

*CFGS-DAW (ies blasco ibáñez cullera)*

## ***MÒDUL: INTRODUCCIÓ AL NÚVOL PÚBLIC***

*DURADA: 96 hores*



xavi blanes (cc) 25/26

# Índex:

*Tema 1: El núvol públic*

*Tema 2: Facturació i Economia del Núvol*

*Tema 3: Infraestructura global i serveis del núvol*

*Tema 4: Mesures bàsiques de seguretat al núvol*

*Tema 5: Xarxes i lliurament de continguts*

*Tema 6: Computació en el núvol i escalat automàtic*

*Tema 7: Bases de dades al núvol*

*Tema 8: Marc de treball Well-Architected*

# Tema 1: El núvol públic

---



---

## 1. Diferències entre el núvol públic, privat i híbrid

1.1 Núvol Públic (Public Cloud)

1.2 Núvol Privat (Private Cloud)

1.3 Núvol Híbrid (Hybrid Cloud)

1.4 Esquema resum

## 2. Què és el núvol?

2.1 Components principals de l'ecosistema del núvol

2.2 Beneficis de l'ús del núvol

2.3 Reptes i consideracions

## 3. IaaS, PaaS i SaaS

## 3. Principis de migració al núvol

3.1. Avaluació i planificació:

3.2. Classificació de càrregues de treball

3.3 Triar l'estratègia de migració ("Les 6 R")

3.4. Seguretat i compliment normatiu

3.5. Prova, validació i optimització

3.6. Formació i gestió del canvi

3.7. Monitorització i manteniment continu

## 1. Diferències entre el núvol públic, privat i híbrid

La computació en el núvol, es un model que permet accedir a recursos informàtics (com servidors, emmagatzematge, bases de dades, xarxes, programari, etc.) a través d'Internet, a demanda i normalment pagant només pel que s'utilitza.

Tenim diversos núvols. Les diferències entre núvol públic, núvol privat i núvol híbrid es basen en com s'ofereixen i s'administren els serveis de computació en el núvol (cloud computing). Tot seguit et detallaré les característiques principals de cadascun:

### 1.1 Núvol Públic (*Public Cloud*)

**Definició:** Infraestructura gestionada per un proveïdor extern (com AWS, Microsoft Azure, Google Cloud), compartida entre diversos clients.

#### Característiques:

- Els recursos (servidors, emmagatzematge, xarxa) s'allotgen als centres de dades del proveïdor.
- Escalabilitat alta i a demanda.
- Model de pagament per ús.
- No cal manteniment per part de l'empresa usuària.

**Exemples:** Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), IBM Cloud.

#### Avantatges:

- Cost inicial baix.
- Fàcil accés des de qualsevol lloc.
- Bona per a xicotetes empreses o startups.

#### Inconvenients:

- Menys control i personalització.
- Pot generar preocupacions de seguretat i privacitat.

### 1.2 Núvol Privat (*Private Cloud*)

**Definició:** Infraestructura dedicada exclusivament a una sola organització, ja siga interna (a les instal·lacions pròpies) o allotjada per un proveïdor extern.

#### Característiques:

- Més control sobre la infraestructura i les dades.
- Altament personalitzable segons necessitats específiques.
- Pot estar ubicada físicament a l'empresa o en un centre de dades dedicat.

#### Avantatges:

- Major seguretat i control de dades.

- Compliment més fàcil amb normatives específiques (ex: RGPD, HIPAA).
- Millor rendiment per a aplicacions crítiques.

#### Inconvenients:

- Cost inicial i de manteniment més alt.
- Més complexitat tècnica.

### 1.3 Núvol Híbrid (Hybrid Cloud)

**Definició:** Combinació de núvol públic i privat que permet compartir dades i aplicacions entre ambdós entorns.

#### Característiques:

- Permet que una part de la infraestructura i serveis estiga en el núvol públic i l'altra en el privat.
- Molt flexible: es poden moure càrregues de treball segons les necessitats.

#### Avantatges:

- Equilibri entre cost, rendiment i seguretat.
- Facilita la transició gradual cap al núvol.
- Es pot usar el públic per pics de demanda i el privat per dades sensibles.

#### Inconvenients:

- Complexitat en la gestió i integració entre ambdós entorns.
- Pot requerir infraestructura i coneixement avançat.

### 1.4 Esquema resum:

Característica	Núvol Públic	Núvol Privat	Núvol Híbrid
<b>Cost</b>	Baix (pagament per ús)	Alt (infraestructura pròpia)	Mitjà
<b>Seguretat</b>	Estàndard	Alta	Depèn de la part privada
<b>Escalabilitat</b>	Alta	Limitada	Alta (si s'integra bé)
<b>Control</b>	Limitat	Total	Parcial
<b>Complexitat tècnica</b>	Baixa	Alta	Alta

## 2. Què és el núvol?

El núvol (o cloud) és un conjunt de serveis informàtics (com emmagatzematge, bases de dades, servidors, aplicacions i xarxes) accessibles a través d'Internet, de manera flexible, escalable i a demanda.

