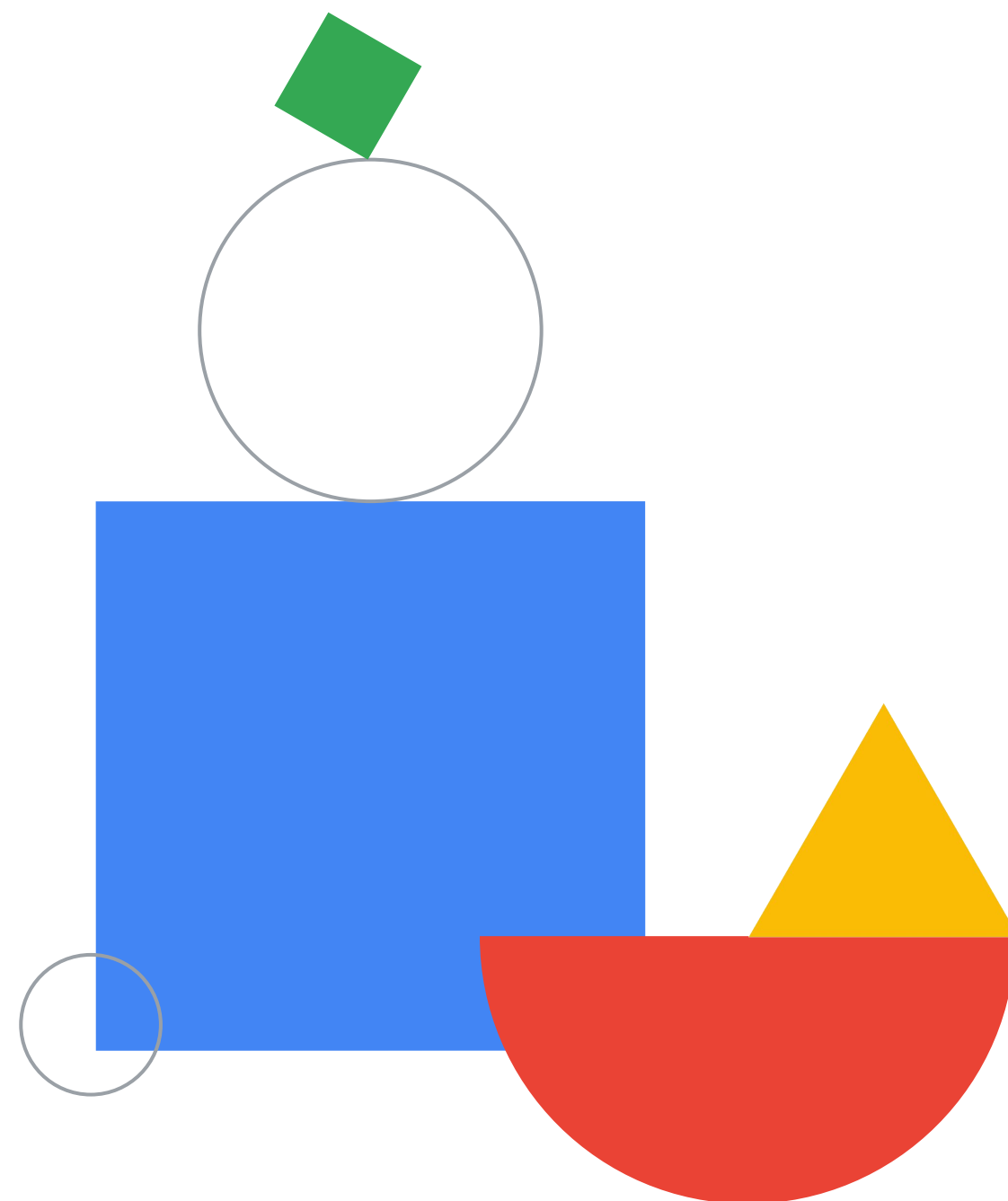


Preparing for Your Professional Cloud Architect Journey

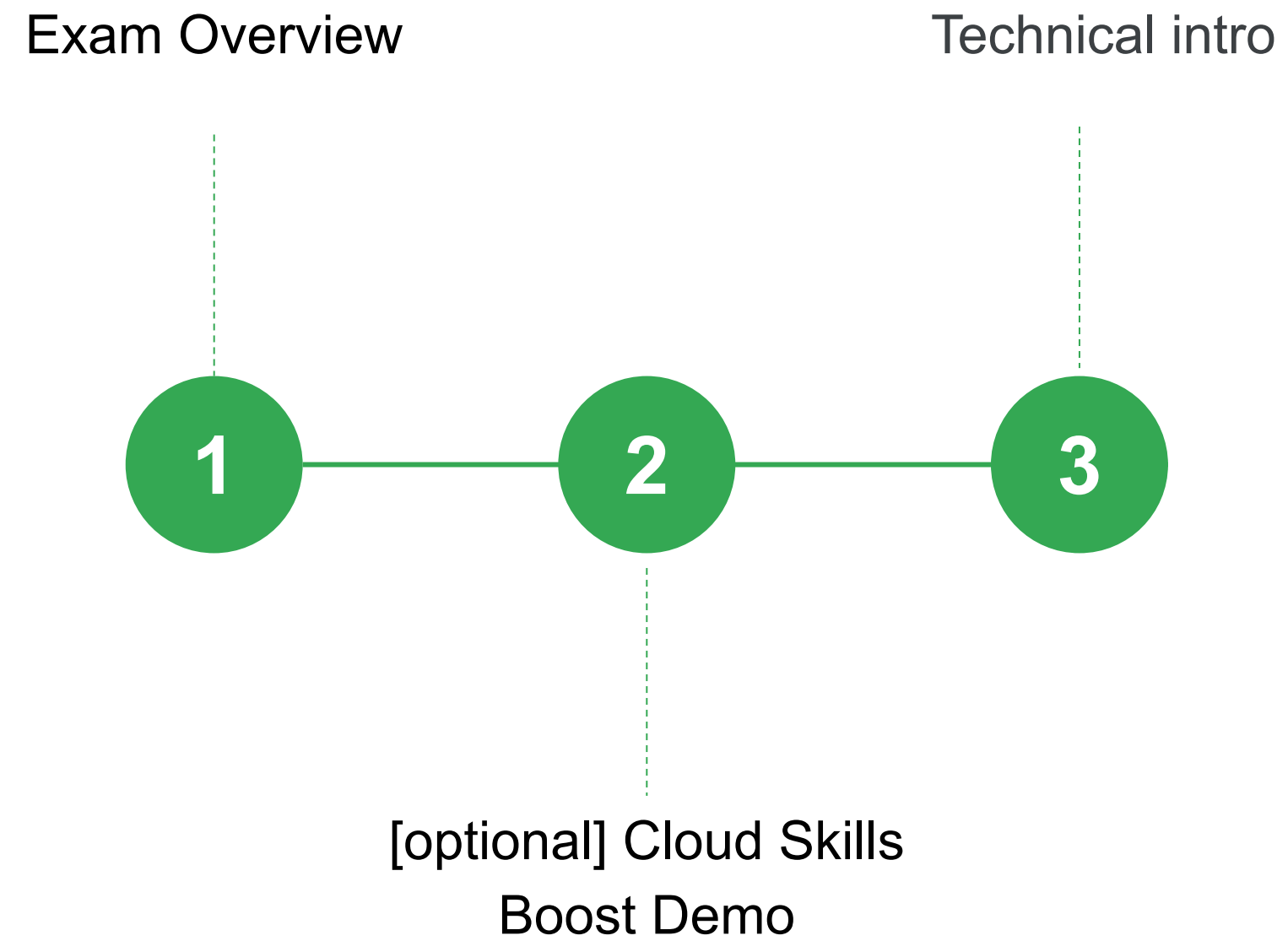
Introduction



Who am I and what's
my role here?



Week 1 topics



Professional Cloud Architect



A Google Cloud Certified Professional Cloud Architect is able to leverage Google Cloud technologies to design, develop, and manage robust, secure, scalable, efficient, cost-effective, highly available, and flexible solutions that drive business objectives. The Professional Cloud Architect should be proficient in enterprise cloud strategy, solution design, workload migration approaches, deployment and orchestration, optimization, and **architectural best practices**. This individual is also experienced with common open-source technologies and software development methodologies for designing multi-tiered distributed applications across legacy, multi-cloud, or hybrid environments.

PCA Exam High-level Overview

- 80h-150h+ to prepare. Consistency is the key!
- PCA = “A mile wide and an inch deep” (at least in most cases)
- Exam structure:
 - 50-60 questions / 2h for the exam. English language only (no additional time for non-native speakers).
 - Multiple-choice theoretical questions, but asking about “real-world” challenges. Most with a single correct answer, some with more (you will know how many). Get a feeling by doing a [sample test](#).
 - In a lot of cases, you will need to choose BEST answer from 2-4 which are technically correct.
 - ~25% (~12-15) of questions are based on Case Studies.
 - NO labs, NO hands-on exercises on the exam (but essential when preparing!).
- It's not clear what is the percentage needed to pass (aim at 85+% accuracy for practise questions).
 - but don't leave any questions unanswered (no negative points).
- 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)

Don't have your own exam strategy? Use mine:

- When looking at a question, use elimination technique (get rid of the “obvious” wrong answers).
- Handle the easier questions first (aim at ~1.5 min per question) and mark the rest for review.

