-roles

Use the gcloud iam list-testable-permissions command to get a list of permissions that are available for custom roles in a specific project or organization. The response lists the permissions that you can use in custom roles for that project or organization.

To list permissions that are available in custom roles for a project or organization, run this command:

*gcloud iam list-testable-permissions **full-resource-name***
--filter="customRolesSupportLevel!=NOT_SUPPORTED"

You can create a custom role at the project or organization level. = NOT ON FOLDER LEVEL!!

To view the role metadata, use one of the methods below:

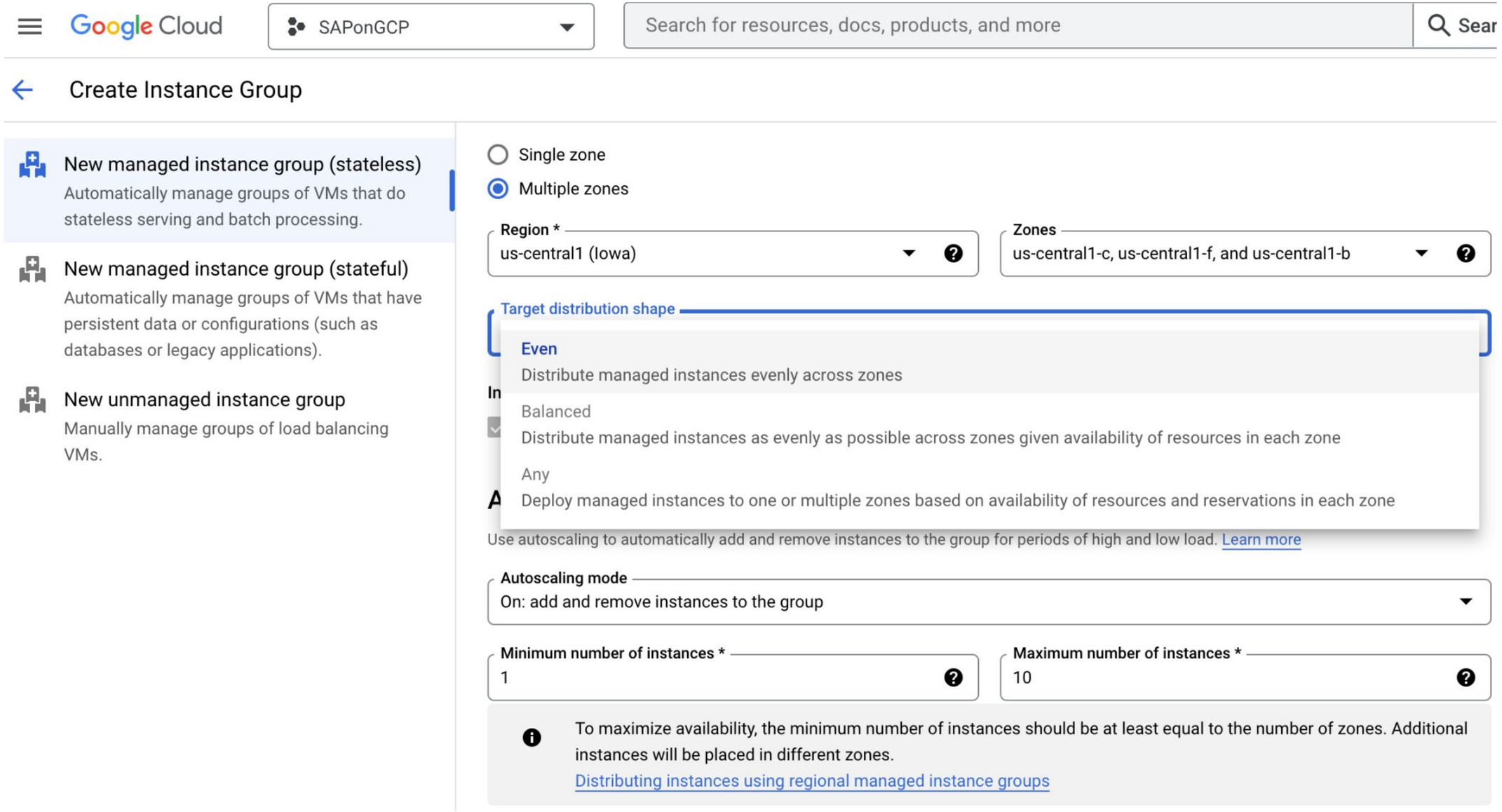
gcloud iam roles describe role-id

Example:

```
gcloud iam roles describe roles/iam.roleViewer
```

```
description: Read access to all custom roles in the project.
etag: AA==
includedPermissions:
- iam.roles.get
```

Pro tip no.2: be curious!

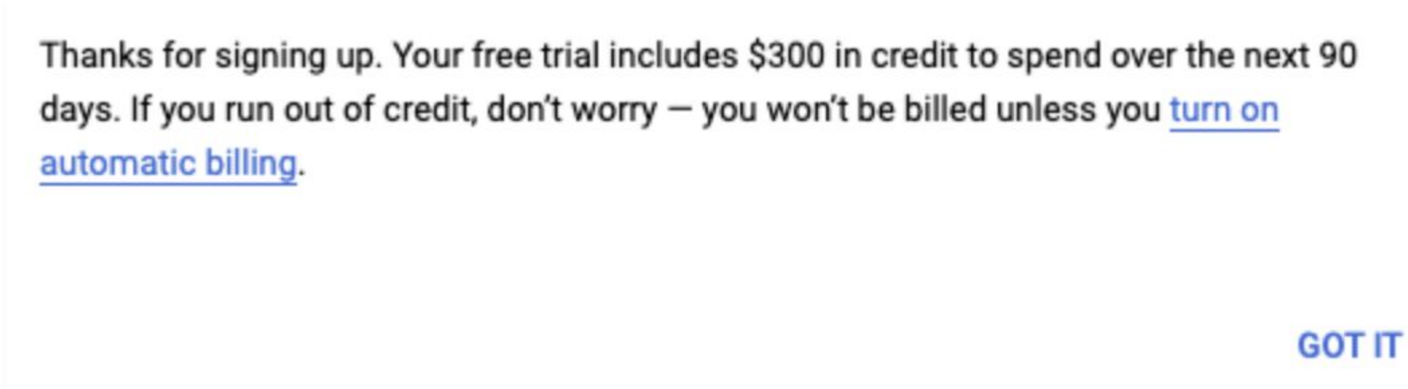


Pro tip no.3: use GCP Free Trial 300USD (*) and Free Tier

It will help you be curious :)

- **90-day, $300 Free Trial**: New Google Cloud and Google Maps Platform users can take advantage of a 90-day trial period that includes $300 in free Cloud Billing credits to explore and evaluate Google Cloud and Google Maps Platform products and services. You can use these credits toward one or a combination of products.

