Google Cloud


# Professional Cloud Architect

Preparing for Professional Cloud Architect Journey for AWS Professionals

In the technical part, make sure to present a demo of resource hierarchy in cloud console.
Required: GCP organization with appropriate folder & project structure (including common projects for networking, logging etc)
TIME NEEDED: 40 mins to cover all. If cohort coordinator takes longer than 20 mins:

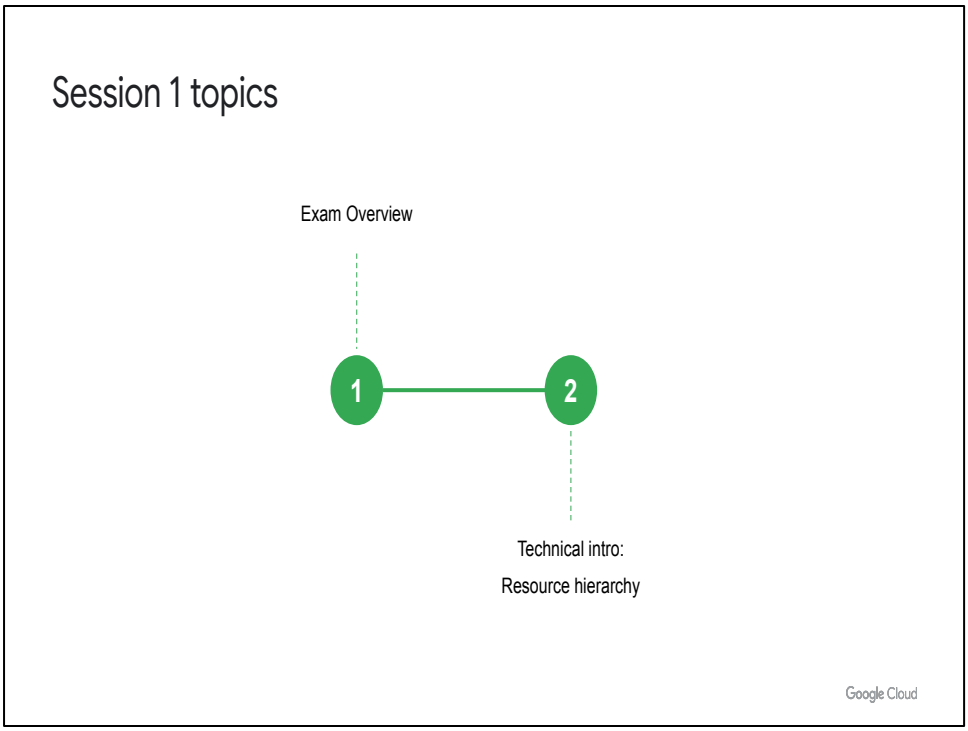
- If you have 35 mins -> just show resource hierarchy, but skip slides (including diagnostic questions);
- If you have 30 mins… no time for resource hierarchy demo at all?

# Who am I and what's my role here?

Google Cloud

TL;DR: say a few words about yourself (years of experience with GCP, delivering a number of cohorts, sharing the knowledge with others). Explain what's your role here:

- Teach only a bit, since the majority of the lectures will be handled by participants using one of the online platforms
- Explain the structure of the exam itself so that you can learn in the most efficient manner possible
- Solve some exam-like questions and teach what to focus on when reading and answering those
- Share different resources (quizzes, study cards etc) so that you [participants] can validate if they're progressing well and if they're ready to take the exam
- Emphasize most important topics which are tested the most
- Support when needed with different technical challenges you [participants] may have throughout the journey.




In this course, you'll learn more about the skills covered on the Professional Cloud Architect certification exam.
Each week we shall do a high-level overview of each of the modules of the exam as stated in the exam guide. We shall not focus on those a lot, but you should definitely go through each of those modules carefully [SHOW THOSE NOW: https://cloud.google.com/learn/certification/guides/professional-cloud-architect] so that you're aware of the exam requirements.

# 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.

Google Cloud

Overview of the exam

## 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.

Google Cloud

[ slide to be presented when explaining the exam structure ]

**C**

A is not correct because having a persistent connection does not handle the case where the device is disconnected.

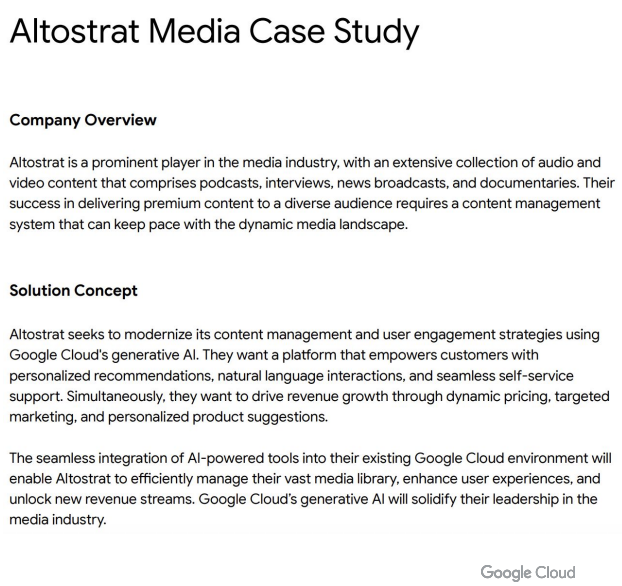
B is not correct because Cloud SQL is a regional, relational database and not the best fit for sensor data. Additionally, the frequency of the writes has the potential to exceed the supported number of concurrent connections.