L'ecosistema del núvol no és només un conjunt de servidors remots, sinó tot un entorn tecnològic que permet a empreses i usuaris desenvolupar, allotjar i gestionar aplicacions i serveis d'una manera més àgil, eficient i global. Entendre els seus components i serveis és clau per a treure'n el màxim profit.

No podem parlar de núvol sense parlar de model servidor client. Però, què és el model Servidor-Client? És un model de comunicació entre dos tipus de dispositius o aplicacions:

El client: és el dispositiu o aplicació que fa una sol·licitud (ex: un navegador web).

El servidor: és l'ordinador o sistema que processa aquesta sol·licitud i retorna una resposta (ex: el servidor d'un lloc web).

Com funciona? El client envia una petició (ex: "Vull veure la pàgina web X"). El servidor rep la petició, la processa i retorna la informació (ex: el contingut HTML d'una pàgina). Per últim, el client mostra aquesta informació a l'usuari.

Exemples:

- Quan entres a [www.wikipedia.org](http://www.wikipedia.org), el teu navegador (client) demana informació al servidor de Wikipedia.
- Aplicacions mòbils que accedeixen a dades des d'un backend (servidor).

El núvol utilitza el model servidor-client. Quan accedeixes a un servei al núvol (com Google Docs), el teu dispositiu actua com a client, i Google Docs actua com a servidor allotjat al núvol. Així, el cloud és una infraestructura basada en servidors que serveixen dades i serveis als clients.

Altra qüestió important serà que els servidors de cloud o datacenters caldrà ubicar-lo atenent a:

- Disponibilitat d'energia
- Connectivitat
- Estabilitat política i ambiental
- Proximitat als usuaris finals

## *2.1 Components principals de l'ecosistema del núvol*

**Proveïdors de núvol:** Empreses que ofereixen infraestructura i serveis de núvol.

- Públics: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), IBM Cloud.
- Privats / híbrids: OpenStack, VMware, Oracle Cloud, etc.

**Models de desplegament:**

- Núvol públic: Infraestructura compartida entre múltiples clients.
- Núvol privat: Infraestructura dedicada a una sola organització.
- Núvol híbrid: Combinació de públic i privat.
- Multinúvol (Multicloud): Ús de diversos proveïdors de núvol alhora.

**Models de servei:** Els serveis en el núvol es classifiquen segons el nivell de control:

- IaaS (Infrastructure as a Service): Infraestructura com a servei (ex: màquines virtuals, xarxes). Ex: AWS EC2.

- PaaS (Platform as a Service): Plataforma per desenvolupar i desplegar aplicacions. Ex: Google App Engine, Heroku.
- SaaS (Software as a Service): Programari ja preparat per ser usat via web. Ex: Gmail, Microsoft 365, Dropbox.

### Serveis més comuns del núvol:

- Emmagatzematge (S3, Google Cloud Storage)
- Processament i servidors virtuals
- Bases de dades (SQL i NoSQL)
- Analítica i big data
- Aprenentatge automàtic i IA
- Xarxes i seguretat
- Monitorització i gestió

### 2.2 Beneficis de l'ús del núvol

- Escalabilitat: Adapta els recursos fàcilment segons la demanda.
- Eficiència de costos: Pagues només pel que utilitzes.
- Accés global: Treballa des de qualsevol lloc.
- Actualitzacions automàtiques: Sempre amb la darrera versió.
- Alta disponibilitat: Sistemes redundants i còpies de seguretat.

### 2.3 Reptes i consideracions

- Seguretat i privadesa de dades
- Compliment normatiu (ex: RGPD)
- Dependència del proveïdor (vendor lock-in)
- Gestió de costos descontrolats
- Integració amb sistemes locals (on-premise)

## 3. IaaS, PaaS i SaaS

Són els models principals del cloud computing.

### IaaS – Infraestructura com a Servei

Què és? El proveïdor et dona accés a infraestructura bàsica: servidors, xarxes, emmagatzematge, etc. Tu controles el sistema operatiu i les aplicacions. Tu gestionas: sistema operatiu, aplicacions, configuració de xarxes.

Exemple:

- Microsoft Azure (VMs)
- Amazon EC2 (servidors virtuals)
- Google Compute Engine

És ideal per a administradors de sistemes, empreses que volen màxim control.

### PaaS – Plataforma com a Servei

Què és? el proveïdor et dona una plataforma per desenvolupar i executar aplicacions, sense preocupar-te per la infraestructura ni pel sistema operatiu. Tu gestionas: el codi i la lògica de la teua aplicació

Exemple:

- Azure App Services
- Google App Engine
- Heroku

Ideal per a desenvolupadors, aplicacions web i mòbils ràpides de desplegar.