Exam question example

Notice the business context!

Your company wants to track whether someone is present in a meeting room reserved for a scheduled meeting. There are 1000 meeting rooms across 5 offices on 3 continents. Each room is equipped with a motion sensor that reports its status every second. You want to support the data ingestion needs of this sensor network. The receiving infrastructure needs to account for the possibility that the devices may have inconsistent connectivity.

Which solution would you choose?

- A. Have each device create a persistent connection to a Compute Engine instance and write messages to a custom application.
- B. Have devices poll for connectivity to Cloud SQL and insert the latest messages on a regular interval to a device specific table.
- C. Have devices poll for connectivity to Pub/Sub and publish the latest messages on a regular interval to a shared topic for all devices.
- D. Have devices create a persistent connection to an App Engine application fronted by Cloud Endpoints, which ingest messages and write them to Datastore.



Case studies

- ~25% of the questions (~12-15) on the certification exam will refer to a case study.
- 4 case studies available for analysis **before** the exam (NO NEW CASE CASE STUDIES ON THE EXAM!):
 - [Altostrat Media](#)
 - [Cymbal Retail](#)
 - [EHR Healthcare](#) - the only “old” case study
 - [KnightMotives Automotive](#)
- You will have access to a full case study during the exam (but it’s not the best time to start analysis...)
- We shall have a **high-level** discussion (with sample questions) on each of the case studies during our meetings (weeks 3-6)

Altostrat Media Case Study

Company Overview

Altostrat is a prominent player in the media industry, with an extensive collection of audio and video content that comprises podcasts, interviews, news broadcasts, and documentaries. Their success in delivering premium content to a diverse audience requires a content management system that can keep pace with the dynamic media landscape.

Solution Concept

Altostrat seeks to modernize its content management and user engagement strategies using Google Cloud's generative AI. They want a platform that empowers customers with personalized recommendations, natural language interactions, and seamless self-service support. Simultaneously, they want to drive revenue growth through dynamic pricing, targeted marketing, and personalized product suggestions.

The seamless integration of AI-powered tools into their existing Google Cloud environment will enable Altostrat to efficiently manage their vast media library, enhance user experiences, and unlock new revenue streams. Google Cloud's generative AI will solidify their leadership in the media industry.

Case study - sample question

For this question, refer to the [EHR Healthcare case study](#).

In the past, configuration errors put public IP addresses on backend servers that should not have been accessible from the Internet. You need to ensure that no one can put external IP addresses on backend Compute Engine instances and that external IP addresses can only be configured on frontend Compute Engine instances. What should you do?

- A. Revoke the compute.networkAdmin role from all users in the project with front end instances.
- B. Create an Identity and Access Management (IAM) policy that maps the IT staff to the compute.networkAdmin role for the organization.
- C. Create a custom Identity and Access Management (IAM) role named GCE_FRONTEND with the compute.addresses.create permission.
- D. Create an Organizational Policy with a constraint to allow external IP addresses only on the frontend Compute Engine instances.

If you happen to fail (hope not!), you shall get a report

Exam Result: Fail

Google Cloud Certification has received your exam result. Although you did not achieve a passing score on the Google Cloud Certified - Professional Cloud Security Engineer exam, we hope you will try again after gaining additional experience or training.

The table below gives information about the composition of the exam and your performance on each of the exam sections. The “approximate % scored questions” column indicates the percentage of the total scored exam questions that came from the section. **"Meets"** indicates that you have met the competency level for skills tested in that section. **"Borderline"** suggests that you have some but not all of the skills tested in that section and additional preparation would be helpful. **"Does not meet"** indicates that you do not yet have the skills tested in that section. This information is intended to be general feedback on your strengths and weaknesses. We encourage you to review all sections before attempting the exam again.

**Please note: score report is only available for exams taken after February 26, 2024.*

Sections	Approximate % Scored Questions	Section Performance
Section 1: Configuring access within a cloud solution environment	27.0%	Meets
Section 2: Configuring perimeter and boundary security	21.0%	Does Not Meet
Section 3: Ensuring data protection	20.0%	Does Not Meet
Section 4: Managing operations within a cloud solution environment	22.0%	Does Not Meet
Section 5: Supporting compliance requirements	10.0%	Meets

New exam version

live Oct 30th 2025

*"The upcoming version of the Professional Cloud Architect exam highlights the [Google Cloud Well-Architected Framework](#) as a key requirement for this role. The framework's pillars (operational excellence, security, reliability, performance optimization, cost optimization, and sustainability) are implicitly and explicitly woven throughout the exam objectives. **The exam also includes new case studies** that allow cloud architects to demonstrate their ability to use Google Cloud's generative AI technology to realize business value."*

Tip: 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.

90-day, \$300 Free Trial

Thanks for signing up. Your free trial includes \$300 in credit to spend over the next 90 days. If you run out of credit, don't worry — you won't be billed unless you [turn on automatic billing](#).

GOT IT

* 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.

Google Skills Demo

Let's start the technical part!

Opex vs Capex

- [CAPEX Vs OPEX - Fundamentals of Cloud #shorts - YouTube](#)
- **Capex:**
 - Traditional, “on-premises” approach. Eg. build a datacenter, but hardware and licenses, amortize over time (years)
 - An organization purchases computing capacity upfront and uses it over time.
 - Easy, but usually not flexible.
- **Opex:**
 - Cloud-native approach. Eg. spin up a storage service and use it as needed (decommission after few days; resize when needed; stop outside of business hours)
 - Based on pay-as-you-go approach, with no upfront payments. Resources and services are available on-demand, often billed based on per-second usage fees.
 - Harder to predict costs (and spend fluctuates each month), but you gain a ton of flexibility (has effects on sizing, time to deliver etc).

***Exam Tip:** Despite Opex is the cloud-native approach, there are ways to cost-optimize workloads by committing to long-term (1-3 years) usage, this leaning towards Capex model a bit.*

SQL vs noSQL

SQL (aka ‘Relational’)	NoSQL (aka ‘Non-relational’)
“traditional” table-based RDBMSes	key-value, wide column, document
Strongly typed, fixed schemas	Dynamic schemas
Almost all ACID-compliant	Mostly BASE
Considerable percentage of logic can be done in database	Most of logic needs to be offloaded to application layer
Default choice for most monoliths	Suitable for some microservices
performance capped at some point (vertical scaling only, plus sharding, offloading read-only etc)	Processing nodes often separate from storage nodes (if network is fast enough)
In GCP: Cloud SQL, Cloud Spanner Outside of GCP: MySQL, Oracle, PostgreSQL, Microsoft SQL Server.	In GCP: Firestore, Bigtable Outside of GCP: MongoDB, Redis, Cassandra, HBase, CouchDB