https://cloud.google.com/free

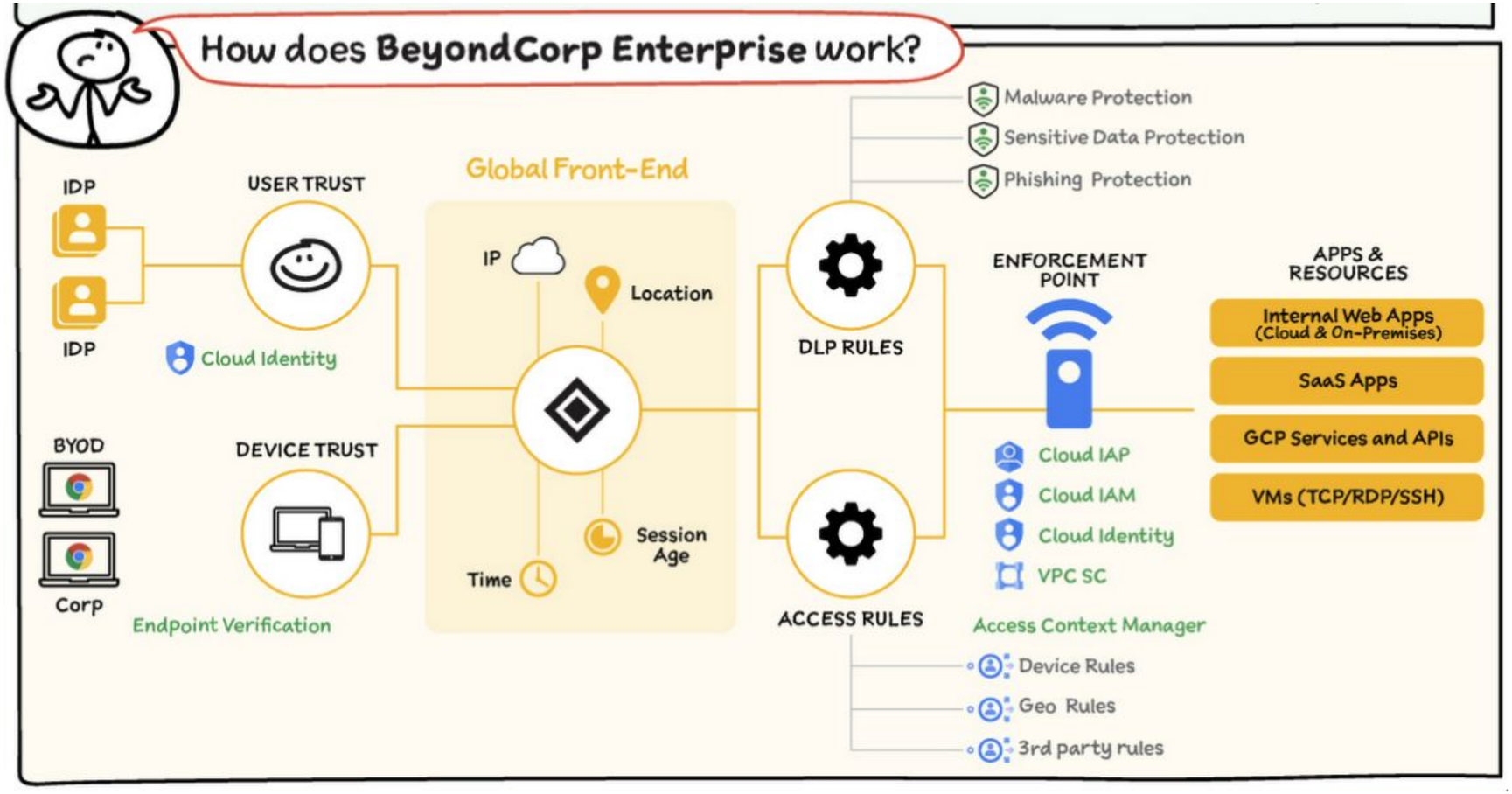


* To complete your Free Trial signup, you must provide a credit card or other payment method to set up a Cloud Billing account and verify your identity. Don't worry, setting up a Cloud Billing account does not enable us to charge you. You are not charged unless you explicitly enable billing by upgrading your Cloud Billing account to a paid account.

Cloud Skills Boost Demo

Let’s start the technical part!

BeyondCorp and BeyondProd: Google's approach to Zero Trust



Intro to Zero Trust; BeyondCorp whitepaper; BeyondProd whitepaper

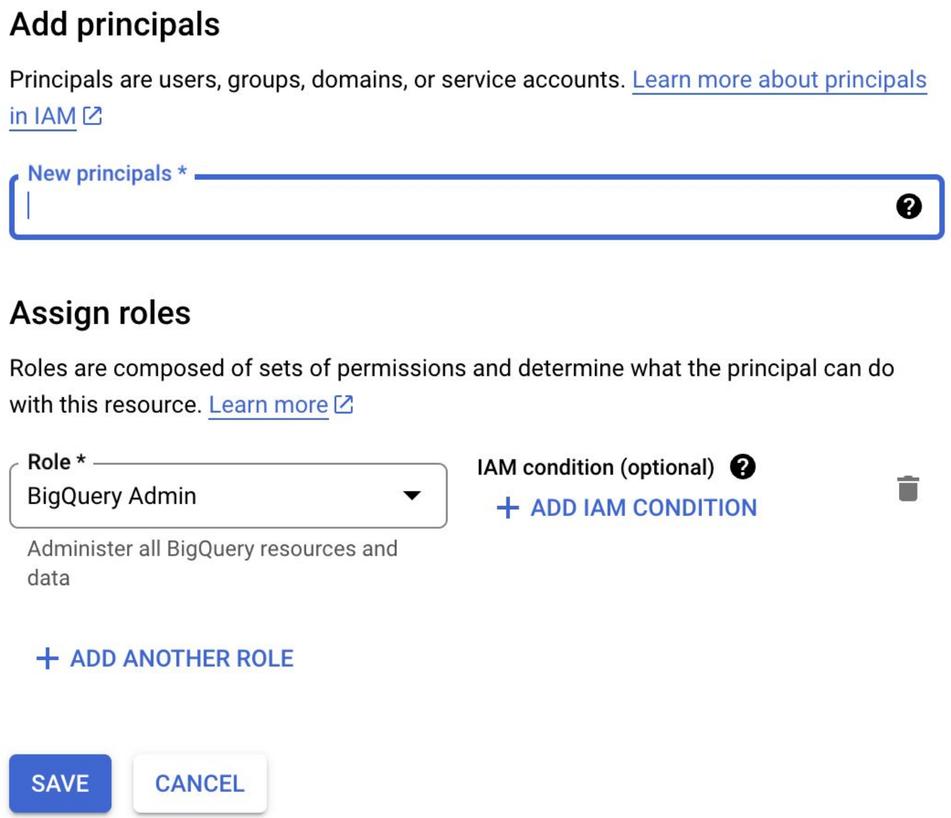
Identity Management

Identity management

"To use Google Cloud, users and workloads need an identity that Google Cloud can recognize."

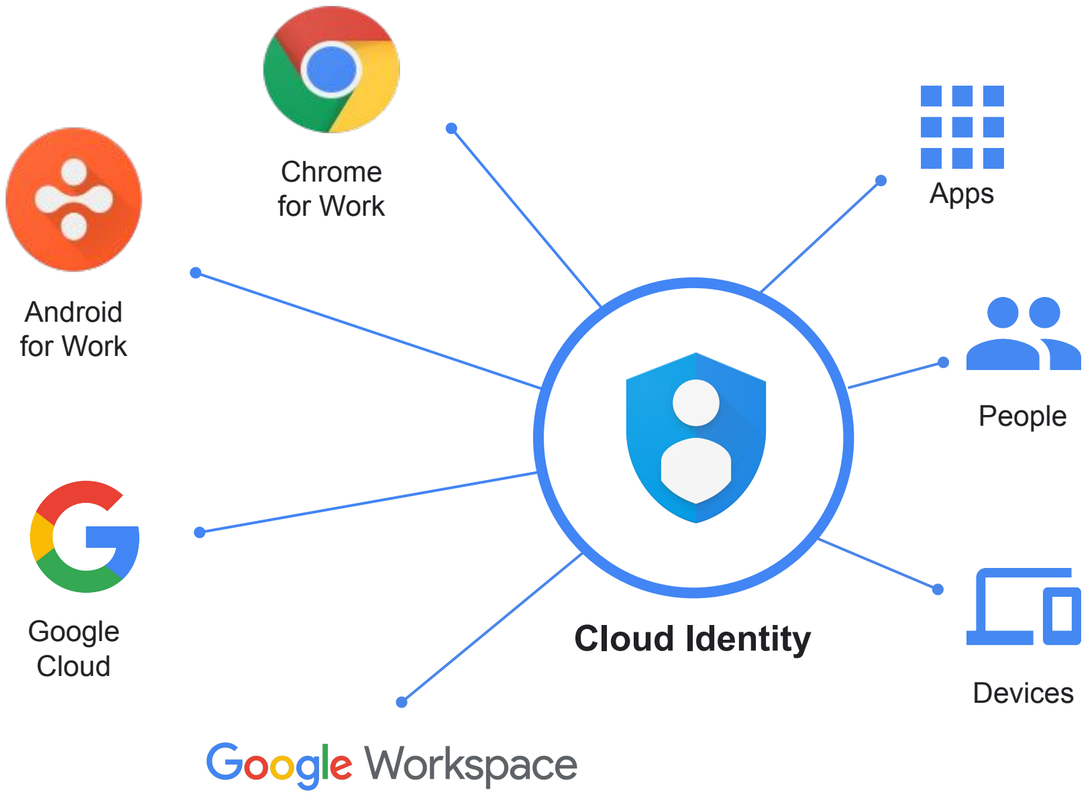
Your options are:

- Google Account… rather not a preferred option from security perspective
- Cloud Identity / Google Workspace accounts
- Federated accounts from 3rd party IdP
    - Replicated to Cloud Identity
    - Not replicated (using Workforce Identity Federation)



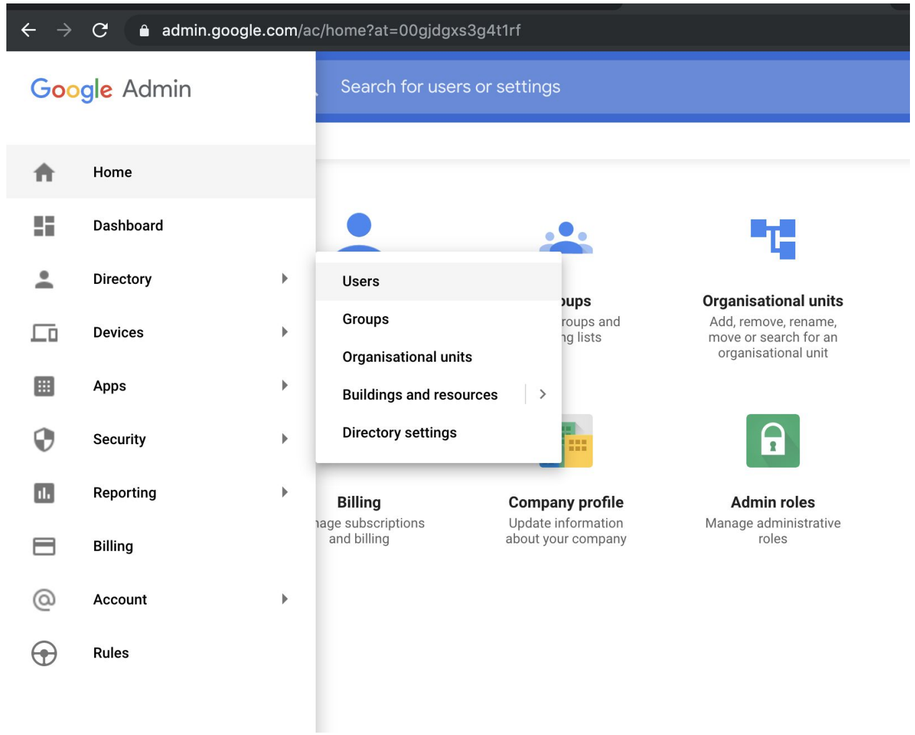
Exam Tip: *have a look at this document to get a better understanding of the options.*

What is Cloud Identity?