### SaaS – Programari com a Servei

Què és? el proveïdor t'ofereix aplicacions llestes per fer servir a través d'Internet. No cal instal·lar ni mantenir res. Tu només inicias sessió i utilitzes el servei.

Exemple:

- Gmail
- Microsoft 365 (Word, Excel online)
- Dropbox
- Zoom

Ideal per a usuaris finals i empreses que volen estalviar temps i costos

Model	Qui ho gestiona?	Tu controles...	Exemple
<b>IaaS</b>	El núvol: maquinari i xarxes	Sistema operatiu i aplicacions	Azure VM, AWS EC2
<b>PaaS</b>	El núvol: infra + OS + entorn	Només el codi de l'app	Heroku, App Engine
<b>SaaS</b>	Tot gestionat pel proveïdor	Només utilitzar l'app	Gmail, Teams, Dropbox

## 4. Principis de migració al núvol

Migrar al núvol és un procés estratègic que implica moure dades, aplicacions i serveis des d'un entorn local (on-premise) cap a una infraestructura basada en el núvol. Per fer-ho de manera eficient i segura, cal seguir una sèrie de principis fonamentals.

### 4.1. Avaluació i planificació:

- Analitzar l'estat actual de la infraestructura: aplicacions, bases de dades, dependències.



- Identificar objectius clars: Reduir costos? Millorar l'escalabilitat? Augmentar la disponibilitat?
- Seleccionar el model de núvol: públic, privat, híbrid o multinúvol.
- Fer una estimació de costos i ROI (retorn de la inversió).

#### *4.2. Classificació de càrregues de treball*

- Classificar aplicacions segons la seua criticitat, complexitat i compatibilitat amb el núvol.
- Decidir quines aplicacions es poden migrar tal com estan i quines s'han de replantejar o substituir.

#### *4.3 Triar l'estratègia de migració ("Les 6 R")*

Les 6 estratègies clàssiques de migració:

- Rehosting (Lift & Shift): moure l'aplicació tal com està.
- Replatforming: fer xicotets ajustos per a adaptar-la al núvol.
- Repurchasing: substituir l'aplicació per una SaaS.
- Refactoring/Re-architecting: redissenyar completament per aprofitar millor el núvol.
- Retire: eliminar aplicacions que ja no calen.
- Retain: mantenir algunes aplicacions on-premise temporalment.

#### *4.4. Seguretat i compliment normatiu*

- Garantir la protecció de dades sensibles durant i després de la migració.
- Complir amb normatives com RGPD, ISO 27001, etc.
- Definir una política de governança del núvol.

#### *4.5. Prova, validació i optimització*

- Realitzar proves pilot abans de migrar en massa.
- Monitoritzar el rendiment, la disponibilitat i la seguretat.
- Optimitzar els recursos per reduir costos i millorar l'eficiència.

#### *4.6. Formació i gestió del canvi*

- Formar els equips tècnics i usuaris finals.
- Gestionar la resistència al canvi amb comunicació i suport.
- Establir nous rols i processos adaptats a l'entorn del núvol.

#### *4.7. Monitorització i manteniment continu*

- Utilitzar eines de monitoratge i gestió per garantir el bon funcionament.
- Revisar i ajustar regularment l'arquitectura per optimitzar costos, rendiment i seguretat.

Pel que fa a les eines, en AWS tenim L'**AWS Migration Hub** és una plataforma centralitzada que et permet planificar, gestionar i fer seguiment de les migracions cap a AWS, ja sigui des de servidors locals, centres de dades, màquines virtuals o altres núvols.

#### Eines principals de migració dins d'AWS:

Eina	Què fa?
<b>AWS Application Migration Service (MGN)</b>	Migra servidors físics o virtuals (com VMware o Hyper-V) automàticament cap a EC2.
<b>AWS Database Migration Service (DMS)</b>	Migra bases de dades (per exemple, d'Oracle o SQL Server a Amazon RDS o Aurora).
<b>Migration Hub Strategy Recommendations</b>	Analitza les aplicacions i fa recomanacions de migració: rehost, replatform, refactor, etc.
<b>Migration Hub Orchestrator</b>	Automatitza tasques repetitives del procés de migració (validacions, scripts, configuracions).

---

## Tema 2: Facturació i Economia del Núvol

---



1. *Models de pagament del núvol*
  - 1.1. *Pay-as-you-go (pagament per ús)*
  - 1.2. *Reserved Instances (RIs)*
  - 1.3. *Spot Instances (instàncies d'oportunitat)*
2. *Costos habituals en una factura de núvol*
3. *Economia del núvol: com optimitzar*
4. *Governança i control de costos. Bones pràctiques:*
5. *la calculadora de costos en el cloud computing*
  - 5.1. *Què és una calculadora de costos al núvol?*
  - 5.2. *Calculadores de costos més populars*
  - 5.3. *Avantatges d'utilitzar la calculadora*
6. *Models de suport tècnic de cloud*
7. *Firebase de Google. És gratis?*

## 1. Models de pagament del núvol

### 1.1. Pay-as-you-go (pagament per ús)

#### Característiques:

- Facturació basada en unitats d'ús (hores de CPU, GB emmagatzemats, peticions API, etc.).
- Flexible i sense compromís a llarg termini.
- Ideal per a startups, entorns de proves o càrregues variables.