C is correct because Pub/Sub can handle the frequency of this data, and consumers of the data can pull from the shared topic for further processing.

D is not correct because having a persistent connection does not handle the case where the device is disconnected.

## 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.

Google Cloud

[ slide to be presented when explaining the exam structure ]

TL;DR: Some exam questions (around 12 of them) will be based on so-called Case Studies. Those are documents describing business scenarios of fake companies which are designed to test yor understanding of the Google Cloud platform, as well as the ability to apply that knowledge to complex, real-world scenarios. They will mostly focus on meeting some specific business and technical requirement when deploying applications to GCP, or planning migrations of existing applications to GCP, all done using best practices, with security, availability, resiliency and others in mind..
There are 4 Case Studies in total (all those linked on this slide) and you will NOT get any other case studies on the exam. Which means you should get a solid understanding on those four and you should be good form the exam perspective. Starting from our 3rd meeting, we will briefly cover each of the case studies and collaborate on some potential solutions for them so that you feel more confident on the exam.

# 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.

Google Cloud

[ slide to be presented when explaining the exam structure ]
D

# Cloud Certification Exam Experience Comparison

| Feature | AWS (Amazon Web Services) | Azure (Microsoft Azure) | GCP (Google Cloud Platform) |
|---|---|---|---|
| Proctoring Platform | Pearson VUE, PSI (OnVUE software) | Pearson VUE, PSI, Certiport | Kryterion Webassessor |
| Question Types | Multiple-choice, Multiple-response, (some labs) | Multi-choice, Case studies, Drag-and-drop, Labs | Multiple-choice, Multiple-select, Case studies |
| Labs in Exams | Increasingly present in some exams | Frequent for many certifications | None |
| Certificate Validity | 3 years | 1 year (Fundamentals non-expiring) | 2 years for professional exams |
| Renewal Process | Retake full exam | Free online assessment (shorter, focused on updates) | Retake full exam or pass PCA "renewal" exam |
| Proctoring Strictness | Moderate (OnVUE scans) | Moderate | Potentially stricter (Kryterion software) |

Google Cloud

Overview of the exam

# 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** |

Google Cloud

## 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."*

Google Cloud

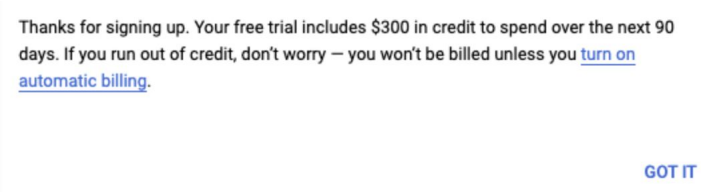
Overview of the exam

## 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




* 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.

And the last tip is really about giving you a bit more freedom when interacting with GCP. When going through the labs, you will always be constrained by time (each lab will last just 60 mins or so) and by different limits and quotas. However, if you're interested in having a long-term project, where you can explore, deploy something, have it running for a while, or go back to where you left off next day, you should definitely follow the link presented on the slide. It's not a part of our program anyhow; it's just Google giving everyone a possibility to get a feeling of their cloud platform by granting everyone 90-day access to GCP and 300USD free credits to deploy just anything you'd like.
We'd highly encourage you to use this opportunity to accelerate your learning journey!

# Google Skills Demo

Google Cloud

[CSB Demo]
https://www.cloudskillsboost.google/course_templates/645?catalog_rank=%7B%22rank%22%3A2%2C%22num_filters%22%3A1%2C%22has_search%22%3Atrue%7D&search_id=30466886

https://www.cloudskillsboost.google/focuses/48483?catalog_rank=%7B%22rank%22%3A2%2C%22num_filters%22%3A1%2C%22has_search%22%3Afalse%7D&parent=catalog

# 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.*

Google Cloud

First, a couple of terms so that we have a common understanding.

Capex is the traditional, on-premises approach where organizations purchase capacity upfront (e.g., datacenters, hardware) and amortize costs over years. It is easy but typically inflexible. Opex is the cloud-native, pay-as-you-go approach. Resources are used as needed, de-commissioned easily, and billed based on per-second usage, providing tremendous flexibility.