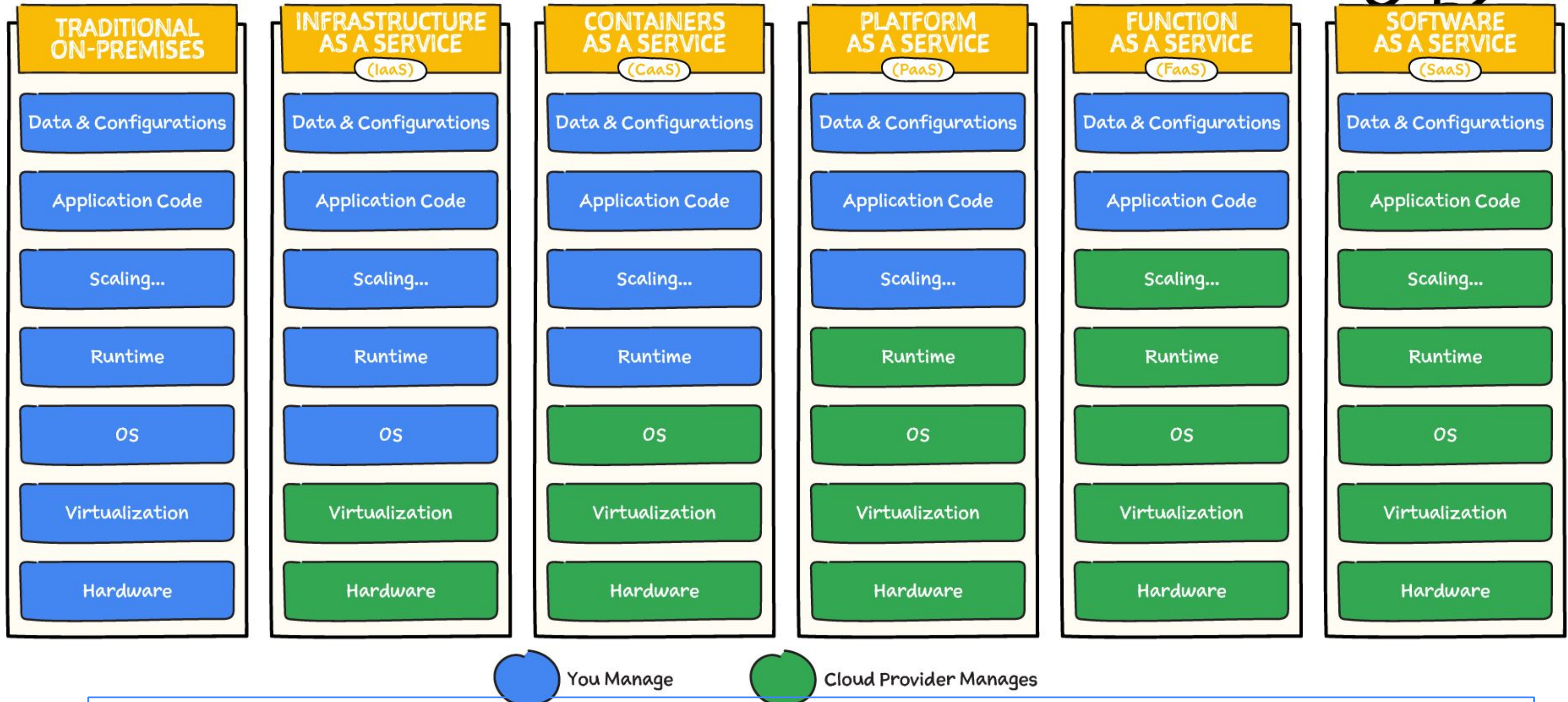
OLTP vs OLAP

OL Transactional P	OL Analytical P
For processing data in transaction-oriented apps	Multi-dimensional, analytical queries used in BI, reporting, data mining etc
Large amounts of transactions	Large volume of data
A mix of Inserts, Updates, Deletes on individual records.	Loading data from source + selects. Optimized for high throughput reads on large number of records
Tables are normalized	Tables are not normalized
ACID & (mostly) SQL	SQL (sometimes NoSQL)
Cloud SQL, Cloud Spanner	BigQuery

***Exam Tip:** [Here](#) you'll find a GREAT Decision tree for database choices on AWS, Microsoft Azure, Google Cloud Platform, and cloud-agnostic*



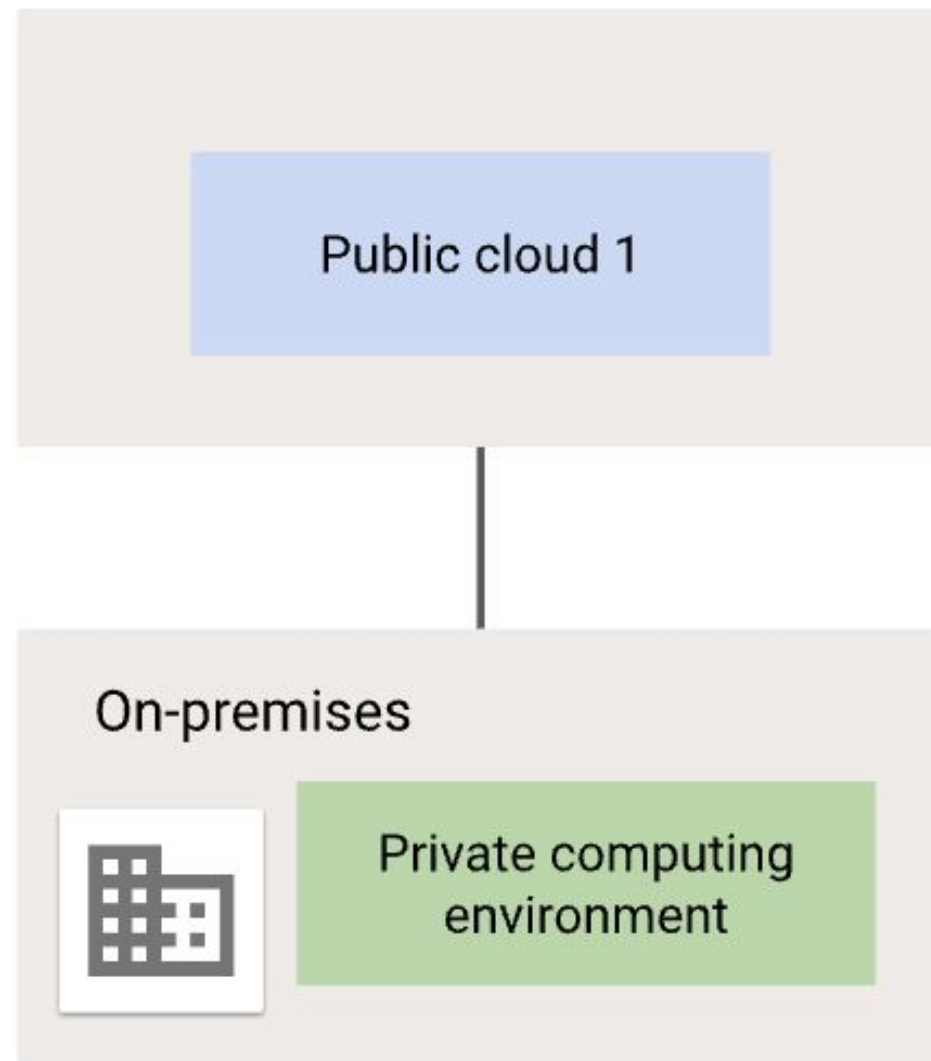
Wait... what is Cloud again?



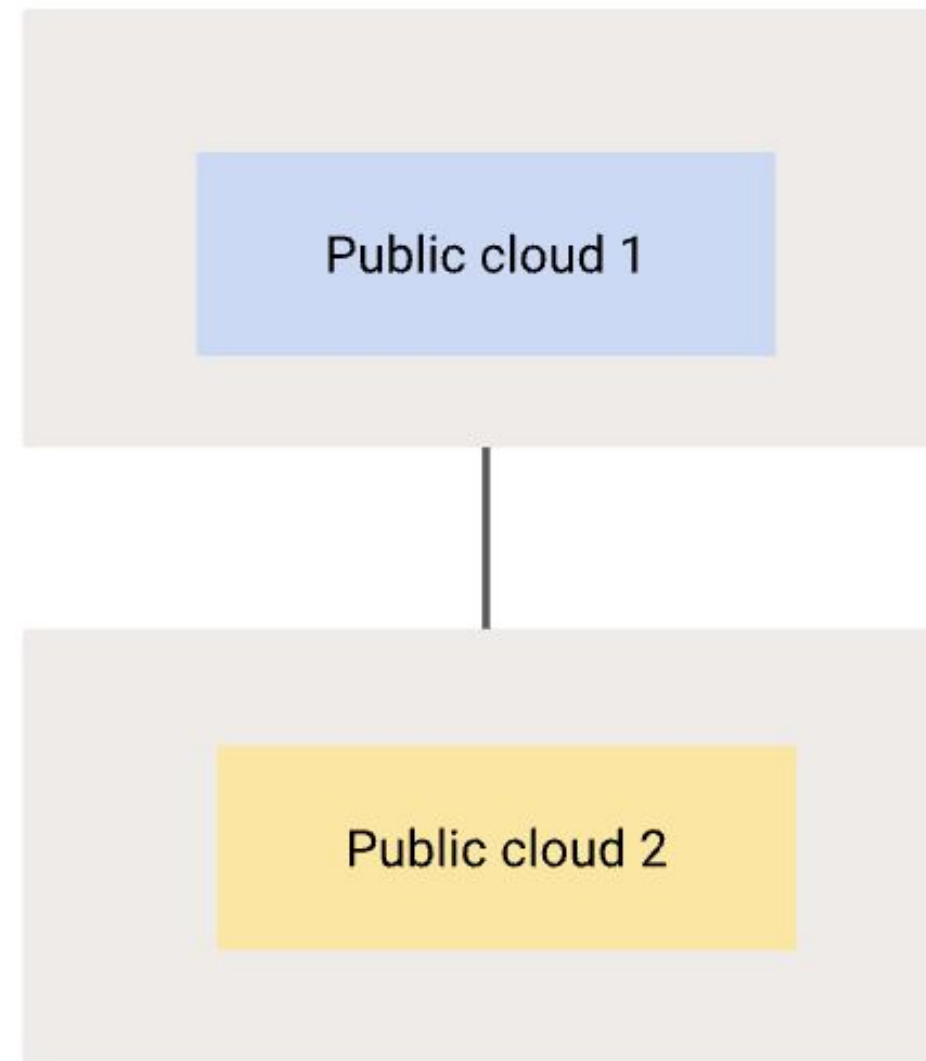
Exam Tip: Get swift in choosing an optimal approach based on business and technical requirements..