### 1.2. Reserved Instances (RIs)

#### Característiques:

- Són compromisos de capacitat a 1 o 3 anys.
- Estalvi de fins a un 75% respecte al model on-demand.
- Ideal per a càrregues de treball previsibles i permanents.

#### Aspectes a considerar:

- Compromís de temps = menys flexibilitat.
- Cal avaluar bé la capacitat futura.

### 1.3. Spot Instances (instàncies d'oportunitat)

#### Característiques:

- Recursos sobrants venuts a preu molt reduït (fins a 90% menys).
- Ideal per a batch jobs, simulacions, renders i IA.
- Es poden interrompre en qualsevol moment per part del proveïdor.

#### Exemple:

- Una instància EC2 que costa \$0.10/h pot passar a costar \$0.02/h com a spot.

## 2. Costos habituals en una factura de núvol

#### Desglossament típic:

Servei	Mètrica de cost	Observacions
CPU / VM	per hora, per tipus d'instància	Càlcul intensiu = més cost
Emmagatzematge	per GB/mes, per tipus (HDD/SSD/Objecte)	S3, EBS, Persistent Disks
Xarxa	per GB eixints (egress)	Entrada normalment gratuïta
DB gestionades	per mida, transaccions, IOPS	MySQL, PostgreSQL, etc.
Serveis avançats	per petició o ús (IA, traducció, etc.)	IA, Lambda, AutoML...

Important: Moltes empreses obliden el cost del tràfic d'eixida, que pot ser significatiu si mouen moltes dades fora del núvol.

### 3. Economia del núvol: com optimitzar

L'economia del núvol fa referència a la gestió eficient dels recursos informàtics al núvol, buscant el màxim rendiment amb el mínim cost. Ací tens algunes estratègies clau per a optimitzar:

- Entendre el model de costos del núvol: Les plataformes com AWS, Azure i Google Cloud cobren per ús (temps, emmagatzematge, transferència de dades, etc.). Hi ha costos ocults com dades sortints (egress), snapshots, serveis inactius...
- Disseny eficient: escalar per demanda. Usa auto-scaling per adaptar recursos segons la càrrega. Tria instàncies spot o reservades per a tasques previsibles o no crítiques (són molt més barates).
- Monitoratge i etiquetatge. Monitoritza l'ús de recursos (amb CloudWatch, Azure Monitor...). També etiquetar (tag) recursos per a saber qui en fa ús i amb quin propòsit.
- Evitar el malbaratament. Apaga entorns de desenvolupament fora d'hores laborals. Elimina volums i snapshots inactius.
- Escull serveis gestionats quan calga. Sovint és més barat (i eficient) usar serveis gestionats com **RDS**, **BigQuery** o **Cloud Functions** que mantenir infraestructura pròpia.
- Auditories i revisions periòdiques. Fes revisions mensuals per identificar serveis sobredimensionats o infrautilitzats. També usar eines com **AWS Trusted Advisor** o **Azure Cost Management**.

Per a controlar els costos a AWS, hi ha diverses eines i pràctiques que poden ajudar-te a fer un seguiment, optimitzar i reduir les despeses. Ací tens una llista de les eines més útils que pots utilitzar:

#### En AWS. Eines clau

- **AWS Cost Explorer**. Per analitzar i visualitzar els teus costos i ús amb gràfics i filtres.
- **AWS Budgets**. Per establir límits de despesa i rebre alertes quan t'hi acostes o els superes.
- **AWS Trusted Advisor**. Dona recomanacions per optimitzar costos, seguretat i rendiment.

#### En Azure. Eines clau

- **Azure Cost Management + Billing**. Plataforma central per veure, analitzar i controlar els costos.
- **Azure Budgets**. Per definir pressupostos i configurar alertes automàtiques.

- Azure **Advisor**. Recomanacions per reduir costos i millorar l'eficiència dels recursos.