Exam Tip: While Opex is cloud-native, architects can optimize costs by committing to long-term usage (1–3 years), which conceptually leans back toward a Capex mode

## 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<br>Outside of GCP: MySQL, Oracle, PostgreSQL, Microsoft SQL Server. | In GCP: Firestore, Bigtable<br>Outside of GCP: MongoDB, Redis, Cassandra, HBase, CouchDB |



SQL (Relational) databases are traditional, table-based, strongly typed with fixed schemas, and mostly ACID-compliant. They are the default choice for monolithic applications. GCP examples: Cloud SQL, Cloud Spanner. NoSQL (Non-relational) databases use key-value, wide column, or document models, featuring dynamic schemas and are mostly BASE compliant. They are suitable for certain microservices. GCP examples: Firestore, Bigtable

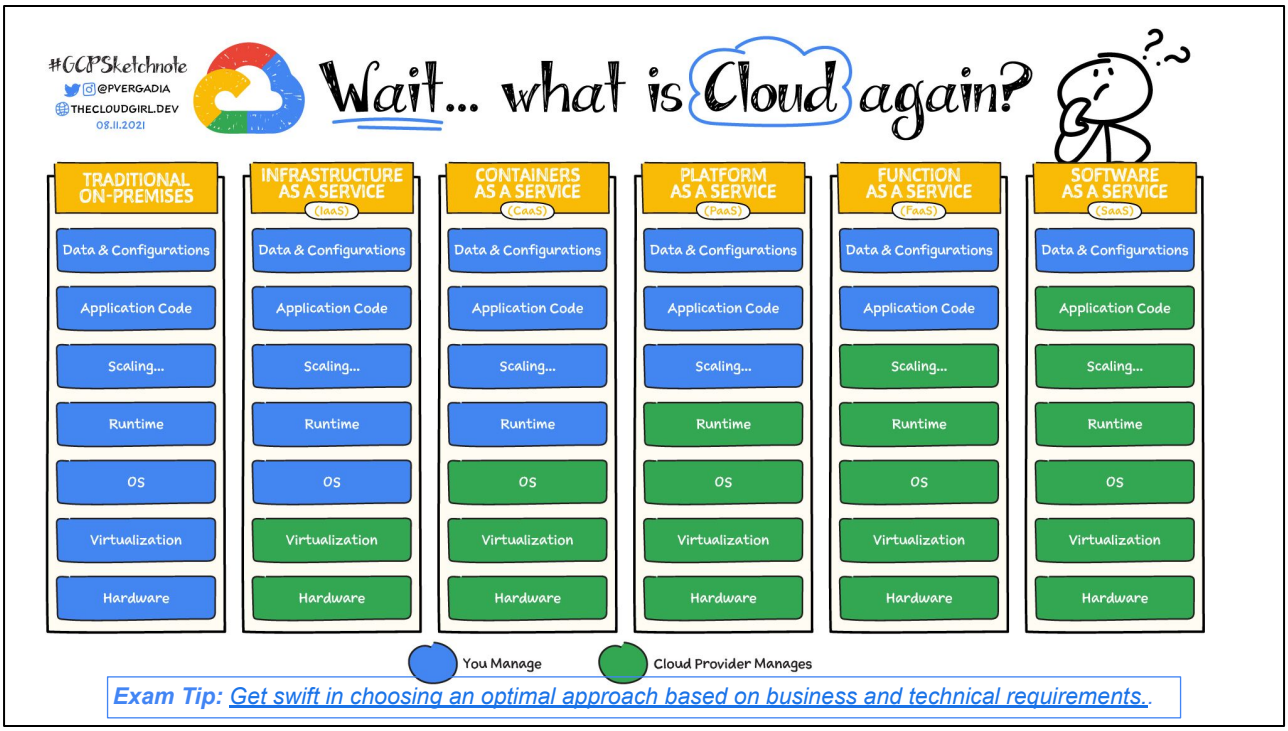
## OLTP vs OLAP

| **OLTransactionalP** | **OLAnalyticalP** |
|---|---|
| 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 |