Hybrid vs multicloud

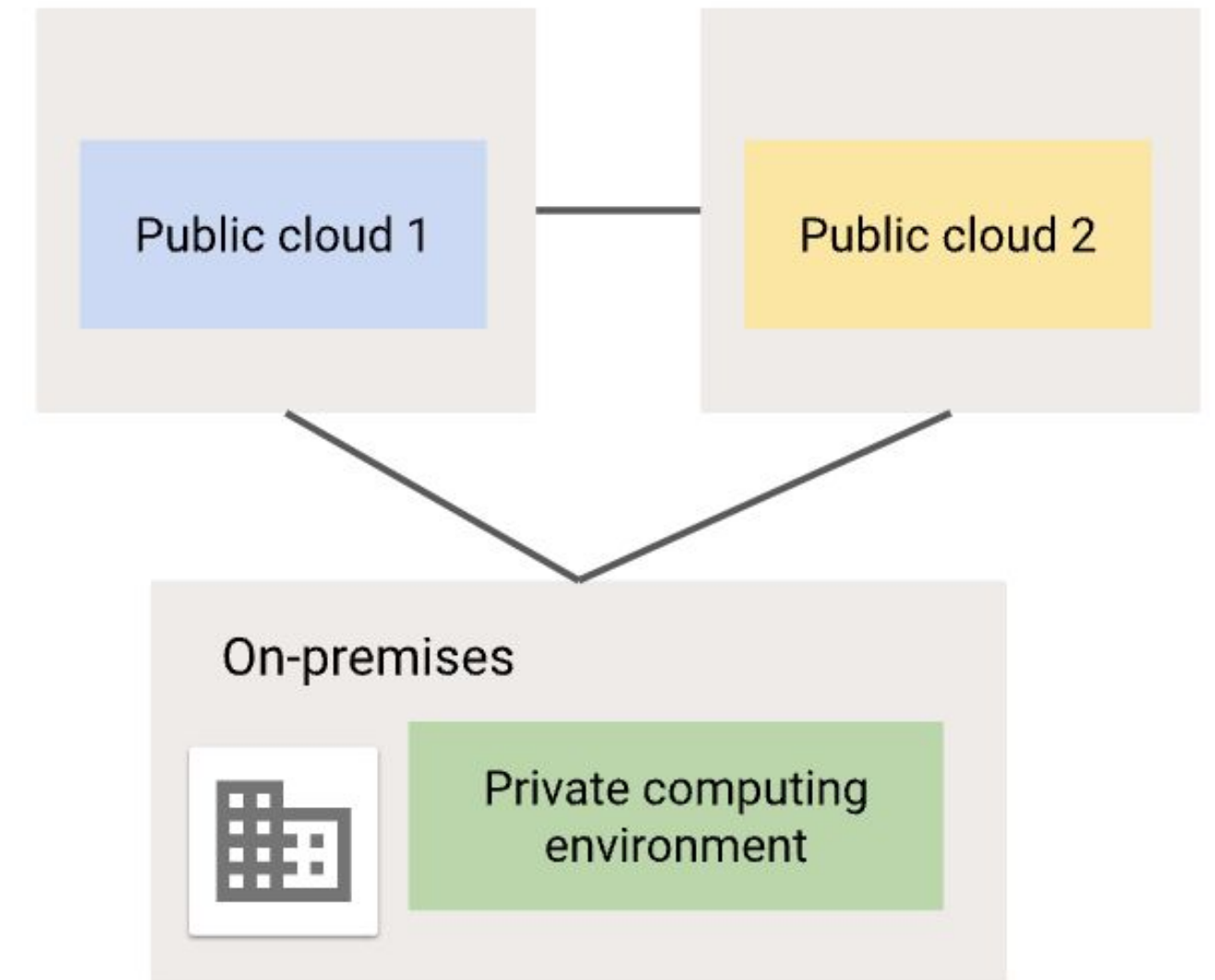
Hybrid architecture



Multicloud architecture

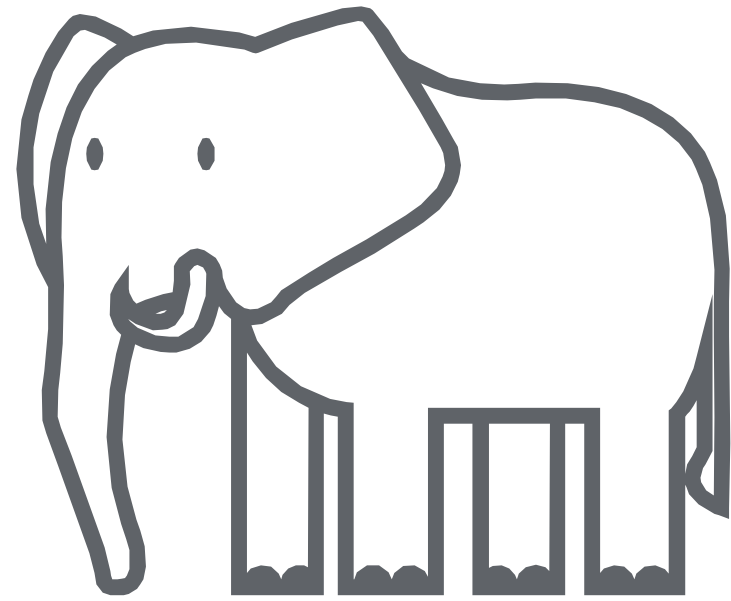


Hybrid and multicloud architecture

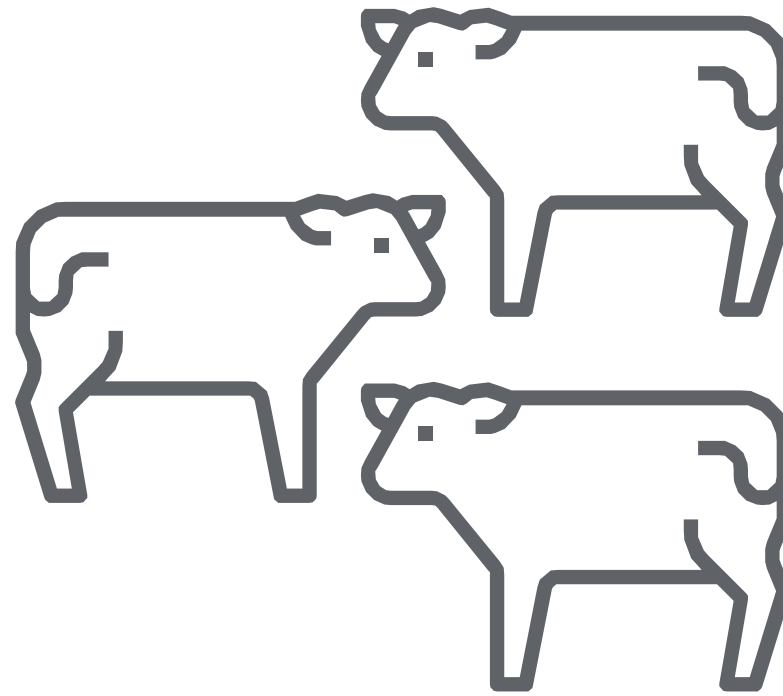


Exam Tip: Have a look at the most common hybrid and multicloud patterns.