#### 4. Governança i control de costos. Bones pràctiques:

- Configurar alertes de pressupost: en AWS, Azure i GCP. Es poden crear alertes per a cada compte o projecte.
- Fer servir eines de cada empresa de cloud:
  - \* AWS Cost Explorer
  - \* Azure Cost Management + Advisor
  - \* GCP Billing Reports
- Polítiques de cost awareness:
  - \* Tallers de conscienciació per equips de desenvolupament.
  - \* Documentar el "núvol amb responsabilitat".
- Estratègies avançades per reduir despeses

Eina/estratègia	Avantatge
Serverless (Lambda, Cloud Run)	No pagues quan no s'executa
Object Storage (S3, GCS)	Més barat que disc SSD/HDD
Auto Scaling i Load Balancers	Eficiència durant pics de demanda
Multi-regió optimitzada	Triar regions amb millor preu
Arquitectura modular	Facilita pagar només pel que s'usa

#### 5. la calculadora de costos en el cloud computing

La calculadora de costos en el cloud computing és una eina essencial per a estimar, planificar i optimitzar la despesa abans d'implementar o migrar recursos al núvol.

Tots els grans proveïdors (AWS, Azure, GCP, etc.) ofereixen calculadores oficials per ajudar-te a comprendre quant pagaràs segons l'ús previst, tenint en compte múltiples factors: temps de funcionament, regions, tipus de màquines, emmagatzematge, tràfic, i més.

##### 5.1. Què és una calculadora de costos al núvol?

És una eina interactiva que et permet:

- Simular configuracions de serveis al núvol.
- Estimar el cost mensual o anual segons el consum.
- Comparar opcions (per exemple: instàncies reservades vs. on-demand).
- Analitzar l'impacte del tipus de servei, la regió i el model de pagament.

##### 5.2. Calculadores de costos més populars

- AWS Pricing Calculator. Permet afegir serveis com EC2, S3, RDS, Lambda, etc. Ofereix opcions de configuració molt detallades (CPU, memòria, OS, zona geogràfica...).
- Microsoft Azure Pricing Calculator. Molt visual i intuïtiva. Et permet exportar estimacions i compartir-les. Compatible amb serveis típics: VM, Cosmos DB, AKS, Logic Apps...
- Google Cloud Pricing Calculator. Permet simular l'ús de Compute Engine, Cloud Storage, BigQuery, etc. Inclou opcions d'ús sostingut, preus per compromís, etc.

Exemple pràctic (AWS). Simular una xicoteta aplicació web:

- \* EC2 t3.micro (1 vCPU, 1 GiB RAM): \$8.47/mes
- \* S3 amb 50 GB d'objectes: \$1.15/mes
- \* 10 GB de tràfic d'eixida: \$0.90/mes

**Total estimat: \$10.52/mes**

És només una estimació. El cost real pot variar segons el trànsit i l'activitat.

### 5.3. Avantatges d'utilitzar la calculadora

- Evites sorpreses a la factura real.
- Pots comprovar diferents escenaris d'ús.
- Ajuda a prendre decisions informades sobre CAPEX vs OPEX.
- És útil per a pressupostos, projectes TIC i auditories de viabilitat.

## 6. Models de suport tècnic de cloud

Els models de suport tècnic al núvol són els serveis que els proveïdors de cloud ofereixen per ajudar-te a resoldre problemes tècnics, optimitzar recursos i garantir el bon funcionament dels teus sistemes. Aquests models varien en funció del nivell de servei, la criticitat de les aplicacions i el pressupost del client. Els Tipus de models de suport més comuns:

● Suport bàsic (gratuït). Inclòs per defecte en la majoria de serveis. Inclou: documentació, fòrums de la comunitat, tutorials.

Limitacions:

- No hi ha assistència directa de tècnics.
- No està pensat per a entorns crítics.
- Ideal per a: desenvolupadors, entorns de proves, startups al principi.

● Suport estàndard (de pagament moderat). Accés a enginyers de suport 24/7 per a problemes amb producció. Temps de resposta més ràpid (en general 4-24 h segons la severitat). Inclou recomanacions bàsiques d'optimització.

● Suport avançat / empresarial (Enterprise Support). Pensat per a entorns crítics, grans empreses o serveis sempre actius.

Característiques:

- Resposta en menys d'1 hora per incidències crítiques.
- Gestor tècnic assignat (Technical Account Manager - TAM).
- Revisions de l'arquitectura, seguiment proactiu, planificació de capacitat.
- Assessorament per optimitzar rendiment i costos.
- Inclou eines avançades de monitoratge i informes mensuals.

Resum:

Característica	Bàsic	Estàndard	Enterprise
Cost	Gratuït	% del consum mensual	% més alt + mínim fix
Suport 24/7	× No	✓ Per incidències	✓ Total
Gestor dedicat (TAM)	× No	× No	✓ Sí
Temps resposta crítica	–	< 4-8 h	< 1 h
Optimització de costos	× No	✓ Bàsic	✓ Avançat
Revisió d'arquitectura	× No	✓ Opcional	✓ Personalitzada
Accés a formació/tallers	× Limitat	✓ Alguns	✓ Complet

Consideracions per a triar un model

- Quina criticitat té el teu entorn? (producció crítica = millor suport)
- Tens personal tècnic intern capacitat?
- Necessites ajuda en migració, arquitectura o seguretat?
- Vols optimitzar costos amb assistència directa?