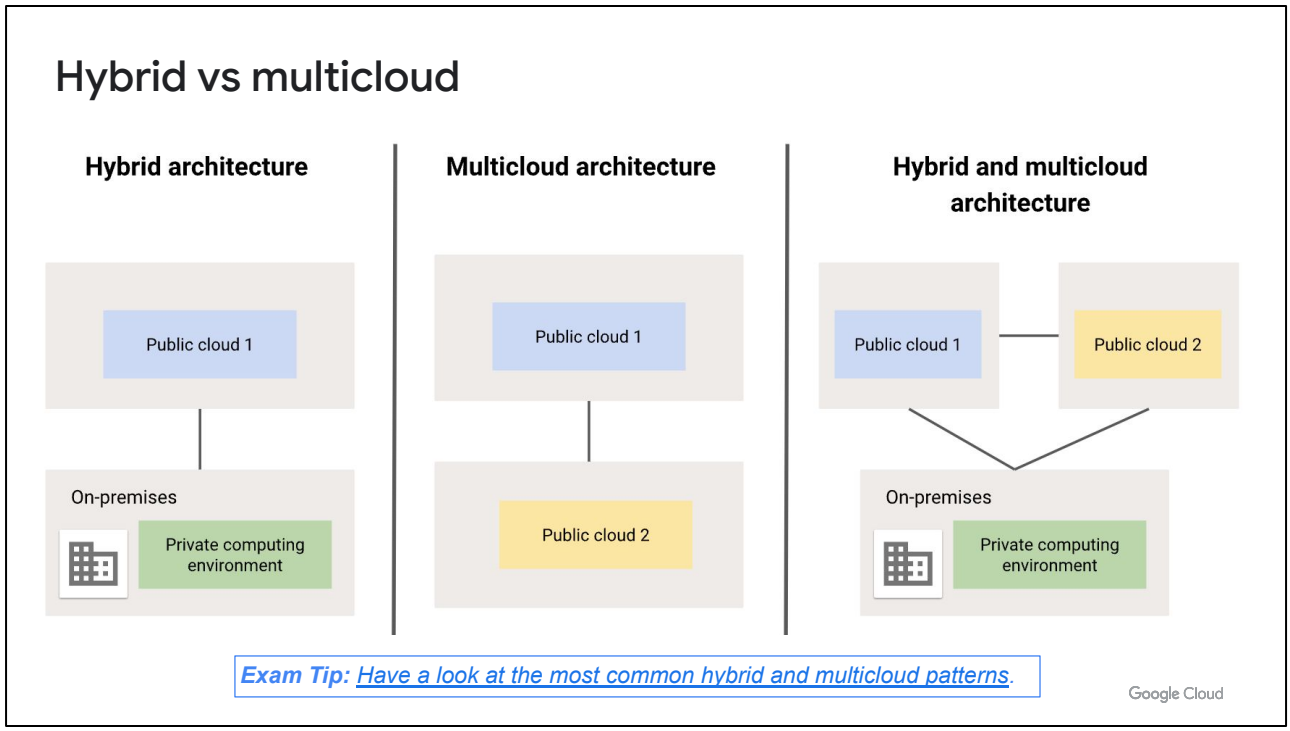
***Exam Tip:*** *Here you'll find a GREAT Decision tree for database choices on AWS, Microsoft Azure, Google Cloud Platform, and cloud-agnostic*

Google Cloud

OLTP (Online Transaction Processing) is for transaction-oriented apps involving large amounts of inserts, updates, and deletes on individual records. Tables are normalized and rely on ACID principles and SQL. GCP examples: Cloud SQL, Cloud Spanner. OLAP (Online Analytical Processing) is for multi-dimensional analytical queries (BI, reporting) involving large data volumes. It is optimized for high-throughput reads and uses non-normalized tables and SQL/NoSQL. GCP example: BigQuery

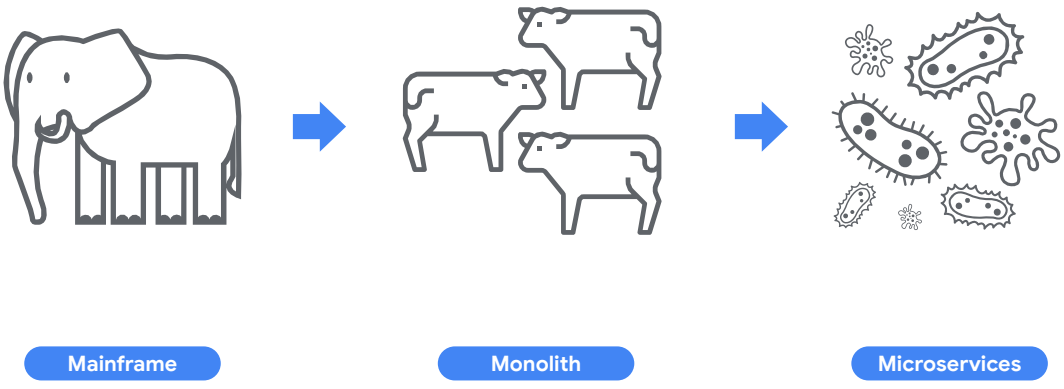



This visual shows the spectrum of service models based on management responsibility. As you move from Traditional On-Premises (where the user manages everything from hardware up) towards SaaS (Software as a Service), the amount of components managed by the Cloud Provider (green) increases. The intermediate models include IaaS (user manages OS up), CaaS (Containers as a Service), PaaS (Platform as a Service), and FaaS (Function as a Service)




Hybrid architecture links a Public cloud environment (Public cloud 1) with an on-premises private computing environment. Multicloud architecture uses resources from two or more public clouds (Public cloud 1 and Public cloud 2). It is also possible to have a combined Hybrid and Multicloud architecture.