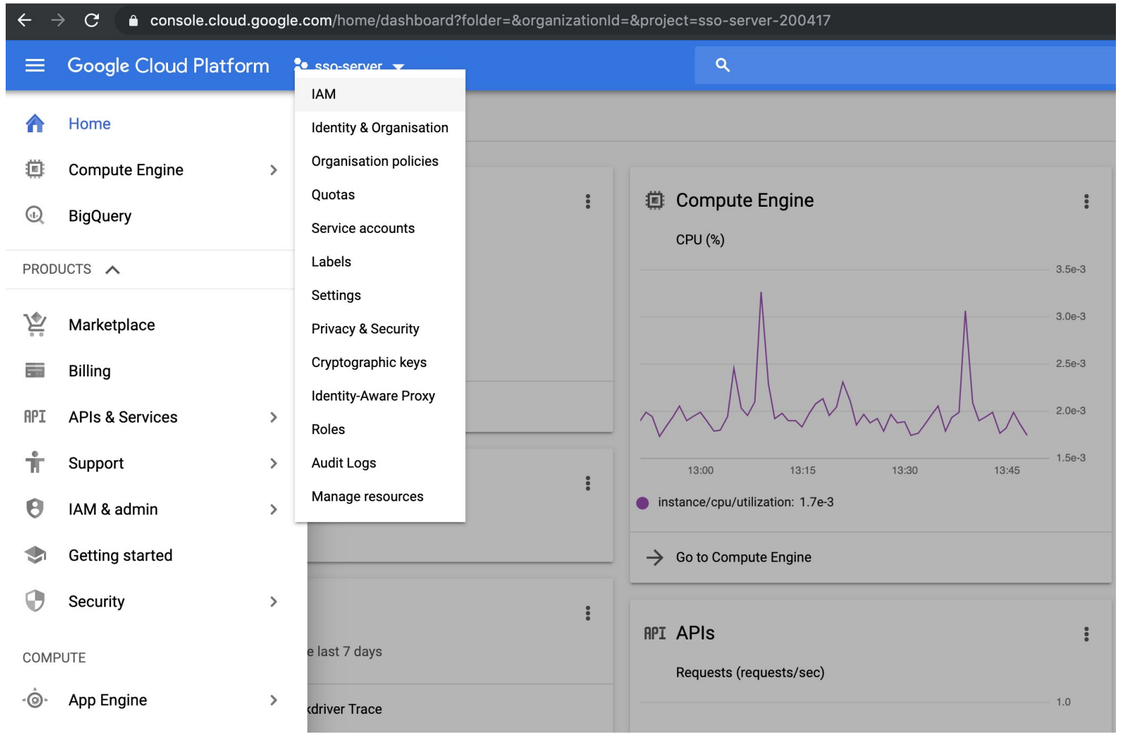
- Cloud Identity is an Identity as a Service (IDaaS) solution that **allows you to centrally manage users and groups** who can access Google Cloud and Google Workspace (formerly known as G Suite) resources
- It is the same identity service that powers Google Workspace and can also be used as IdP for third-party applications (supports SAML and LDAP applications)

Two consoles for administration



Cloud Identity (`admin.google.com`)

Managing Users, Groups, and Authentication settings



Google Cloud (`console.cloud.google.com`)

Roles & Authorization for Google Cloud

Cloud Identity vs IAM

Cloud Identity	IAM
Identity as a Service (IDaaS) solution that centrally manages users and groups. Often configured to federate identities between Google and other identity providers (AD etc).	Service that lets authorize who can take action on specific GCP resources
In Cloud Identity, you manage BOTH identities AND privileges (via roles). However, it's NOT GCP-specific…	With IAM, you manage privileges (via roles) only. Identities need to be created in advance, in most cases: in Cloud Identity (with the exception of Service Accounts).
Most important role: Super Admin (full access and manage other Admins). Needed to configure GCP organization (= grant Oganization Administrator role to others). NOT for daily use. Should use MFA	Most important role: Organization Administrator. Designed to manage day to day organization operations in GCP (= mostly grant IAM roles to identities).
Has a Free and Premium editions, each with different features.	

Exam Tips:

- *Make sure to differentiate and know best practices of Super Admin (Cloud Identity role) vs Organization Administrator (IAM Role)*
- *If you'd like to know how to create new GCP organization, see this guide.*

Two key admin functions

	(CI) Super Admin	(Cloud IAM) Org. Admin
Role	**Google Cloud Org. Admin by default**	It can add/assume any other IAM roles
Manages	**User/group account lifecycle** and Org's security settings	**IAM policies** and Resource Manager hierarchy
Delegates	**Google Cloud Org. Admin role** and CI admin roles	**Google Cloud IAM roles** to users and groups
Managed in	**Admin console**	**Google Cloud console**
Visibility	**Cloud Identity and Google Cloud environments**	**Google Cloud environment**

(Cloud Identity) Super Admin ≠ **(Cloud IAM) Organization Admin**

Exam Tip: *make sure to carefully go through this explanation of Super Admin and Org Admin roles.*

User provisioning

User provisioning in Cloud Identity

	Method	Effort	Staff involved	Notes
	Manual provisioning	High	Google Workspace admin	Easiest method, but not scalable
	CSV upload via Admin Console	Medium	Google Workspace admin	More flexibility, but not scalable
Best Practice	**Google Cloud Directory Sync**	**Medium**	**IdP Admin**	**Integrates with LDAP, scalable, requires no programming**
Best Practice	**3Third-party tools (Okta, Ping, Azure AD, ...)**	**Medium**	**IdP Admin**	**Scalable, may incur additional cost**
	Admin SDK Directory API	High	IdP Admin Development staff	Scalable, flexible, requires in-depth programming

Google Cloud Directory Sync (GCDS)

Best Practice

Provision from a single source of truth

Best Practice

Run in dedicated machine on-prem

- One-way synchronization of corporate data (no writing to LDAP system)
- Only synchronizes deltas for fastest possible provisioning
- Syncs all object types (users, aliases, profiles, groups, OUs, and shared contacts)
- Utilizes Google APIs to provision all object types, the same APIs available to customers

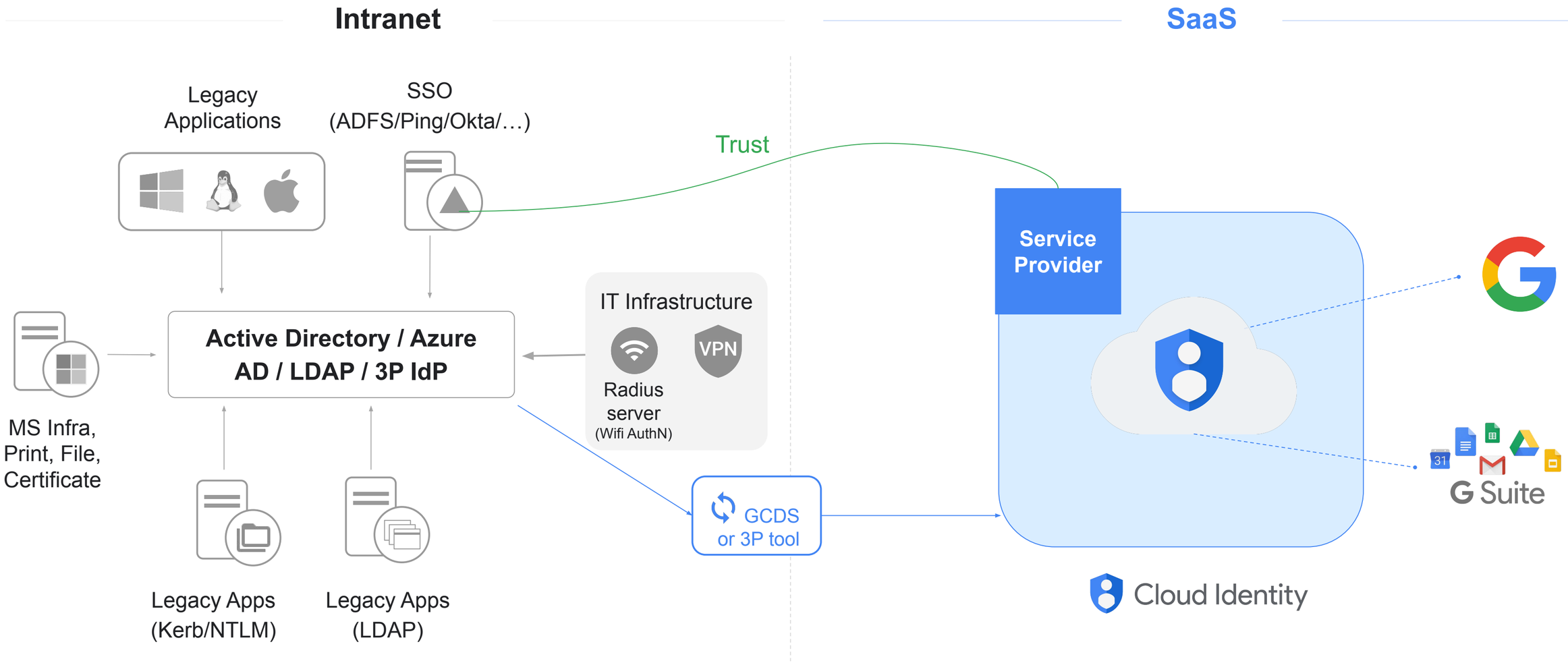
Exam Tips:

- *GCDS is a preferred user provisioning option, hence the exam will mostly focus on this one.*
- GCDS Best Practices

How Google Cloud Directory Sync works

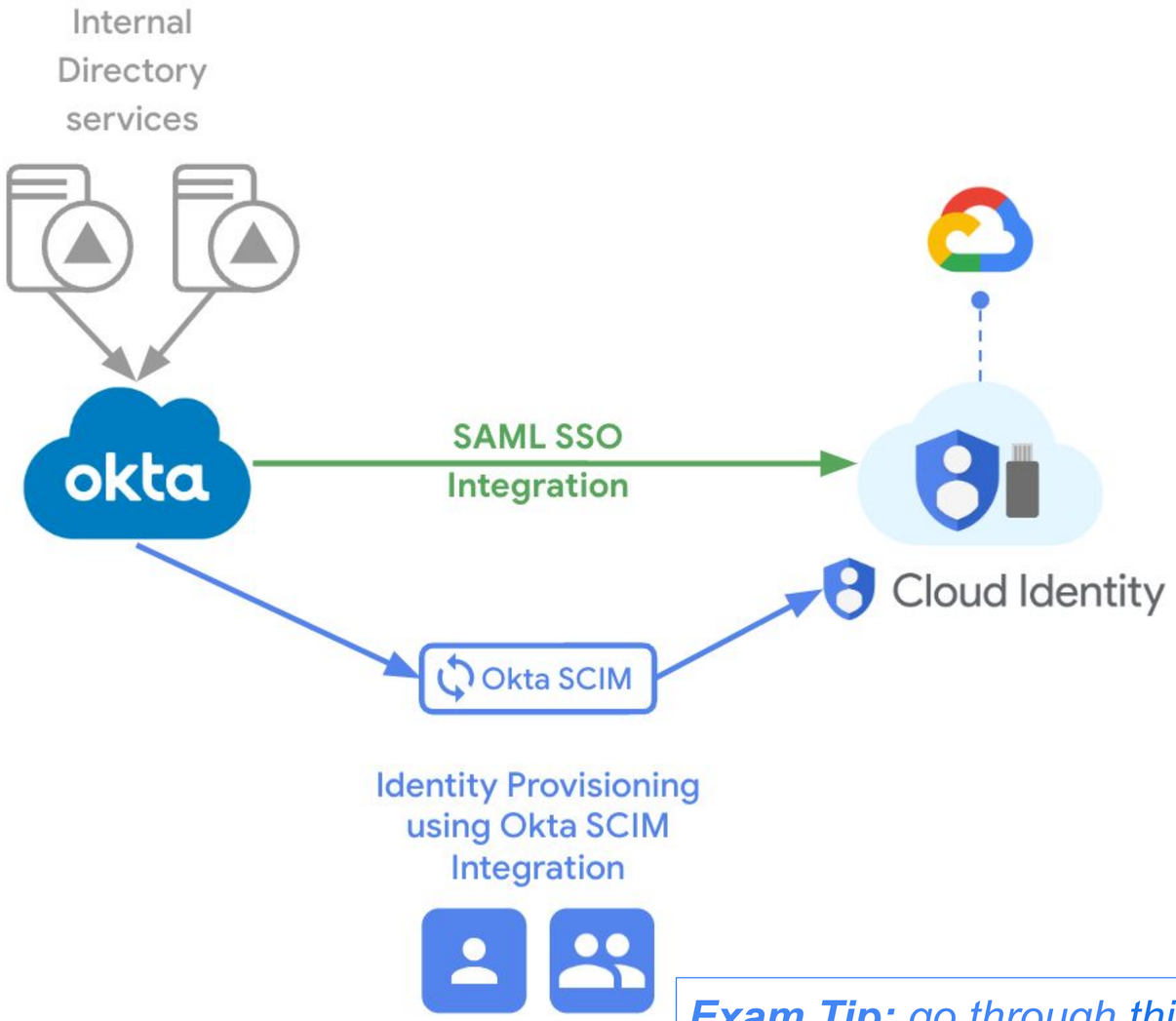
1. Data is exported from your LDAP server or Active Directory.
2. GCDS connects to the Google domain and generates a list of Google users, groups, and shared contacts that you specify.
3. GCDS compares these lists and updates your Google domain to match the data.
4. When the synchronization is complete, a report is emailed.

Third-party as an identity provider: Typical architecture



Exam Tip: *Have a look at typical GCDS + ADFS setup scenarios.*

Okta direct integration



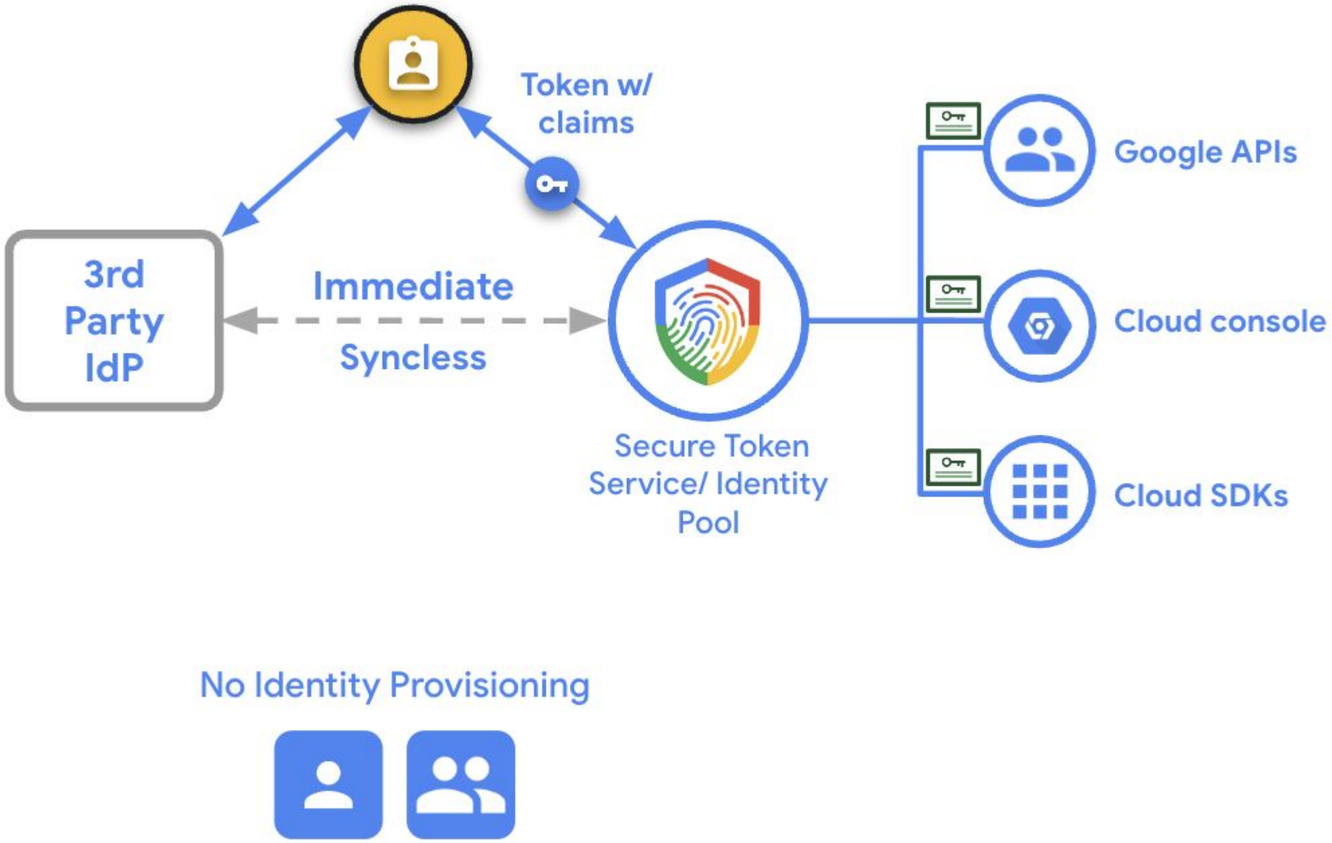
Complex enterprises often leverage an external IdP as a consolidation point for multiple directories, e.g. Okta

- Okta acts as the source of truth for corporate identity and authorisation
- Okta provisions relevant users and groups for use with GCP access policies
- SSO is provided through SAML integration to Google Cloud Identity, allowing seamless login
- 2SV options can be implemented through Cloud Identity for stronger protection
- Access to GCP Console and APIs can be further restricted using BeyondCorp access policies