## 7. Firebase de Google. És gratis?

A Firebase de Google, hi ha una combinació de serveis gratuïts i de pagament, que depenen del pla de tarifes que tries. Firebase ofereix principalment dos plans:

*Pla gratuït – Spark Plan*

Aquest pla és ideal per a desenvolupament i aplicacions xicotetes. Inclou:

- Authentication (Autenticació).



- 10.000 usuaris/anònims/mes.
- Mètodes bàsics com email/password i Google/Facebook/Twitter, etc.
- Cloud Firestore (base de dades NoSQL)
  - 50.000 lectures/dia.
  - 20.000 escrits/dia.
  - 1 GB d'emmagatzematge.
- Realtime Database
  - 1 GB d'emmagatzematge.
  - 100.000 connexions simultànies.
  - 1 GB descarregat/dia.
- Hosting
  - 1 GB d'emmagatzematge.
  - 10 GB/mes de transferència.
- Cloud Functions
  - 125.000 invocacions/mes.
  - 40.000 GB-segons/mes.
  - 40.000 CPU-segons/mes.
- Firebase ML (Machine Learning)
  - Algunes funcions gratuïtes (com text recognition, face detection).
- Analytics, Crashlytics, Performance Monitoring, App Distribution
  - Il·limitats i gratuïts.

### *Pla de pagament – Blaze Plan (pagament per ús)*

Aquest pla és escalable i pagues segons l'ús real dels serveis. Ofereix:

- Firestore
- Realtime Database
- Hosting
- Cloud Storage (per pujar fitxers com imatges o vídeos)
- Test Lab (test automatitzat d'apps Android/iOS)
- Phone Authentication (verificació via SMS)

### *Quins serveis són sempre gratuïts?*

- Google Analytics per Firebase

- Crashlytics
- App Distribution
- Performance Monitoring

Resumit:

<b>Servei</b>	<b>Spark (Gratuït)</b>	<b>Blaze (Pagament per ús)</b>
Firestore	Limitat	Escalable, es paga
Realtime Database	Limitat	Escalable, es paga
Hosting	1 GB / 10 GB transferència	Es paga extra
Cloud Functions	125k invocacions gratis	Es paga després
Autenticació SMS	Molt limitat	Es paga segons país
Analytics / Crashlytics	Gratuït	Gratuït

---

# Tema 3: Infraestructura global i serveis del núvol

---



## 1. Infraestructura global del cloud

- 1.1. Components clau de la infraestructura global
- 1.2. Exemple real: Infraestructura de AWS
- 1.3. Per què és important aquesta infraestructura?
- 1.4. Comparativa entre proveïdors:

## 2. Categories de Serveis

- 2.1. Càlcul (Compute).
- 2.2. Emmagatzematge (Storage).
- 2.3. Bases de dades (Databases).
- 2.4. Xarxa i CDN (Networking & Content Delivery).
- 2.5. Seguretat, identitat i compliment (Security, Identity & Compliance).
- 2.6. Monitoratge i gestió (Monitoring & Management).
- 2.7. Machine Learning i IA.
- 2.8. DevOps i eines de desenvolupament.

## 3. Exploració de la Consola d'Administració

## 1. Infraestructura global del cloud

La infraestructura global del cloud és la xarxa de centres de dades, regions i zones de disponibilitat que utilitzen els proveïdors de serveis al núvol (com AWS, Microsoft Azure o Google Cloud) per oferir serveis escalables, disponibles i segurs per tot el món.

Podem dir que es l'estructura física i lògica que permet als usuaris accedir a serveis de computació, emmagatzematge, bases de dades, xarxes, IA, etc., a través d'Internet, amb alta disponibilitat i redundància.

### 1.1. Components clau de la infraestructura global

Element	Descripció
<b>Regions (Regions)</b>	Àrees geogràfiques grans amb diversos centres de dades interconnectats.
<b>Zones de disponibilitat (AZs)</b>	Centres de dades físicament separats dins d'una regió. Permeten alta disponibilitat.
<b>Edge Locations</b>	Punts de presència propers als usuaris per millorar la latència (CDN, DNS, etc.).
<b>Backbone de xarxa</b>	Xarxa d'alta velocitat que interconnecta regions i zones globals.

### 1.2. Exemple real: Infraestructura de AWS

+33 regions al món (com París, Frankfurt, Singapur, São Paulo...)

Cada regió té 2-6 zones de disponibilitat (AZs)

+450 punts Edge per serveis de lliurament de continguts (Amazon CloudFront)

Parem ací, dins de cada regió tenim diverses zones de disponibilitat que fan precisament això: garantir la disponibilitat o, millor dit, la alta disponibilitat. La idea principal és la redundància per a garantir la disponibilitat i per tant la seguretat. Al remat és una manera d'organitzar els recursos.