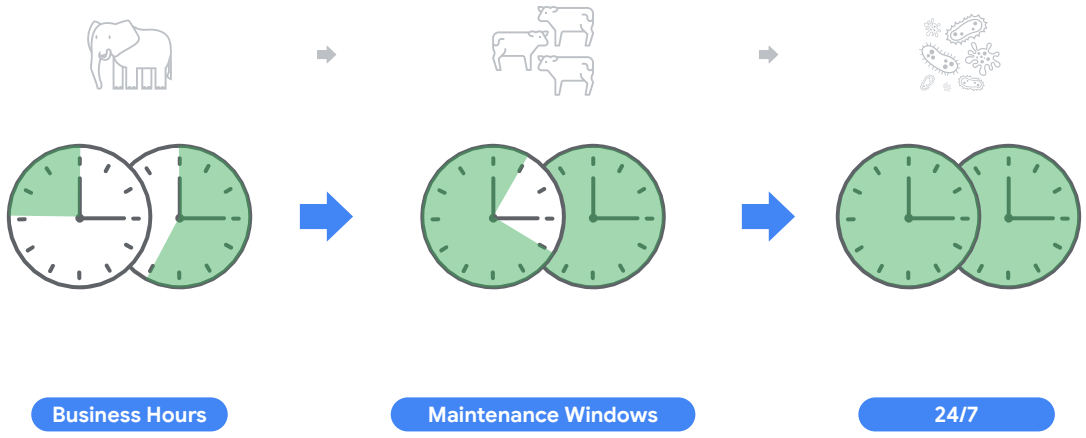
## Microservices - evolution




Let's now go a bit deeper into microservices, which are Google's preferred option for most types of workloads.

The architectural evolution progressed from the Mainframe model, to the Monolith model, and finally to the Microservices model

## Microservices - evolution




Operationally, this evolved from systems only running during Business Hours, requiring Maintenance Windows, to achieving continuous 24/7 operation

## 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.

Google Cloud

Key advantages include the ability to independently test and deploy services, the freedom to use different languages and frameworks for different use cases, the ability to dedicate teams to specific services, the loosening of dependencies between teams, and easier design for failure by having clear service boundaries

## 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.

Google Cloud

Disadvantages include increased overall system complexity. Communication occurs over a network, which can raise security concerns (often solved by tools like Istio, which automatically encrypts traffic). Performance can be challenging due to network latencies between services. Finally, observability (understanding production behavior) is harder, a problem Istio also addresses

# 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.

Which approach should you take?

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



B

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.

# 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.

Which approach should you take?

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

*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.*

Google Cloud

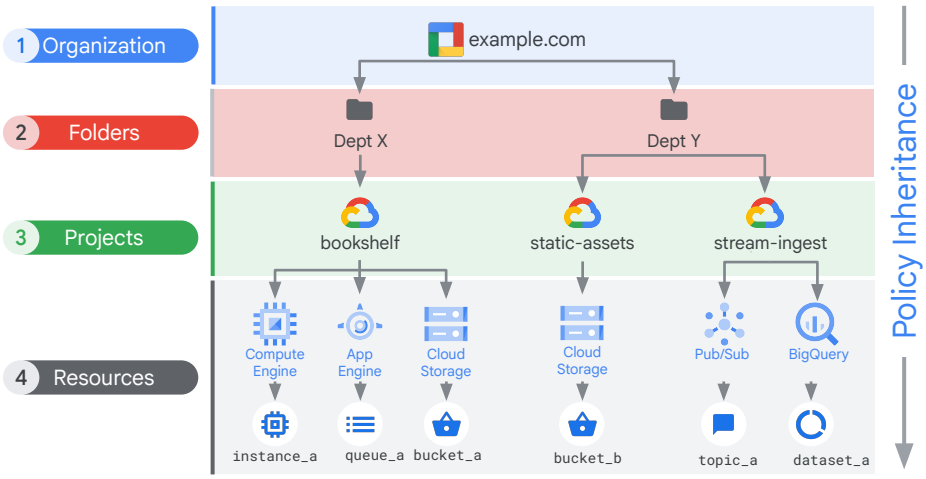
B

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.

# Resource hierarchy

1. Group “connected” resources and Isolate others
    a. Segregation of duties (privileges to different projects)
    b. Billing per project
2. Centralize / have central projects for “common” functionalities. ASK WHAT… networking, logging, monitoring, “project factory” / automation
    a. Mention a common misunderstanding, where networking and projects are thought of a 1:1 relationship
3. “Inheritance” used extensively (security, networking etc)

# Resource hierarchy in GCP






Source: Architecting with Compute Engine slides.

Speaker Notes: You can nest folders up to 10 (ten) levels deep.

Google Cloud resources are organized hierarchically, as shown in this tree structure. The Organization node is the root node in this hierarchy, folders are the children of the organization, projects are the children of the folders, and the individual resources are the children of projects. Each resource has exactly one parent.

The organization resource represents your company. IAM roles granted at this level are inherited by all resources under the organization.

The folder resource could represent your department. IAM roles granted at this level are inherited by all resources that the folder contains.

Projects represent a trust boundary within your company. Services within the same project have a default level of trust.