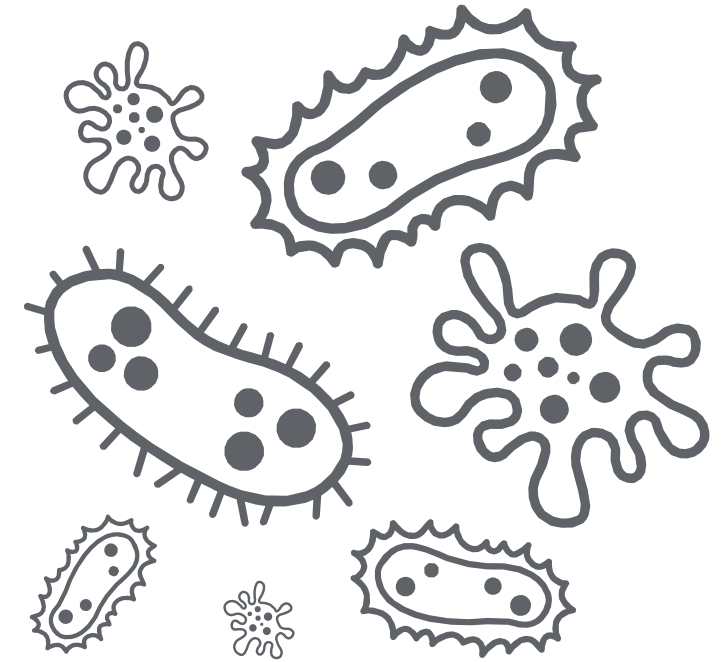
Microservices - evolution



Mainframe

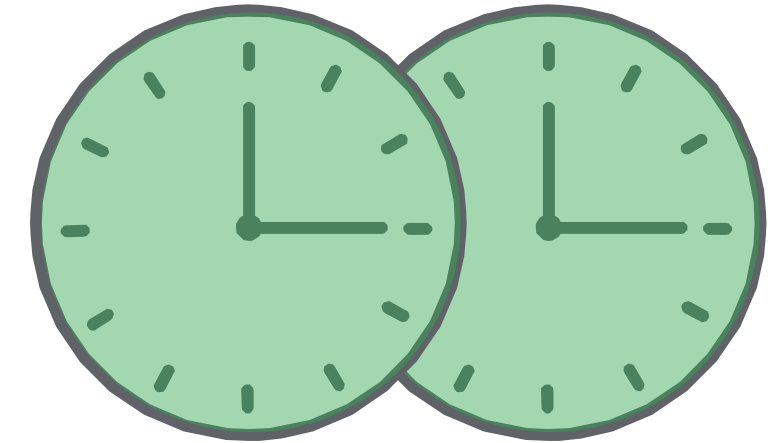
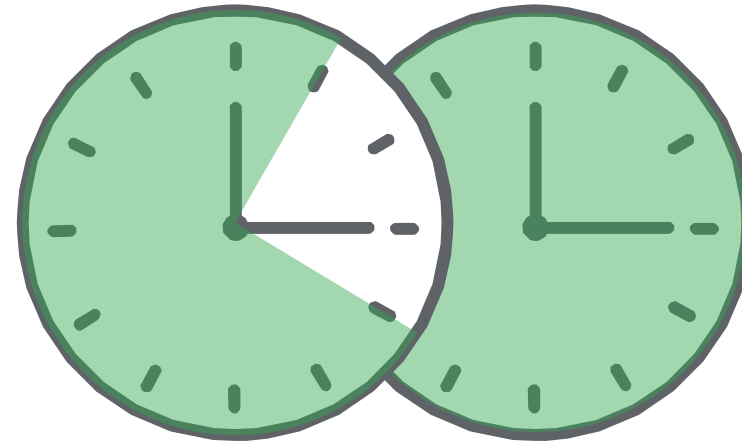
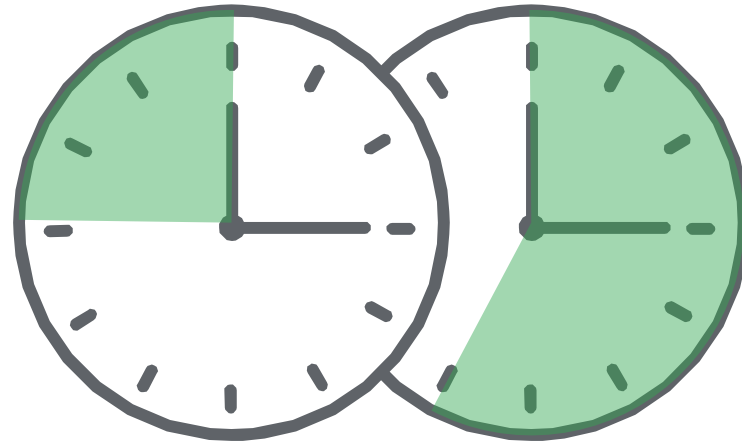
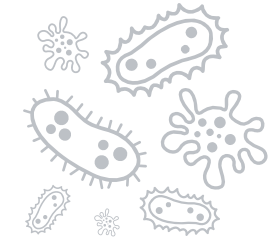
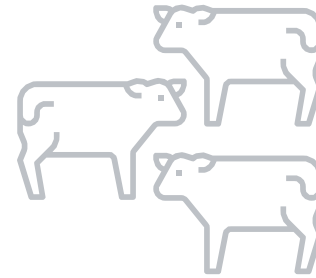
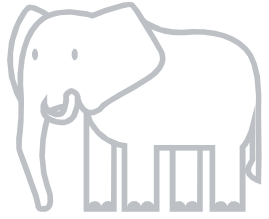


Monolith



Microservices

Microservices - evolution



Business Hours

Maintenance Windows

24/7

Microservices - advantages

- The microservices can be **independently tested and deployed**. The **smaller** the unit of deployment, the easier the deployment.
- They can be implemented in **different languages and frameworks**. For each microservice, you're free to choose the best technology for its particular use case.
- They can be managed by different teams. The boundary between microservices makes it easier to **dedicate a team to one or several microservices**.
- By moving to microservices, you **loosen the dependencies** between the teams. Each team has to care only about the APIs of the microservices they are dependent on. The team doesn't need to think about how those microservices are implemented, about their release cycles, and so on.
- You can more easily design for failure. By having clear boundaries between services, it's easier to determine what to do if a service is down.

Microservices - disadvantages

- Because a microservice-based app is a **network** of different services that often interact in ways that are not obvious, the overall **complexity** of the system tends to grow.
- Unlike the internals of a monolith, **microservices communicate over a network**. In some circumstances, this can be seen as a security concern. [Istio](#) solves this problem by automatically encrypting the traffic between microservices.
- It can be hard to achieve the same level of **performance** as with a monolithic approach because of **latencies** between services.
- The behavior of your system isn't caused by a single service, but by many of them and by their interactions. Because of this, **understanding how your system behaves in production (its observability) is harder**. Istio is a solution to this problem as well.

Diagnostic Question Discussion



You want to re-architect a monolithic application so that it follows a microservices model. You want to accomplish this efficiently while minimizing the impact of this change to the business.

- A. Deploy the application to Compute Engine and turn on autoscaling.
- B. Replace the application's features with appropriate microservices in phases.
- C. Refactor the monolithic application with appropriate microservices in a single effort and deploy it.
- D. Build a new application with the appropriate microservices separate from the monolith and replace it when it is complete

Which approach should you take?

Diagnostic Question Discussion



You want to re-architect a monolithic application so that it follows a microservices model. You want to accomplish this efficiently while minimizing the impact of this change to the business.

- A. Deploy the application to Compute Engine and turn on autoscaling.
- B. Replace the application's features with appropriate microservices in phases.**
- C. Refactor the monolithic application with appropriate microservices in a single effort and deploy it.
- D. Build a new application with the appropriate microservices separate from the monolith and replace it when it is complete

Which approach should you take?

When transitioning from a monolithic application to a microservices architecture, it is generally best to do it incrementally, rather than all at once. This allows you to break down the application into smaller, manageable pieces and make sure each piece is functioning correctly before moving on to the next. It minimizes risk, allows for easier troubleshooting, and reduces the impact on the business because you can gradually shift traffic to the new services as they are tested and deployed.