### 1.3. Per què és important aquesta infraestructura?

- ✓ Alta disponibilitat. Si una zona cau, el trànsit es pot redirigir a una altra zona automàticament.
- ✓ Baixa latència. Els serveis estan més prop físicament dels usuaris finals.
- ✓ Compliment legal i sobirania de dades. Algunes dades no poden eixir d'un país o regió, aleshores la infraestructura regional permet el compliment.
- ✓ Escalabilitat global. Pots desplegar serveis a escala mundial en minuts.

### 1.4. Comparativa entre proveïdors:

Proveïdor	Regions	Zones de disponibilitat	Edge Locations
AWS	33+	100+	450+
Azure	60+	???	200+
Google Cloud	40+	100+	300+ (Cloud CDN + POPs)

Microsoft Azure té ??? en zones de disponibilitat, però sí que en té. Potser hi ha una mica de confusió sobre com s'organitzen.

Les zones de disponibilitat (Availability Zones) són ubicacions físiques separades dins d'una mateixa regió d'Azure. Cada zona té la seva pròpia alimentació elèctrica, refrigeració i xarxa, cosa que permet que les aplicacions siguin més resilient davant fallades locals.

Per què pot semblar que no n'hi ha? Hi ha algunes raons per les quals pot semblar que Azure no té zones de disponibilitat:

- No totes les regions tenen zones de disponibilitat: Algunes regions més xicotetes o més noves poden no tenir-les encara.
- No tots els serveis són compatibles amb zones de disponibilitat: Alguns serveis només estan disponibles a nivell regional.
- La terminologia pot confondre: Azure utilitza termes com "regions" i "conjunts de disponibilitat (availability sets)", que poden dur a confusió.

Exemple: La regió "West Europe" (Països Baixos) té zones de disponibilitat. Si desplegues una màquina virtual allà, pots escollir una zona específica (com la zona 1, 2 ó 3) per garantir alta disponibilitat.

## 2. Categories de Serveis

Si prenem com a exemple AWS, ofereix més de 200 serveis, classificats per funcionalitats. Ací tens les categories principals:

**2.1. Càlcul (Compute).** Per executar aplicacions, serveis o màquines virtuals.

- **Amazon EC2 – Màquines virtuals al núvol.** És un servei fonamental d'AWS que et permet llogar màquines virtuals (VMs) al núvol per executar aplicacions com si foren servidors físics.

Amazon EC2 et dona la capacitat de crear i gestionar instàncies de computació (servidors virtuals) de manera flexible, escalable i a demanda.

Característiques clau:

- Escalabilitat: Pots afegir o eliminar instàncies segons la càrrega.
- Personalització: Pots triar el sistema operatiu, CPU, memòria, disc, etc.
- Pagament per ús: Només pagues pel temps que utilitzes.

- Integració amb altres serveis AWS: Com S3 (emmagatzematge), RDS (bases de dades), IAM (seguretat), etc.

Exemple d'ús:

- Desplegar una web: Crear una instància EC2 amb Ubuntu, instal·lar Nginx i desplegar la teva web.
- Machine Learning: Utilitzar instàncies amb GPU per entrenar models.
- Backends d'aplicacions: Executar microserveis o APIs.

Tipus d'instàncies:

Tipus	Ús principal
t3.micro	Proves, webs petites
m5.large	Ús general
c6g.xlarge	Càlcul intensiu
p4d.24xlarge	Entrenament de models d'IA amb GPU

- **AWS Lambda – Codi sense servidor (serverless)**. És un servei de computació sense servidor (en anglès, serverless) proporcionat per Amazon Web Services (AWS). Et permet executar codi sense haver de gestionar ni mantenir cap servidor.

Com funciona? Escris el teu codi (en llenguatges com Python, Node.js, Java, etc.). El puges a AWS Lambda. Lambda executa aquest codi automàticament quan es produeix un esdeveniment (com ara la pujada d'un fitxer a S3, una petició HTTP, un missatge en una cua, etc.).

Característiques principals:

- Sense servidor: No cal preocupar-se per servidors, escalabilitat ni manteniment.
- Escalabilitat automàtica: Lambda escala segons la demanda.
- Pagament per ús: Només pagues pel temps que el teu codi s'executa (en mil·lisegons).
- Integració amb altres serveis d'AWS: Com S3, DynamoDB, API Gateway, CloudWatch, etc.

S'utilitza per a:

- Automatitzar processos (per exemple, processar imatges quan es pugen a S3).
- Crear backends d'aplicacions web o mòbils.
- Desenvolupar APIs sense servidor.
- Processament de dades en temps real.
- Crear notificacions, bots, o integracions entre serveis.

- **Amazon ECS (Elastic Container Service)**

Què és? Un servei de gestió de contenidors desenvolupat per AWS. Permet executar i escalar aplicacions en contenidors (Docker) de manera senzilla.