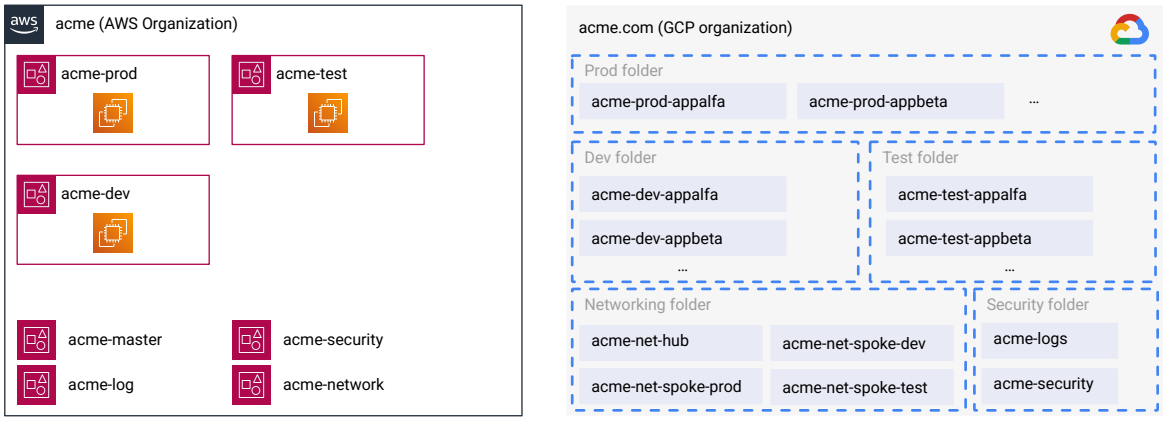
# Resource Management



AWS accounts → GCP projects

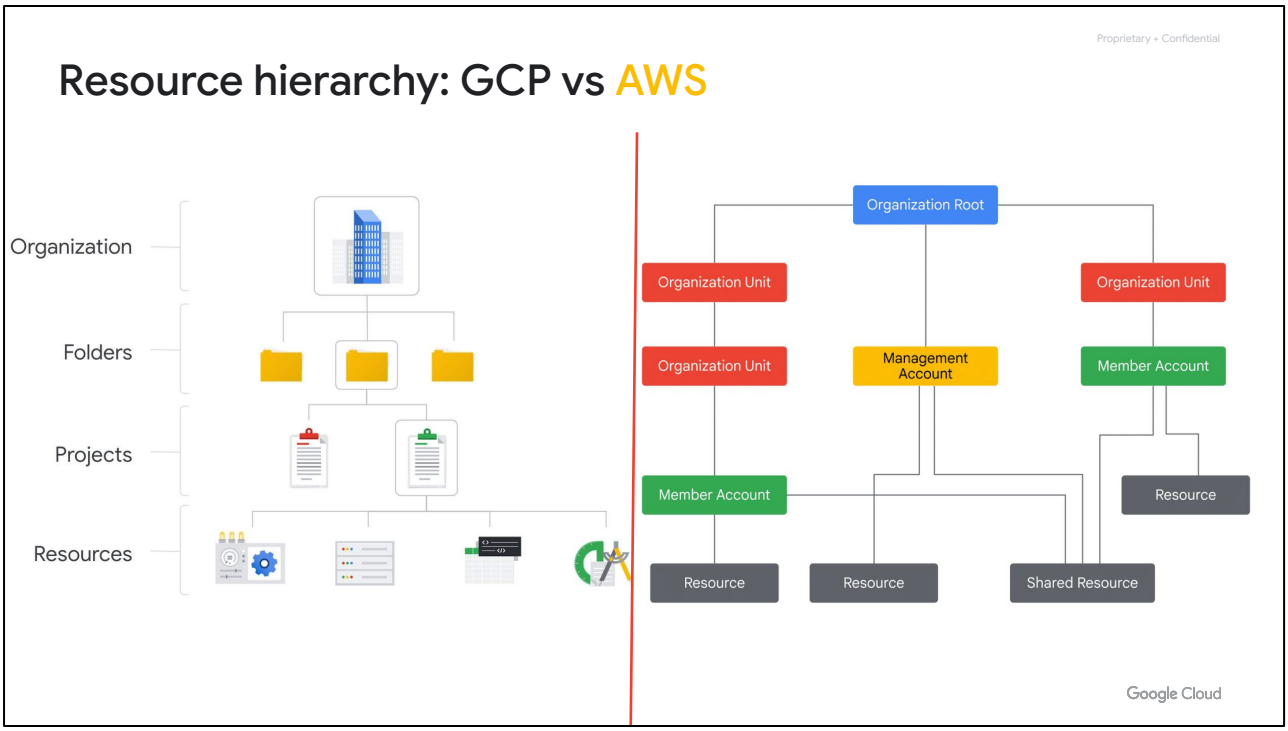
Few AWS accounts (one per environment and a *shared services* one) → Many GCP projects (one per project per environment).

AWS folders exist but have almost no impact → GCP folders are used extensively to organize permissions and firewalls.