Controlling access

Authentication



Cloud Identity

Authorization



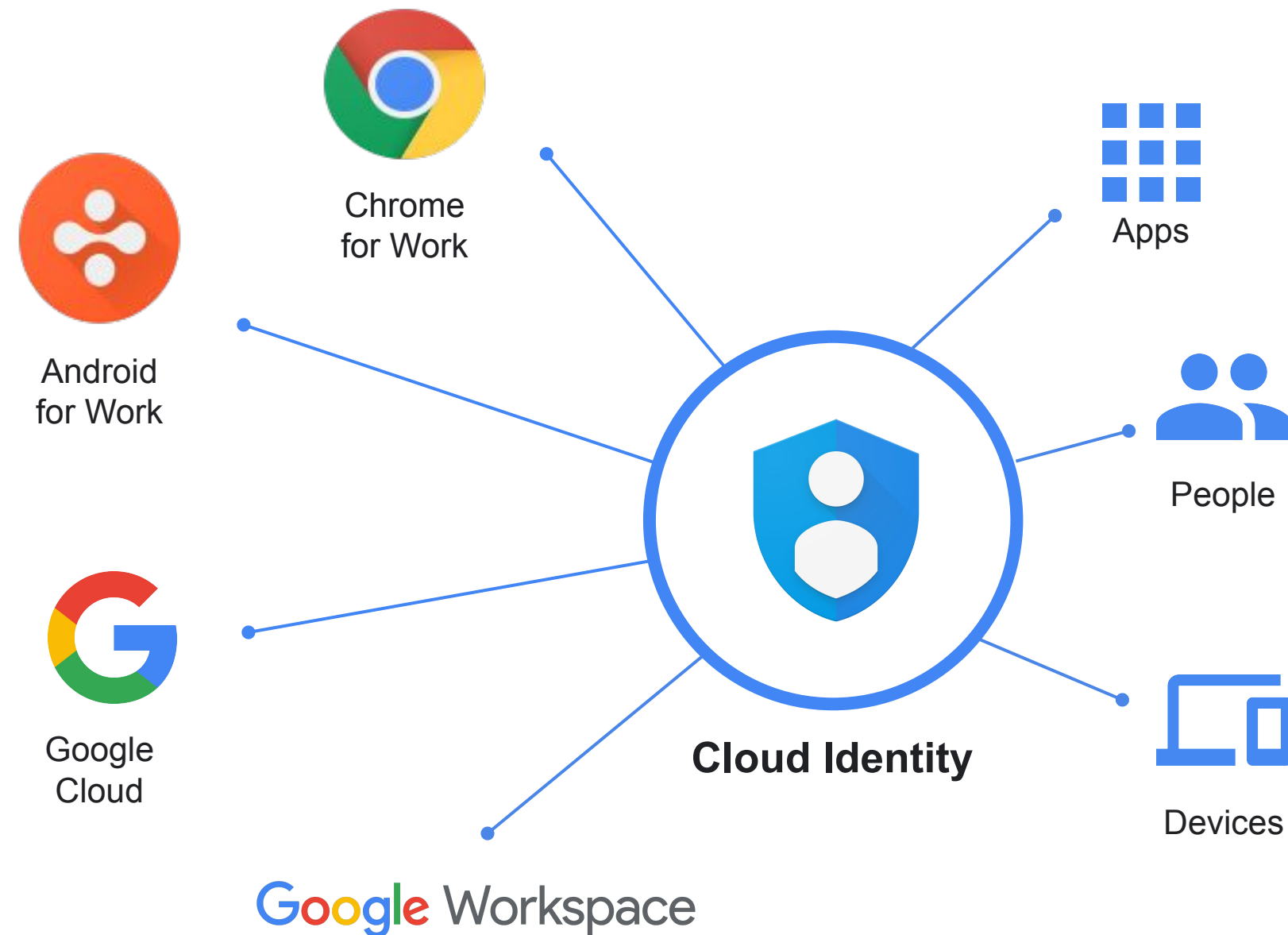
Cloud IAM

Auditing



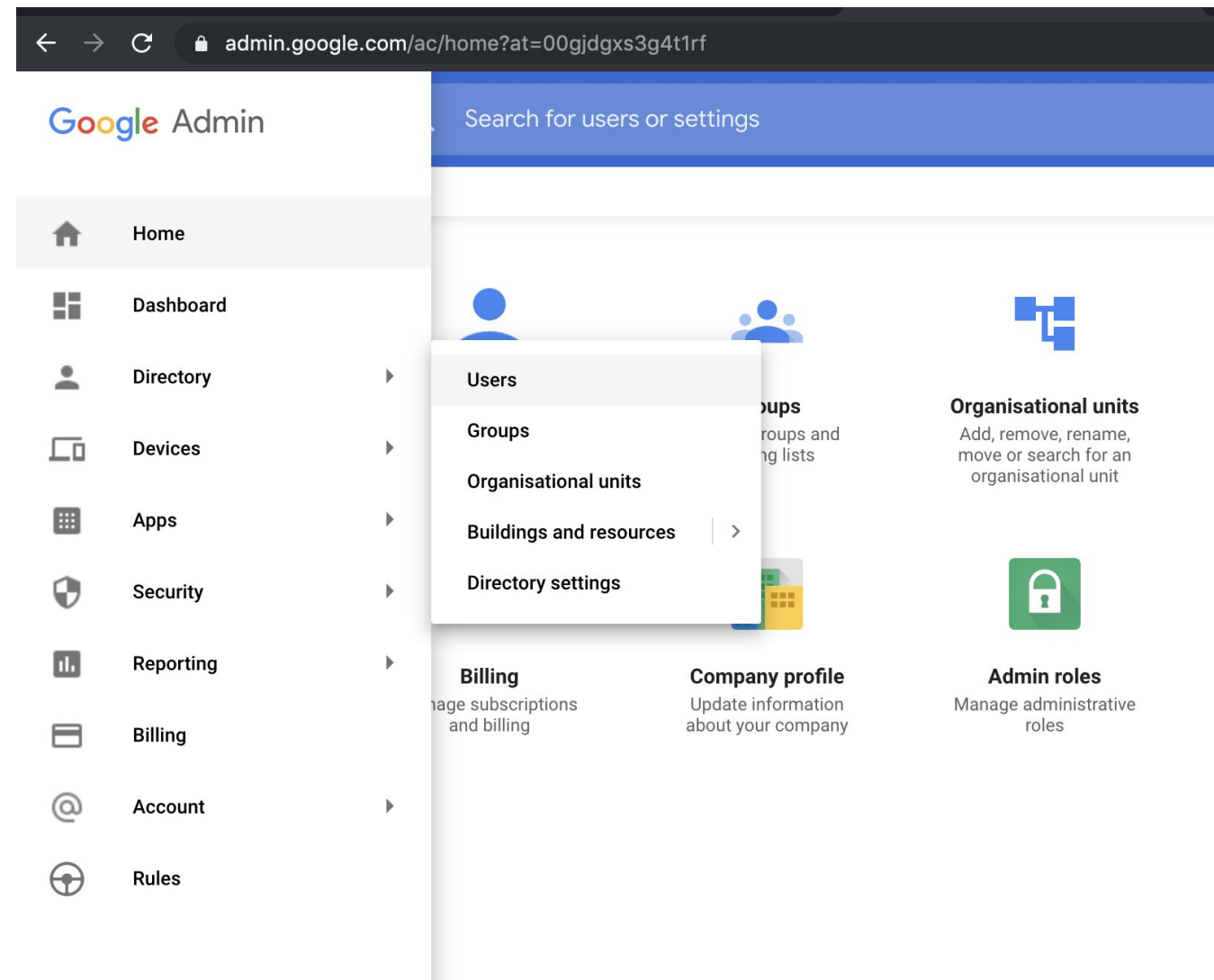
Cloud Operations
Audit Logging &
Reports API

What is Cloud Identity?



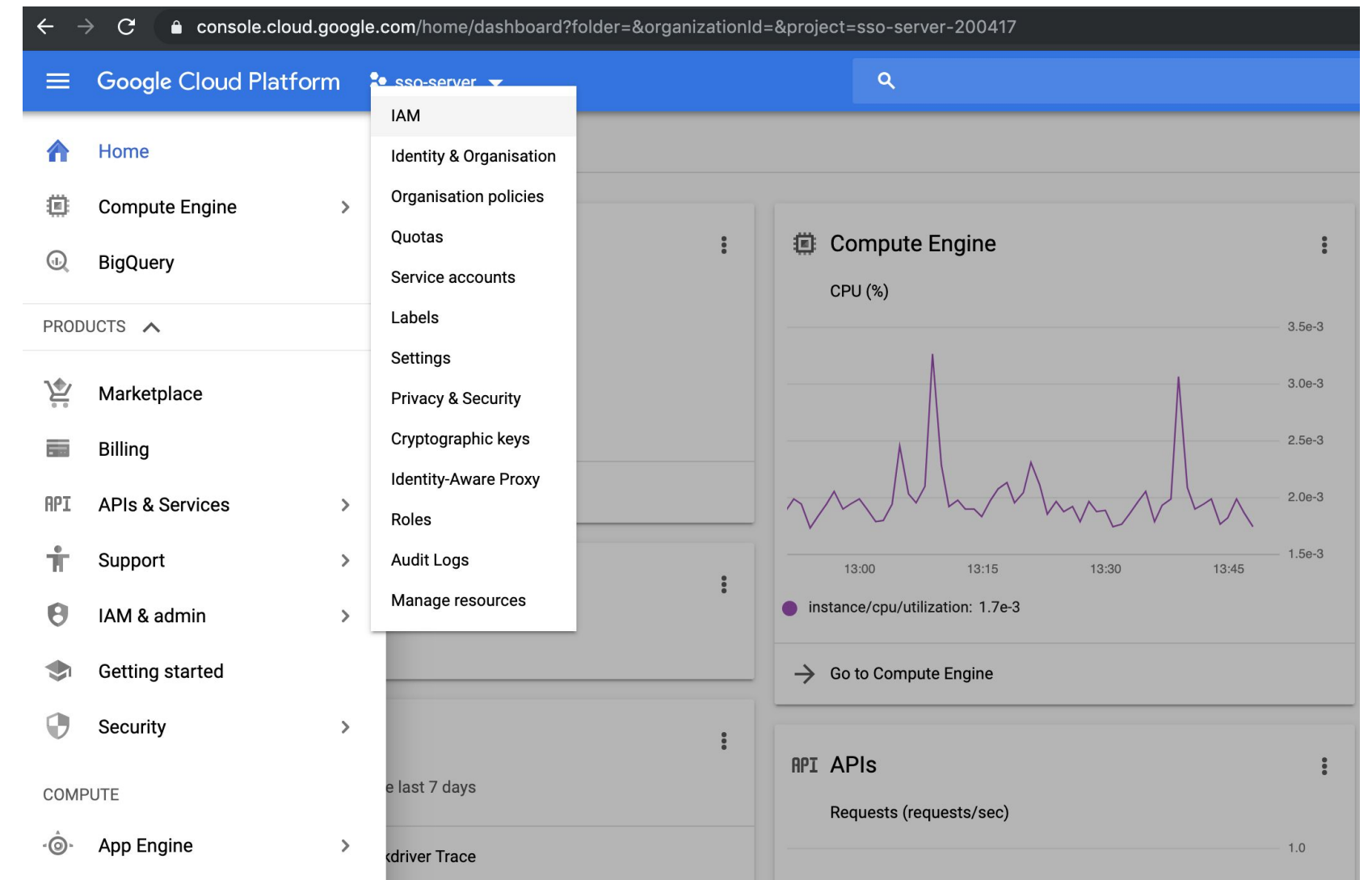
- Cloud Identity is an Identity as a Service (IDaaS) solution that **allows you to centrally manage users and groups** who can access Google Cloud and Google Workspace (formerly known as G Suite) resources
- It is the same identity service that powers Google Workspace and can also be used as IdP for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