Exam Tip: *go through this document to see how it works on high-level.*

Workforce Identity Federation

No need of identity provisioning in Cloud Identity

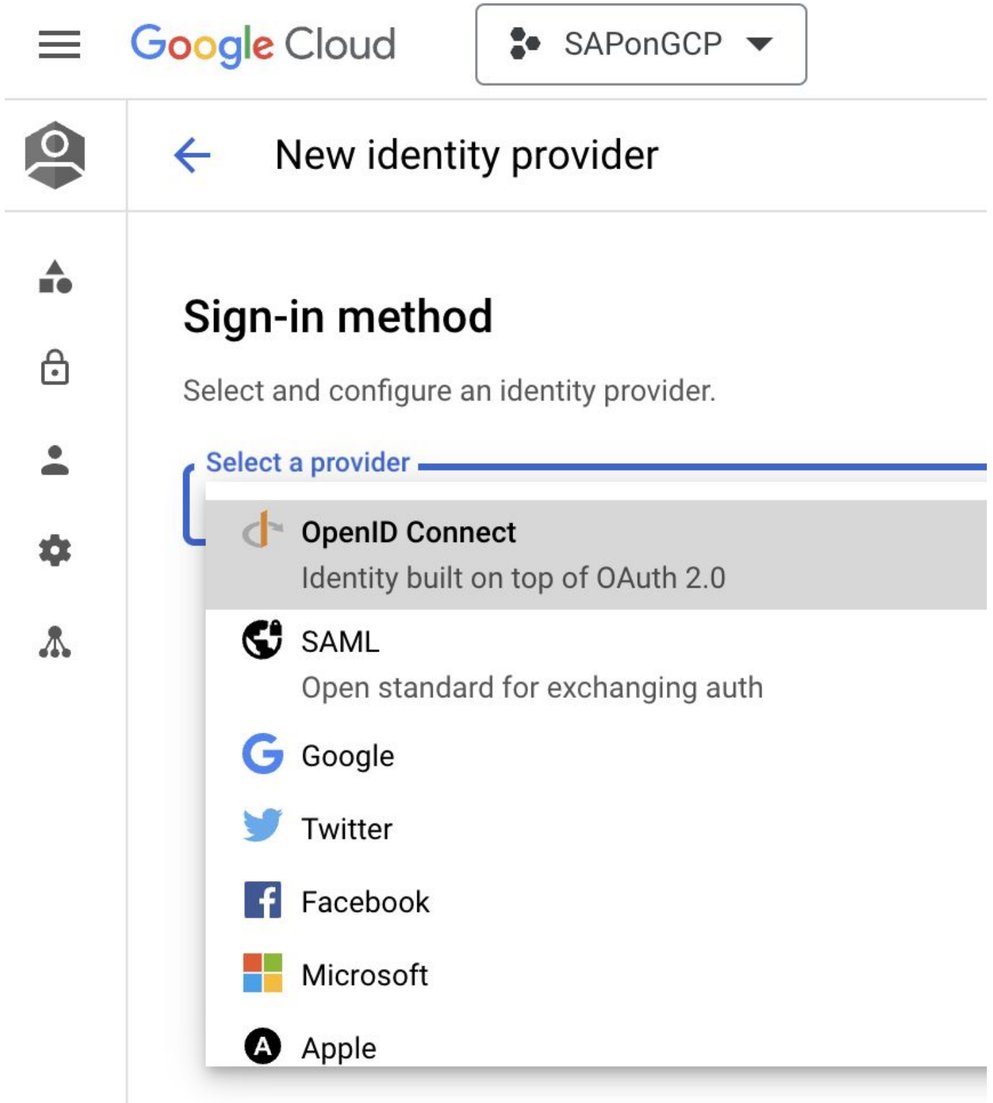


1. Secure access to GCP services and APIs without syncing identities to GCP (syncless) and while using their own identity provider
2. Able to create Identity pool per user type/group (employees, partners)
3. Supports multiple identity protocols (SAML, OIDC), multiple IdPs per identity pool
4. Allows you to control identity and personal data being shared with GCP

Exam Tips: *have a look at the overview of Workforce Identity Federation. In short, it aggregates human users, whereas Workload Identity Federation aggregates machine workloads.*

Identity Platform

Cloud Identity ≠ Identity Platform



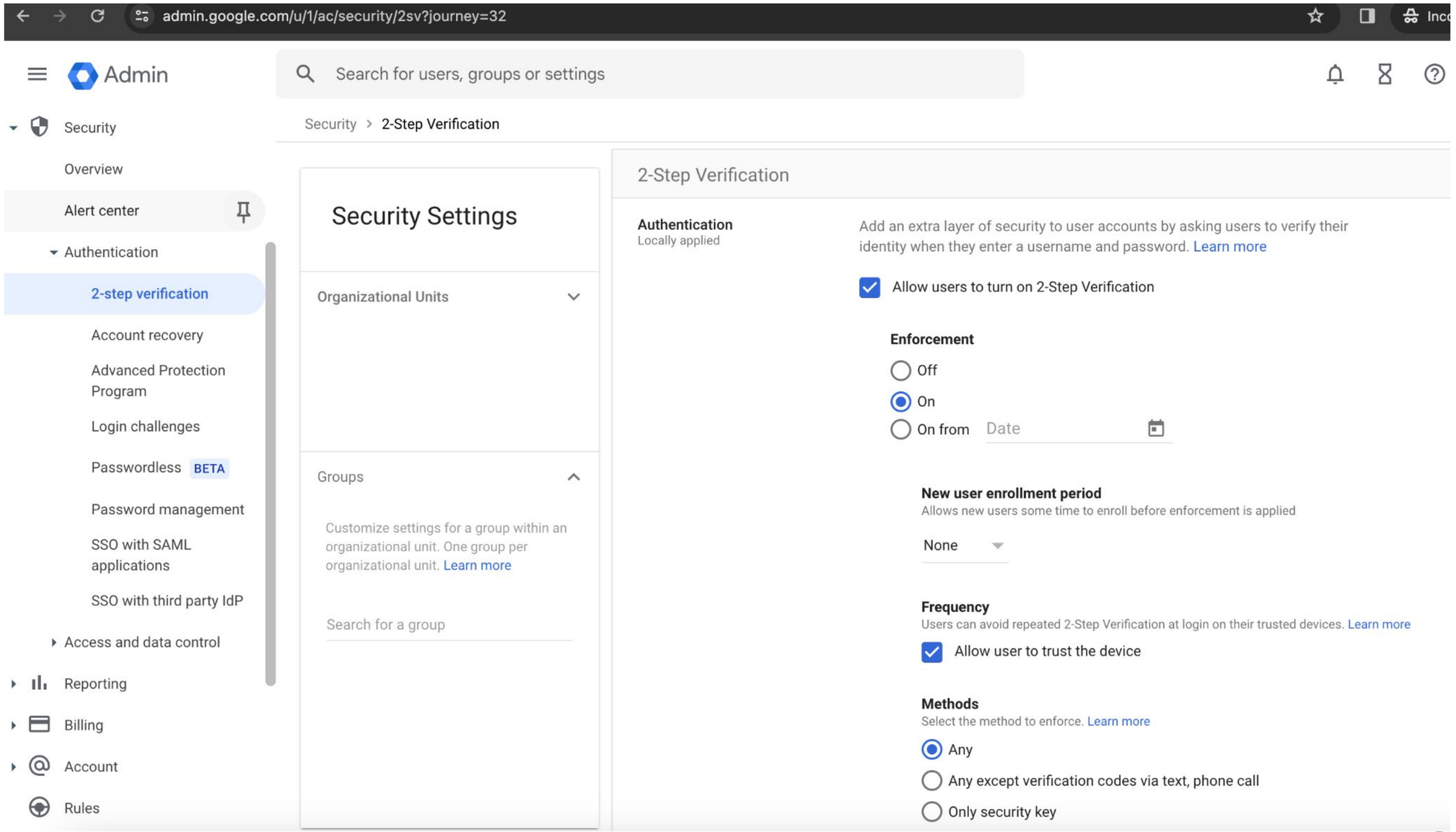
- **CUSTOMER IAM (CIAM)** which allows to add identity and access management functionality to your applications
- make it easier to manage and authentincate users to your apps and services.
- Example use-case: you (the app developer) are building an app and use GCIP + our SDKs to allow your customers to authenticate to this app.
- Identity Platform supports multiple authentication methods (SAML, OIDC, email/password, social, phone, and custom auth)

Cloud Identity, Identity Platform, Workforce Identity Platform, BeyondCorp …

Exam Tip: *must-read to get a high-level understanding of all those Identity Management products.*