- In **AWS**, the core boundary is the **Account**. You manage resources by creating multiple accounts (e.g., one for dev, one for prod) and grouping them with **AWS Organizations**.
- In **GCP**, the core boundary is the **Project**. You manage resources by creating multiple projects (e.g., `my-app-dev`, `my-app-prod`) which all live inside a single, hierarchical **Organization**.

This core difference influences everything from security and billing to policy enforcement (




AWS emphasizes account-based isolation, while GCP prioritize project/folders  for organization.

n GCP, the basic container is the “project,” which contains the resources for a single application. A “folder” is a container that can aggregate several projects. The folder consists of a nested structure all the way up in the organizational tiers. In GCP, the project is also the billing unit.

https://cloud.theodo.com/en/blog/manage-cloud-project

---

Remember, the AWS resource hierarchy has four levels:

1. Organization Root: A container that holds all the accounts that are shared within an organization.
2. Organization Unit: A container for accounts of other organizational units.
3. Accounts: A container for resources. This can be a management account or a member account.
4. Resource

Using AWS services requires having an account.

Organizational units are optional.

A management account is required for an organization, and is responsible for all charges accrued by that organization. All other accounts in AWS are member accounts.

## Resource hierarchy: GCP vs AWS

| Google Cloud | AWS |
|---|---|
| Organization | Organizational Root |
| Folder | Organizational Unit |
| Project | Management Account<br>Member Account |
| Resources | Resources<br>Shared Resources |

AWS emphasizes account-based isolation, while GCP prioritize project/resource groups for organization.

https://cloud.theodo.com/en/blog/manage-cloud-project


**TL;DR / Purpose of the slide:**

- Discuss the **rationale behind** the **best practice** of using **many projects**

**Key points:**

- The **first thing** to discuss is how will **resources** by **organized into projects**
- **Few projects**
  - It's **easy** to have just **one project** for all workloads
  - However, achieving **least privilege** and **managing IAM** will be **very complex and difficult**
- **Many projects**
  - There's more **management overhead** with this approach
  - However, achieving **least privilege** and **managing IAM** will be **much more manageable**
  - Solving **cross project communication** will also be needed
- Using **many projects** and is the **absolute best practice**.

**Probing questions (optional):**

- None

Proprietary + Confidential

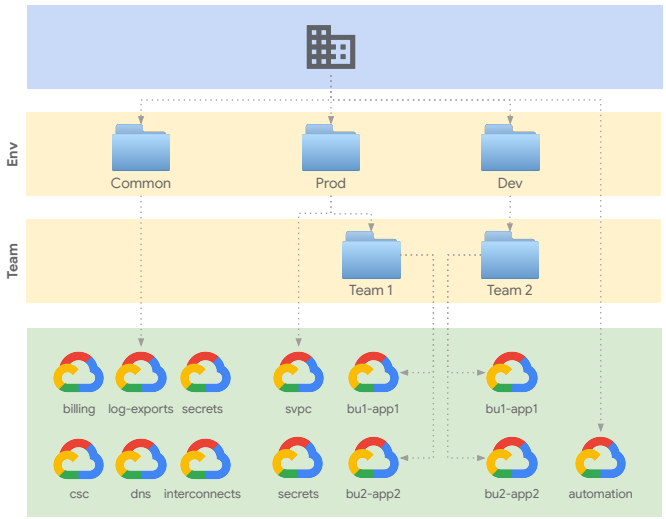
# Most common pattern: Environment-driven

A simplification of the pattern used by the security blueprints.

The main benefits of this design are to set up **virtually identical environments** that can be managed as clones, especially via IaC.

There is **limited aggregation of IAM and security policies**, which mainly happens at the environment level.

Aggregation can be increased somewhat by **adding additional folders**, like the team folders here.

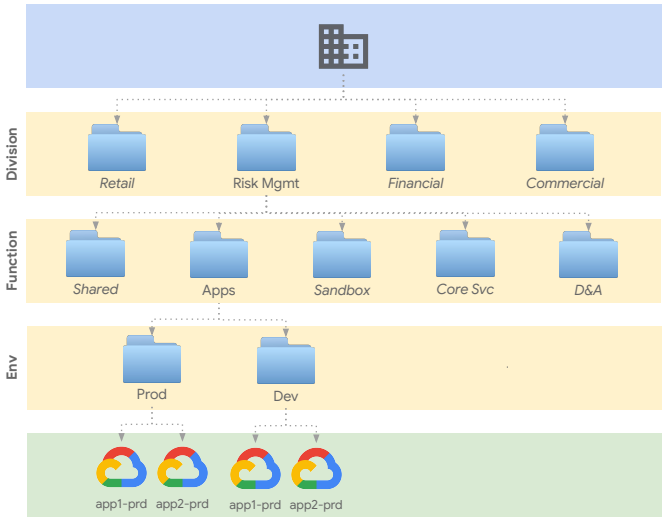


# Antipattern - Business-driven

A 1:1 mapping between a company's organizational layout and Google Cloud resources **rarely works**.