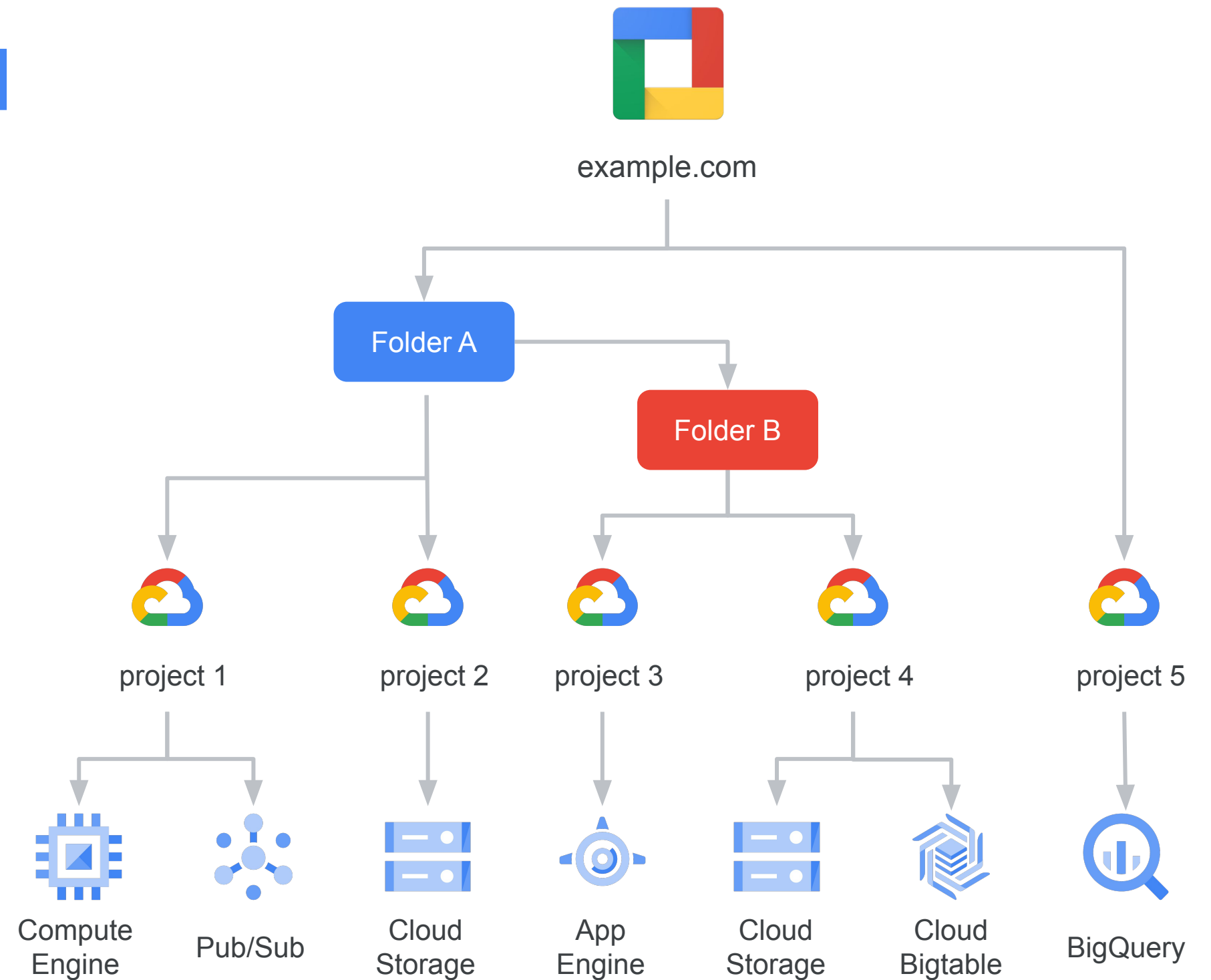
Exam Tips:

- 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](#).

Organization hierarchy helps organize access **control and** **policy for resources**

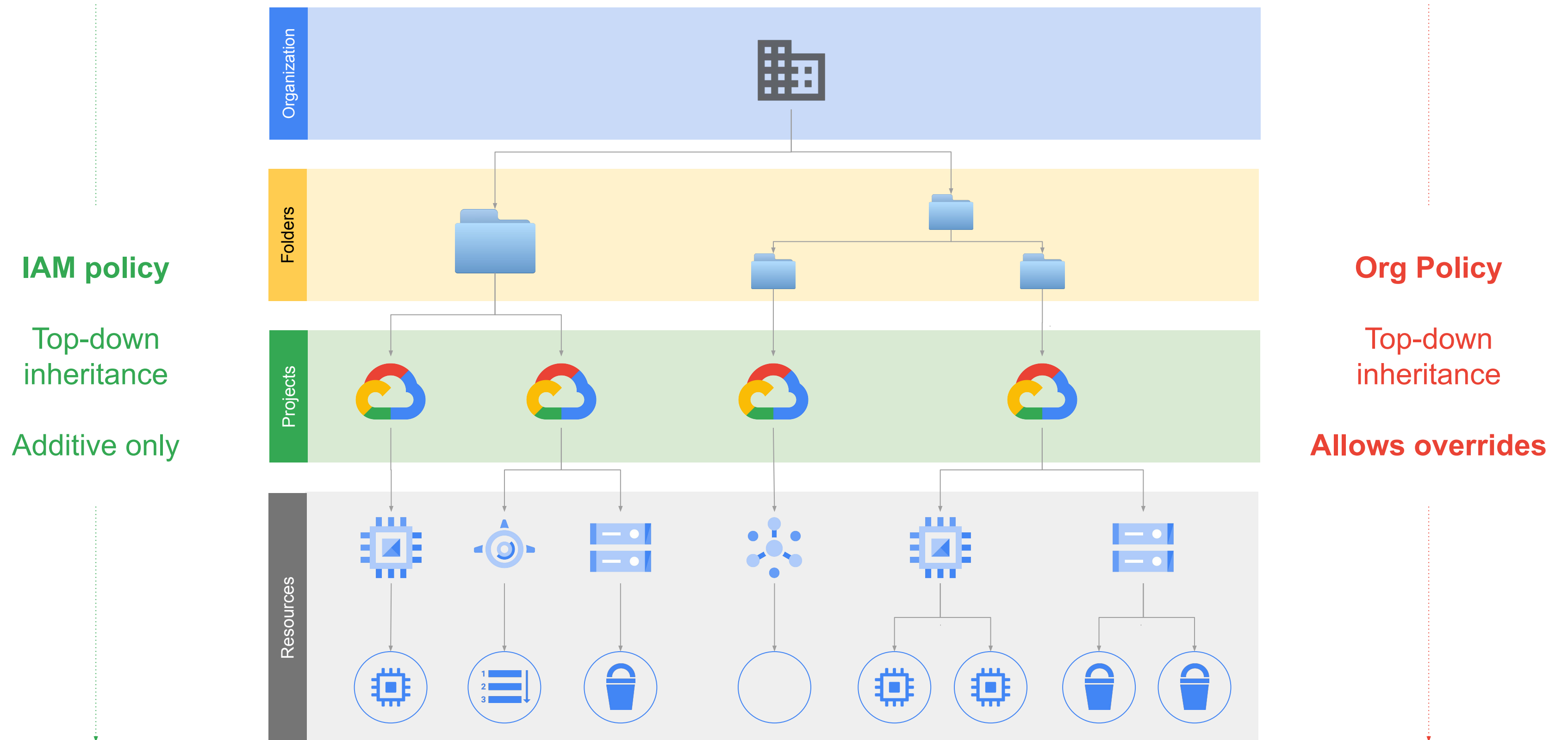
Folders provide for flexible hierarchy
of Projects

- Organization policy and access control can be bound at any level and flow downwards



[Know how to migrate projects across folders / orgs](#)

Hierarchy inheritance



Exam Tip: Watch out for IAM Deny policies!