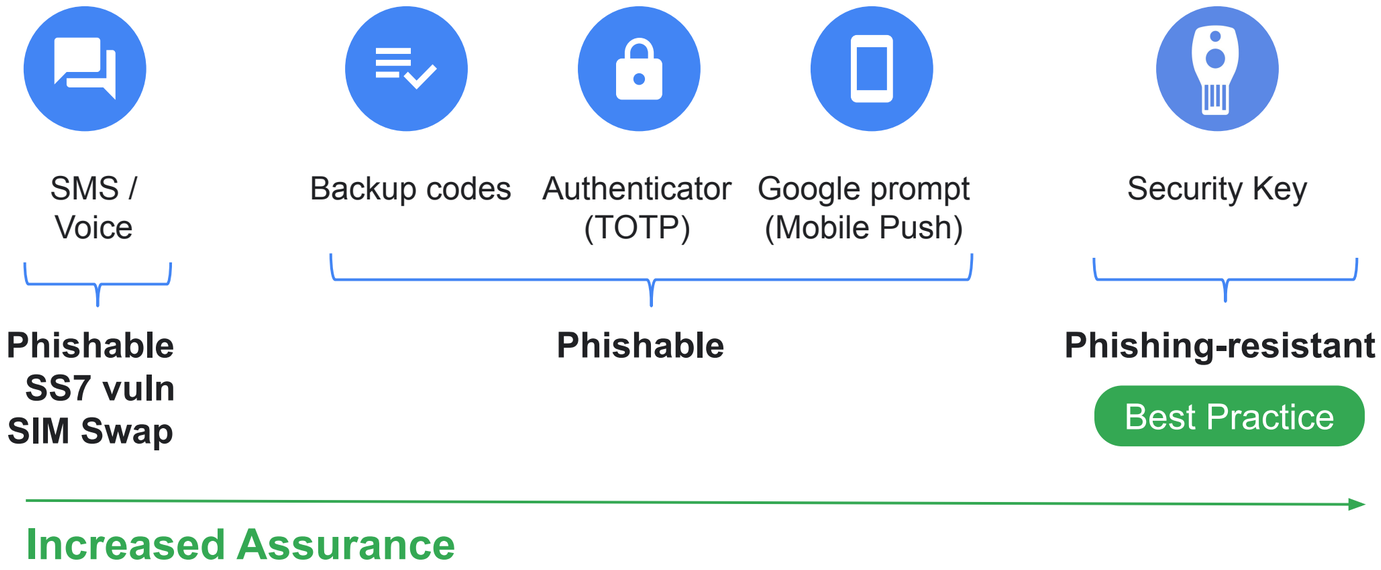
User Authentication
options

Enforcing 2-step verification (2SV) in Cloud Identity

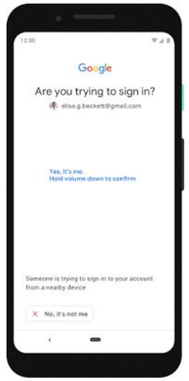


2SV with Google authentication

Any 2SV is better than no 2SV, but not all the 2SV methods are the same



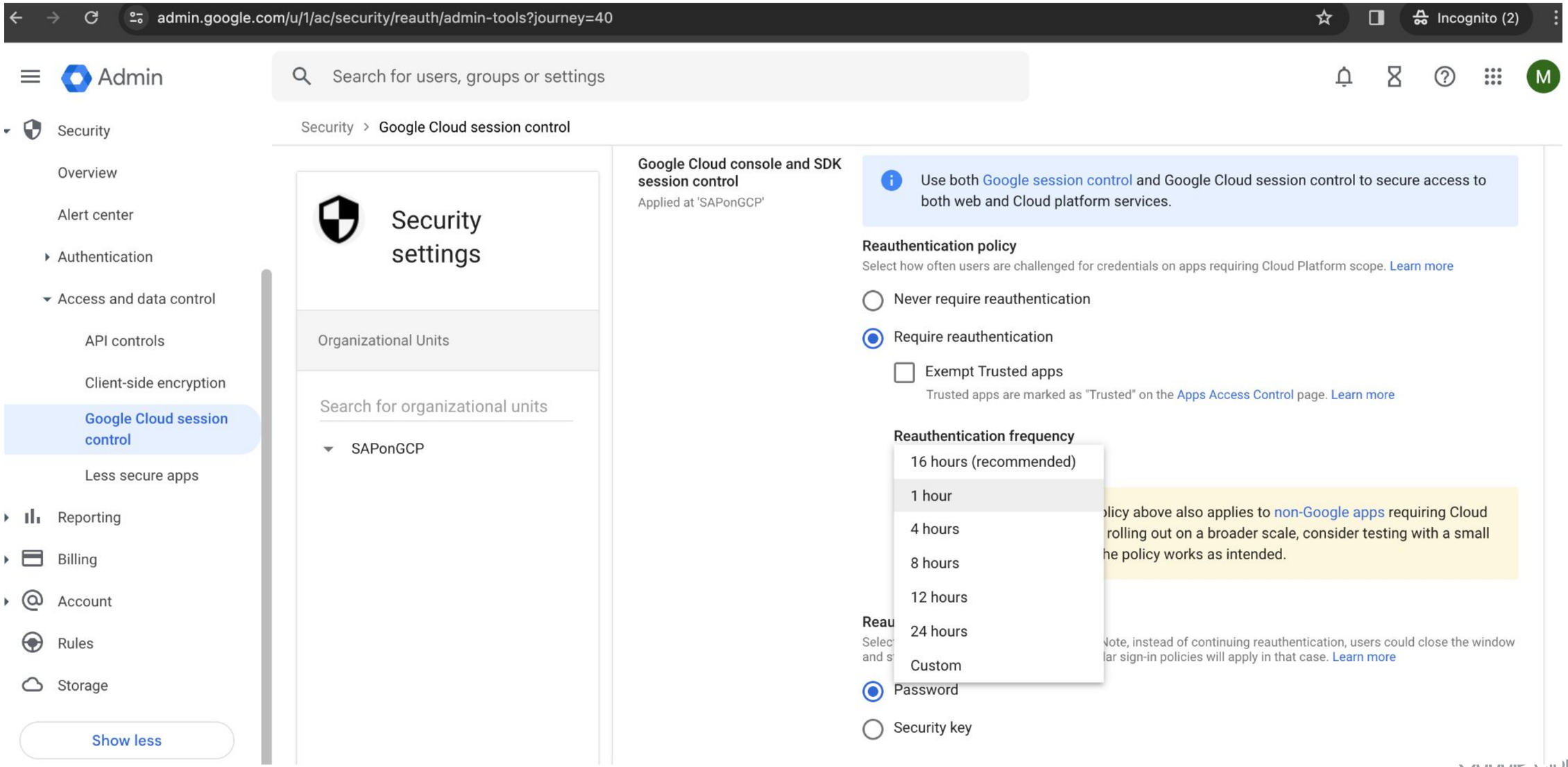
- 2SV adds critical protection against compromised passwords
- **Google recommends Security Keys for best in class security**
- Zero reported account hijackings after security key deployment
- **Google 2SV can be enforced also post-SSO**
- Android/iOS devices can also be used as Security Keys (!= Google Prompt)