IAM needs to be applied at all levels of the hierarchy, and there's **no provision for centrally shared services** (like interconnects). Folders are often used as logical groups.

Start from this layout only if a strict division between business units is necessary, and/or **the org will primarily be used for managed Google Cloud services**.



# Diagnostic Question Discussion

Your client created an Identity and Access Management (IAM) resource hierarchy with Google Cloud when the company was a startup. Your client has grown and now has multiple departments and teams. You want to recommend a resource hierarchy that follows Google-recommended practices.

What should you do?

A. Keep all resources in one project, and use a flat resource hierarchy to reduce complexity and simplify management.

B. Keep all resources in one project, but change the resource hierarchy to reflect company organization.

C. Use a flat resource hierarchy and multiple projects with established trust boundaries.

D. Use multiple projects with established trust boundaries, and change the resource hierarchy to reflect company organization.



**Feedback:**
A. Incorrect. Mirror your Google Cloud resource hierarchy structure to match your organization structure. Use projects to group resources that share the same trust boundary.
B. Incorrect. Use projects to group resources that share the same trust boundary.
C. Incorrect. Mirror your Google Cloud resource hierarchy structure to match your organization structure.
D. Correct! Because the environment has evolved, update the IAM resource hierarchy to reflect the changes. Use projects to group resources that share the same trust boundary.

**Where to look**:
https://cloud.google.com/iam/docs/resource-hierarchy-access-control
https://cloud.google.com/iam/docs/resource-hierarchy-access-control#best_practices

**Content mapping:**
Architecting with Google Cloud: Design and Process, M8

**Summary:**
Best practices are incredibly important for Identity and Access Management (IAM). You encountered two best-practice rules in this question, but you should be familiar

with the rest. Look at the best practices in more detail in Google documentation.

# Diagnostic Question Discussion

Your client created an Identity and Access Management (IAM) resource hierarchy with Google Cloud when the company was a startup. Your client has grown and now has multiple departments and teams. You want to recommend a resource hierarchy that follows Google-recommended practices.

What should you do?

A. Keep all resources in one project, and use a flat resource hierarchy to reduce complexity and simplify management.

B. Keep all resources in one project, but change the resource hierarchy to reflect company organization.

C. Use a flat resource hierarchy and multiple projects with established trust boundaries.

**D. Use multiple projects with established trust boundaries, and change the resource hierarchy to reflect company organization.**



**Feedback:**
A. Incorrect. Mirror your Google Cloud resource hierarchy structure to match your organization structure. Use projects to group resources that share the same trust boundary.
B. Incorrect. Use projects to group resources that share the same trust boundary.
C. Incorrect. Mirror your Google Cloud resource hierarchy structure to match your organization structure.
D. Correct! Because the environment has evolved, update the IAM resource hierarchy to reflect the changes. Use projects to group resources that share the same trust boundary.

**Where to look**:
https://cloud.google.com/iam/docs/resource-hierarchy-access-control
https://cloud.google.com/iam/docs/resource-hierarchy-access-control#best_practices

**Content mapping:**
Architecting with Google Cloud: Design and Process, M8

**Summary:**
Best practices are incredibly important for Identity and Access Management (IAM). You encountered two best-practice rules in this question, but you should be familiar

with the rest. Look at the best practices in more detail in Google documentation.

# Diagnostic Question Discussion

You want to allow your operations team to store logs from all the production projects in your Organization, without including logs from other projects. All of the production projects are contained in a folder. You want to ensure that all logs for existing and new production projects are captured automatically.

What should you do?

A. Create an aggregated export on the Production folder. Set the log sink to be a Cloud Storage bucket in an operations project.

B. Create an aggregated export on the Organization resource. Set the log sink to be a Cloud Storage bucket in an operations project.

C. Create log exports in the production projects. Set the log sinks to be a Cloud Storage bucket in an operations project.

D. Create log exports in the production projects. Set the log sinks to be BigQuery datasets in the production projects, and grant IAM access to the operations team to run queries on the datasets.



A.
But first eliminate C & D!

# Diagnostic Question Discussion

You want to allow your operations team to store logs from all the production projects in your Organization, without including logs from other projects. All of the production projects are contained in a folder. You want to ensure that all logs for existing and new production projects are captured automatically.

What should you do?

**A. Create an aggregated export on the Production folder. Set the log sink to be a Cloud Storage bucket in an operations project.**

B. Create an aggregated export on the Organization resource. Set the log sink to be a Cloud Storage bucket in an operations project.

C. Create log exports in the production projects. Set the log sinks to be a Cloud Storage bucket in an operations project.

D. Create log exports in the production projects. Set the log sinks to be BigQuery datasets in the production projects, and grant IAM access to the operations team to run queries on the datasets.



A.
But first eliminate C & D!

## Make sure to...

Enjoy the journey as much as the destination!




Now that you know about the overall setup of this course and how to use the workbook, let's get started by exploring section 1 of the exam guide.