IAM policy pattern example

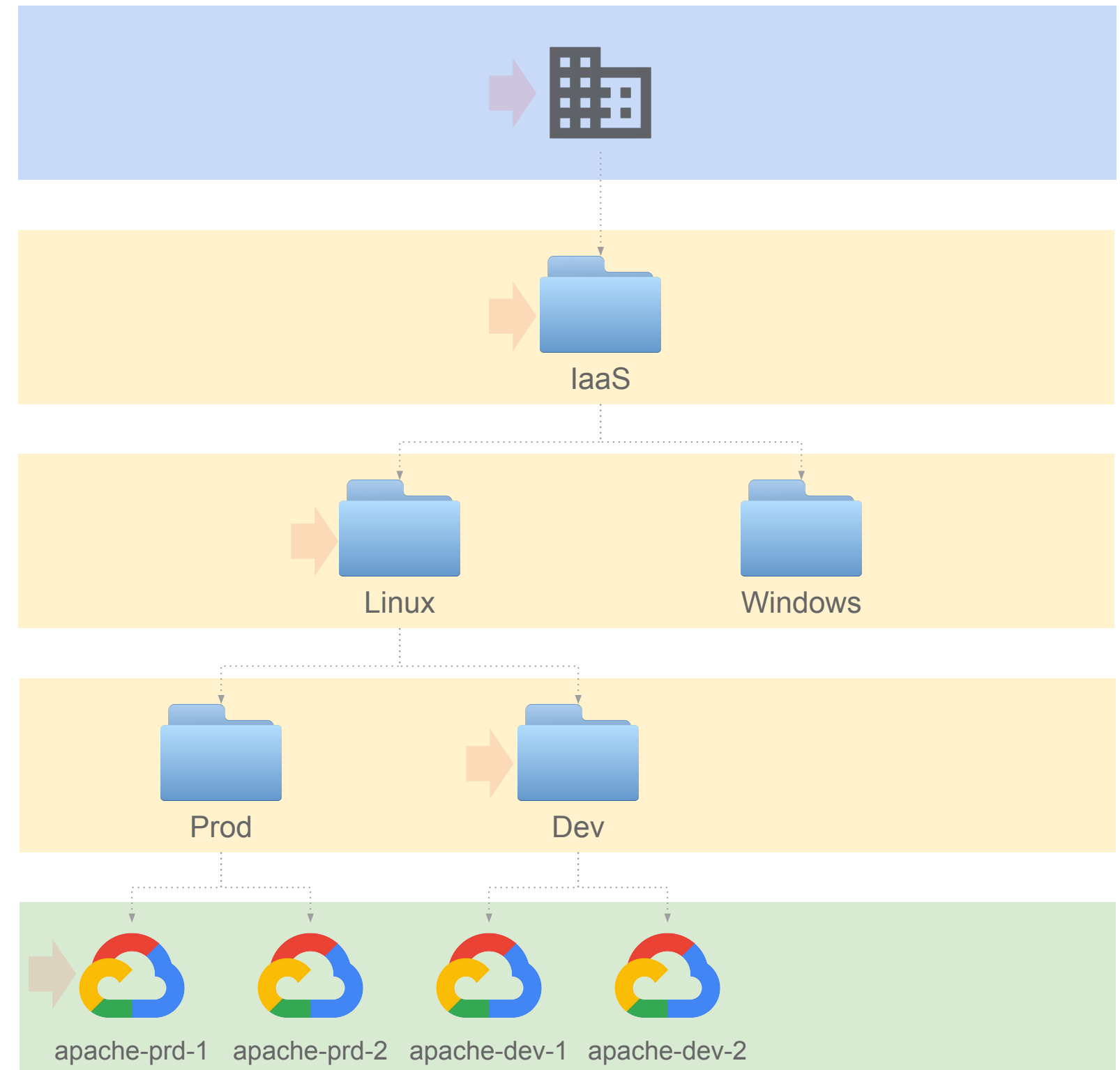
roles/browser → domain:example.org
all domain users should be able to see the hierarchy

roles/viewer → group:first-lvl-support@
support users should be able to view logs and VMs

roles/compute.admin → group:linux-os@
instance admins should manage resources

roles/logging.logViewer → group:app-team-1@
app admins should view logs in dev

roles/storage.admin → serviceAccount:app1@
ad-hoc permissions on project or single resource

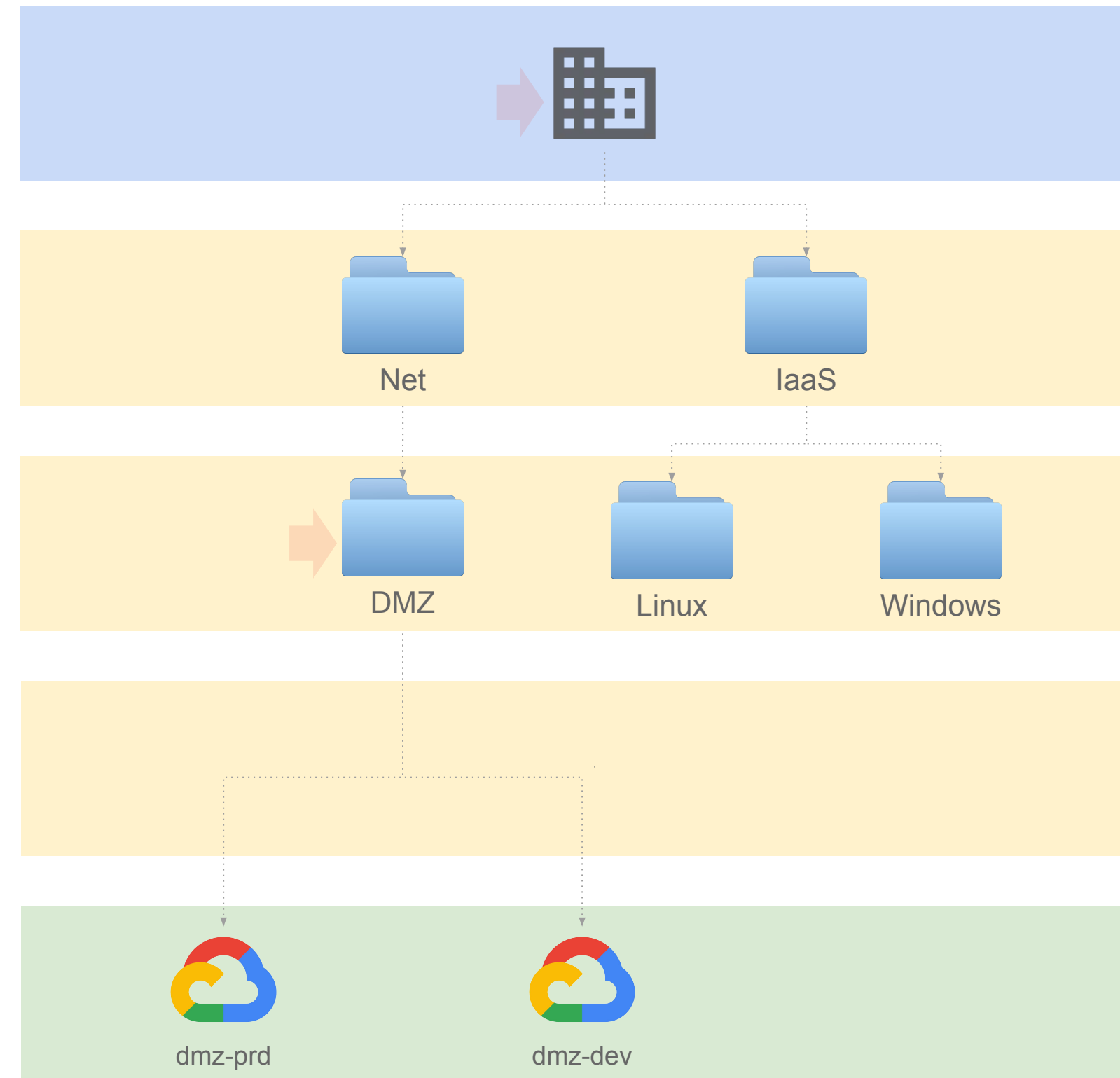


Organization policy pattern example

`constraints/compute.vmExternalIpAccess` → `false`
no VMs should be able to use external IPs

`constraints/compute.vmExternalIpAccess` → `true`
DMZ appliances should be able to use external IPs

inheritance



Most common Organization Policy constraints

Policy Constraint	Description
<i>compute.vmExternallpAccess</i>	A list of project/zone/instance names that are allowed to have external IP addresses and deny all others. Attempts to create any other VMs with an external IP address will fail.
<i>compute.trustedImageProjects</i>	A list of projects that contain trusted images that can be used as the basis for a VM and deny all others. Attempting to instantiate a VM with an image from another project is denied.
<i>compute.skipDefaultNetworkCreation</i>	Disables the creation of <u>default VPC</u> when creating a project. The default VPC uses auto mode subnetworks and includes default firewall rules which are often incompatible with production deployments.
<i>iam.disableServiceAccountKeyCreation</i>	This boolean constraint disables the creation of service account external keys where this constraint is set to `True`.
<i>gcp.resourceLocations</i>	This list constraint defines the set of locations where location-based GCP resources can be created. Policies for this constraint can specify multi-regions such as asia and europe, regions such as us-east1 or europe-west1, or individual zones such as europe-west1-b as allowed or denied locations.
<i>sql.restrictPublicIp</i>	This boolean constraint restricts configuring Public IP on Cloud SQL instances where this constraint is set to True. This constraint is not retroactive, Cloud SQL instances with existing Public IP access will still work even after this constraint is enforced. By default, Public IP access is allowed to Cloud SQL instances.
<i>sql.disableDefaultEncryptionCreation</i>	Restrict default Google-managed encryption on Cloud SQL instances
<i>compute.requireShieldedVm</i>	This boolean constraint, when set to True, requires that all new Compute Engine VM instances use Shielded disk images with Secure Boot, vTPM, and Integrity Monitoring options enabled. Secure Boot can be disabled after creation, if desired. Shielded VM features add verifiable integrity and exfiltration resistance to your VMs.

Organization Policy vs IAM Policy

Organization Policies	IAM Policies
Constraints that allow you to: <ul style="list-style-type: none">• Limit resource sharing based on domain.• Limit the usage of Identity and Access Management service accounts.• Restrict the physical location of newly created resources.	Effectively they're bindings which specify what access should be granted to principal on resources.
Focuses on “what” . Allows to set restrictions on specific resources to determine how they can be configured	Focuses on “who” . Let's you authorize who can take action on specific resources based on permissions
Can be set on different levels (org, folder, project), propagate down but lower-level policy overwrites a higher-level one.	Effective IAM Policy on each level is a SUM of all privileges (* with an exception of “ deny policies ”, which are not covered on the exam as of Q1 '23)
Both should be used as part of a security posture! It's NOT one or the other.	

Make sure to...

Enjoy the journey as much
as the destination!