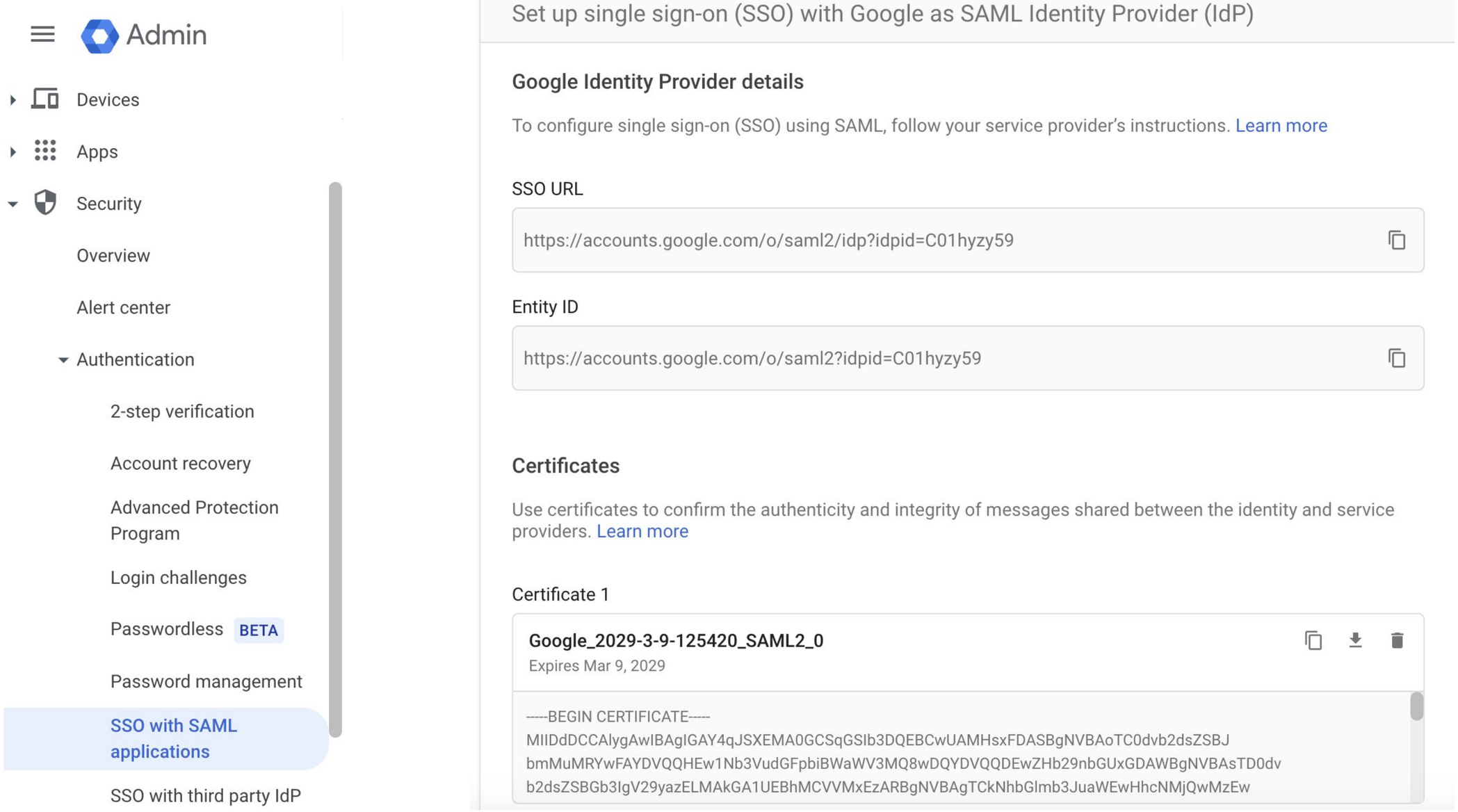
Hardware tokens

- Cloud Identity can enforce the use of security keys for 2SV
- Can enforce verification at every sign-on
- Provides stronger protection for admins and other high value users, using public key cryptography
- Works with security keys using the FIDO U2F (universal second factor) protocol, including Google's Titan security key
- A single key can be used for multiple identities
- Supports backup keys

Google Cloud session control (1h is the minimum)

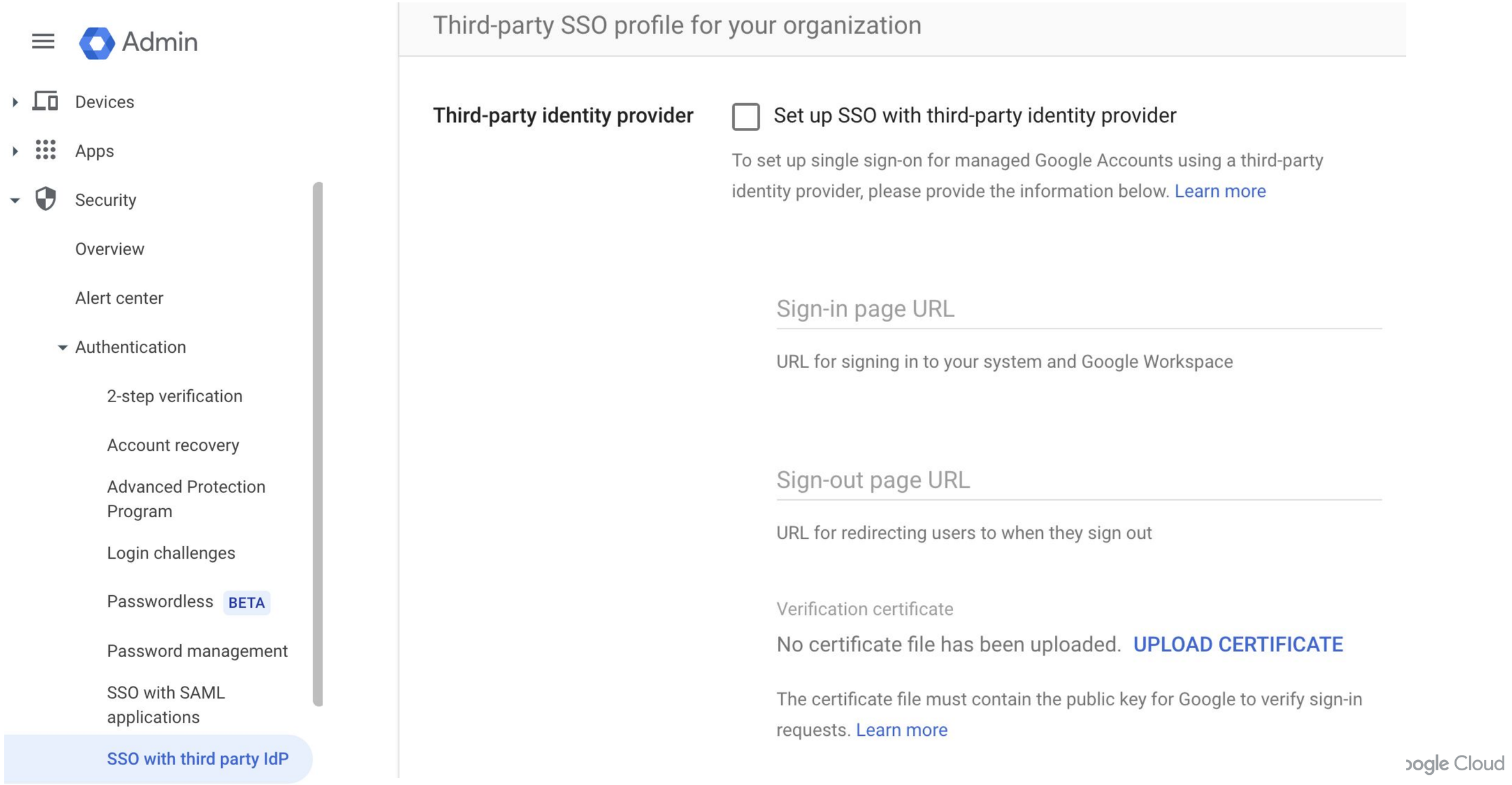


Configure single sign-on: Google as SAML Identity Provider



Google Cloud

Configure single sign-on: 3rd party Identity Providers



SSO authentication with third party

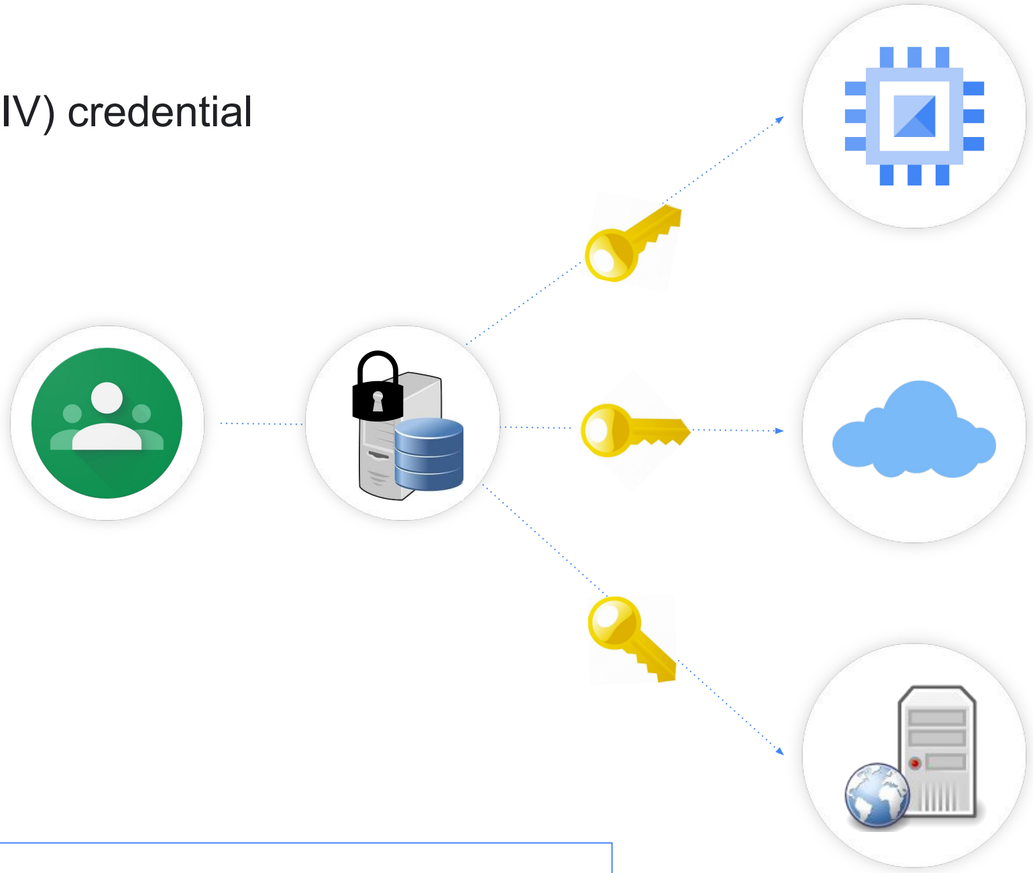
Delegate authentication to a third-party identity provider that is SAML 2.0 compliant (Azure, Ping Identity, Okta, etc.)

Pros

- Use for U.S government's Personal Identity Verification (PIV) credential
- Single credential for corporate web applications
- SSO servers can provide custom security controls (time, location, password policies, etc.)
- Leverage existing IDM and authentication systems

Cons

- Not leveraging Google advanced security features
- Security features vary from different SSO vendors
- Third-party SSO software required
- Potential single point of failure



Exam Tip:

- *Super admins are never redirected to SSO when they access admin.google.com*
- *Have a look at how SSO process works in GCP.*

1.1 Diagnostic Question 01 Discussion

Cymbal Bank has acquired a non-banking financial company (NBFC). This NBFC uses Active Directory as their central directory on an on-premises Windows Server. You have been tasked with migrating all the NBFC users and employee information to Cloud Identity.

What should you do?

A. Run Microsoft System Center Configuration Manager (SCCM) on a Compute Engine instance. Leave the channel unencrypted because you are in a secure Google Cloud environment. Deploy Google Cloud Directory Sync on the Compute Engine instance. Connect to the on-premises Windows Server environment from the instance, and migrate users to Cloud Identity.

B. Run Configuration Manager on a Compute Engine instance. Copy the resulting configuration file from this machine onto a new Compute Engine instance to keep the production environment separate from the staging environment. Leave the channel unencrypted because you are in a secure Google Cloud environment. Deploy Google Cloud Directory Sync on this new instance. Connect to the on-premises Windows Server environment from the new instance, and migrate users to Cloud Identity.

C. Use Cloud VPN to connect the on-premises network to your Google Cloud environment. Select an on-premises domain-joined Windows Server. On the domain-joined Windows Server, run Configuration Manager and Google Cloud Directory Sync. Use Cloud VPN's encrypted channel to transfer users from the on-premises Active Directory to Cloud Identity.

D. Select an on-premises domain-joined Windows Server. Run Configuration Manager on the domain-joined Windows Server, and copy the resulting configuration file to a Compute Engine instance. Run Google Cloud Directory Sync on the Compute Engine instance over the internet, and use Cloud VPN to sync users from the on-premises Active Directory to Cloud Identity.

1.1 Diagnostic Question 01 Discussion

Cymbal Bank has acquired a non-banking financial company (NBFC). This NBFC uses Active Directory as their central directory on an on-premises Windows Server. You have been tasked with migrating all the NBFC users and employee information to Cloud Identity.

What should you do?

A. Run Microsoft System Center Configuration Manager (SCCM) on a Compute Engine instance. Leave the channel unencrypted because you are in a secure Google Cloud environment. Deploy Google Cloud Directory Sync on the Compute Engine instance. Connect to the on-premises Windows Server environment from the instance, and migrate users to Cloud Identity.

B. Run Configuration Manager on a Compute Engine instance. Copy the resulting configuration file from this machine onto a new Compute Engine instance to keep the production environment separate from the staging environment. Leave the channel unencrypted because you are in a secure Google Cloud environment. Deploy Google Cloud Directory Sync on this new instance. Connect to the on-premises Windows Server environment from the new instance, and migrate users to Cloud Identity.

C. Use Cloud VPN to connect the on-premises network to your Google Cloud environment. Select an on-premises domain-joined Windows Server. On the domain-joined Windows Server, run Configuration Manager and Google Cloud Directory Sync. Use Cloud VPN's encrypted channel to transfer users from the on-premises Active Directory to Cloud Identity.

D. Select an on-premises domain-joined Windows Server. Run Configuration Manager on the domain-joined Windows Server, and copy the resulting configuration file to a Compute Engine instance. Run Google Cloud Directory Sync on the Compute Engine instance over the internet, and use Cloud VPN to sync users from the on-premises Active Directory to Cloud Identity.

1.1 Diagnostic Question 02 Discussion

Cymbal Bank has certain default permissions and access for their analyst, finance, and teller teams. These teams are organized into groups that have a set of role-based IAM permissions assigned to them. After a recent acquisition of a small bank, you find that the small bank directly assigns permissions to their employees in IAM. You have been tasked with applying Cymbal Bank's organizational structure to the small bank. Employees will need access to Google Cloud services.

What should you do?

A. Leave all user permissions as-is in the small bank's IAM. Use the Directory API in the Google Workspace Admin SDK to create Google Groups. Use a Python script to allocate users to the Google Groups.

B. Reset all user permissions in the small bank's IAM. Use Cloud Identity to create dynamic groups for each of the bank's teams. Use the dynamic groups' metadata field for team type to allocate users to their appropriate group with a Python script.

C. Reset all user permissions in the small bank's IAM. Use Cloud Identity to create the required Google Groups. Upgrade the Google Groups to Security Groups. Use a Python script to allocate users to the groups.

D. Reset all user permissions in the small bank's IAM. Use the Directory API in the Google Workspace Admin SDK to create Google Groups. Use a Python script to allocate users to the groups.

1.1 Diagnostic Question 02 Discussion

Cymbal Bank has certain default permissions and access for their analyst, finance, and teller teams. These teams are organized into groups that have a set of role-based IAM permissions assigned to them. After a recent acquisition of a small bank, you find that the small bank directly assigns permissions to their employees in IAM. You have been tasked with applying Cymbal Bank's organizational structure to the small bank. Employees will need access to Google Cloud services.

What should you do?

A. Leave all user permissions as-is in the small bank's IAM. Use the Directory API in the Google Workspace Admin SDK to create Google Groups. Use a Python script to allocate users to the Google Groups.

B. Reset all user permissions in the small bank's IAM. Use Cloud Identity to create dynamic groups for each of the bank's teams. Use the dynamic groups' metadata field for team type to allocate users to their appropriate group with a Python script.

C. Reset all user permissions in the small bank's IAM. Use Cloud Identity to create the required Google Groups. Upgrade the Google Groups to Security Groups. Use a Python script to allocate users to the groups.

D. Reset all user permissions in the small bank's IAM. Use the Directory API in the Google Workspace Admin SDK to create Google Groups. Use a Python script to allocate users to the groups.

Additional content

Additional content 1

[READING]

- Configuration of GCDS using Configuration Manager - it's good to have an overview of this process
- Google Workspace - Secure LDAP - what is a Secure LDAP Service?
- Patterns for authenticating corporate users in a hybrid environment
- Best practices for federating identities
- Super administrator account best practices
- Security best practices for administrator accounts
- Understanding roles
- Understanding IAM custom roles
- Creating and managing custom roles
- Overview of Google identity management
- Audit logs for service accounts - Just to get a feeling what kind of information is ingested into Cloud Logging
- Best practices for managing service account keys - lenghty, but super important!
- Creating and managing service accounts
- Manage service account insights
- Delegating domain-wide authority to the service account
- Enforce and monitor password requirements for users
- Managing SAML and OIDC providers

Additional content 2

- Deploy 2-Step Verification
- Adding multi-factor authentication to your web app
- Setting up OS Login with 2-step verification - important for secure logging to VMs via ssh
- Overview of IAM Conditions
- What is an IAM Policy?
- Understanding IAM Policies
- IAM Policy Troubleshooter - how to check why a user has access to a resource or doesn't have permission to call an API
- Using IAM securely - best practices for using IAM
- IAM details for GCS Buckets
- Creating and managing organizations
- IAM roles on Organization level
- Resource Hierarchy
- How to migrate projects - also between organizations
- Introduction to the Organization Policy Service (Org Policies are NOT the same as IAM Policies!)
- Understanding Constraints in Organization Policies
- Service Account Key rotation and best practices

Additional content 3

[VIDEOS]

- Security in the Cloud (vs on premises)
- 6 layers of Google Cloud data center security
  a. It also contains introduction to SCC (Security Command Center)
- great Cloud Identity (& more) demo from ~12:30 to ~28:00: Cloud OnAir: Unify identity, device, and app management with Cloud Identity
- How to start with GCP as an organization - a unique opportunity to see how to validate & attach a domain to GCP, create an organization and set up Cloud Identity in a recommended, secure way: Level Up From Zero Episode 1: Domains, Identity, and Admin Accounts
- How to design resource hierarchy in GCP: Level Up From Zero Episode 2: Organizations & the Resource Hierarchy
- Creating IAM Policies (= granting permissions) at different levels of a resource hierarchy in a recommended, secure-oriented manner: Level Up From Zero Episode 3: Identity & Access Management
- Advanced IAM: Hacks, tips, and tricks for policy management
- How to secure your Service Accounts
- Service Account keys and impersonation
- Super-important to know how to use and impersonate Service Accounts: Service Accounts in action
- Organization Policy Service example: How to limit public IPs on Google Cloud

Additional content 4

[PODCASTS]

- Zero Trust: Fast Forward from 2010 to 2021
- (RECOMMENDED; super helpful in understand identities and privilege concepts in GCP vs on-premises): Impersonating Service Accounts in GCP and Beyond
- Cloud Migrations: Security Perspectives from The Field
- Preparing for Cloud Migrations from a CISO Perspective, Part 1

[DEEP DIVES]

- Customer-Supplied Encryption Keys overview.
- Google infrastructure security design overview.
- High-level GCP security overview.

Security-related glossary

- SOC: Security Operations Center
- NOC: Network Operations Center
- CISO: Chief Information Security Officer
- **Toil**: *“the kind of work tied to running a production service that tends to be manual, repetitive, automatable, tactical, devoid of enduring value, and that scales linearly as a service grows.”.* **Alternative definition***: “If your service remains in the same state after you have finished a task, the task was probably toil.”*
- DevSecOps - Security part of DevOps team
- IDS: Intrusion Detection System
- IPS: Intrusion Prevention System
- SIEM: security information & event management
- NTA: network traffic analytics
- Shifting left: The process of checking for vulnerabilities earlier in development
- Forensics is the application of science to criminal and civil laws. It is a proven approach for gathering and processing evidence at a crime scene.
- IP: Intellectual Property
- TTP: Tactics, Techniques and Procedures
- IOC - Indicator Of Compromise

Make sure to…

Enjoy the journey as much as the destination!