Característiques:

- Totalment gestionat per AWS.
- Pots usar-lo amb Fargate (sense gestionar servidors) o amb instàncies EC2.
- Integració profunda amb altres serveis d’AWS (IAM, CloudWatch, etc.).
- No requereix coneixements de Kubernetes.

Ideal per a usuaris que volen una solució senzilla i nativa d’AWS per executar contenidors.

#### - Amazon EKS (Elastic Kubernetes Service)

Què és? Un servei gestionat de Kubernetes. Kubernetes és l’orquestrador de contenidors més popular i de codi obert.

Característiques:

- AWS gestiona el pla de control de Kubernetes.
- Compatible amb eines i extensions de l’ecosistema Kubernetes.
- Més flexible i potent, però també més complex.
- Pots usar-lo amb Fargate o EC2.

Ideal per a equips que ja coneixen Kubernetes o volen aprofitar el seu ecosistema.

#### - Auto Scaling – Escalabilitat automàtica.

És una funcionalitat que permet augmentar o reduir automàticament el nombre d’instàncies (servidors virtuals) que tens en funcionament, segons la demanda de la teva aplicació.

Com funciona Auto Scaling? Defineixes una política: per exemple, si la CPU supera el 70% d’ús durant 5 minuts, afegeix una nova instància.

AWS Auto Scaling supervisa les teves instàncies (EC2, ECS, DynamoDB, etc.) i ajusta automàticament el nombre d’instàncies per mantenir el rendiment i optimitzar costos.

Característiques principals:

- Escalabilitat automàtica: puja o baixa el nombre de recursos segons la càrrega.
- Alta disponibilitat: assegura que sempre hi hagi prou recursos per atendre els usuaris.
- Estalvi de costos: evita tenir recursos innecessaris quan la demanda és baixa.
- Integració amb CloudWatch: per monitoritzar i activar accions segons mètriques.

Exemples d’ús:

- Una botiga en línia que rep més visites durant el Black Friday.

- Una aplicació mòbil que té pics d'ús a certes hores del dia.
- Un sistema de processament de dades que necessita més potència en hores punta.

## 2.2. Emmagatzematge (Storage).

Per guardar dades de forma segura i escalable.

### - Amazon S3 – Emmagatzematge d'objectes.

És un servei d'emmagatzematge al núvol que està dissenyat per oferir una emmagatzematge escalable, segur i altament disponible per a qualsevol tipus de dades, com ara fitxers, imatges, vídeos, còpies de seguretat, dades d'aplicacions, etc.

Característiques principals d'Amazon S3:

- Escalabilitat automàtica: pots començar amb poca capacitat i augmentar-la segons les teues necessitats, sense haver de fer cap canvi d'infraestructura.
- Alta disponibilitat i durabilitat: les dades es repliquen automàticament en diversos centres de dades per garantir-ne la seguretat i la disponibilitat.
- Control d'accés: pots definir qui pot accedir a quines dades mitjançant polítiques de permisos.
- Integració amb altres serveis AWS: com EC2, Lambda, CloudFront, etc.
- Pagament per ús: només pagues per l'espai i el trànsit que utilitzes.

Com funciona? Les dades a S3 s'organitzen en:

- Buckets: contenidors on es guarden els fitxers.
- Objectes: cada fitxer que pugues és un objecte, i pot tenir metadades associades.

Exemple d'ús típic: Una empresa pot utilitzar Amazon S3 per:

- Emmagatzemar còpies de seguretat de bases de dades.
- Servir imatges i vídeos d'un lloc web.
- Guardar fitxers generats per una aplicació mòbil.

- **Amazon EBS – Discos per EC2.** (Elastic Block Store) és un servei d'emmagatzematge de blocs proporcionat per Amazon Web Services (AWS). Està pensat per ser utilitzat conjuntament amb instàncies EC2 (servidors virtuals) i proporciona un emmagatzematge persistent, similar a un disc dur o SSD.

Característiques principals d'Amazon EBS:

- Emmagatzematge de blocs: a diferència de S3 (que és d'objectes), EBS emmagatzema dades en blocs, com un disc dur tradicional.
- Persistència: les dades es mantenen encara que l'instància EC2 es reinicie o es pare.



- Alt rendiment: ideal per a aplicacions que requereixen accés ràpid a dades, com bases de dades, sistemes de fitxers o aplicacions empresarials.
- Tipus de volums: pots triar entre diferents tipus (SSD, HDD) segons el rendiment i el cost que necessites.
- Snapshots: pots fer còpies de seguretat (snapshots) dels volums EBS i guardar-les a Amazon S3.

Com funciona? Crees un volum EBS. L'associes a una instància EC2. El sistema operatiu de l'instància el veu com un disc dur addicional. Pots llegir, escriure i formatar-lo com qualsevol altre disc.

Exemple d'ús típic:

- Una base de dades MySQL que corre en una instància EC2 pot utilitzar un volum EBS per emmagatzemar les seves dades.
- Pots fer snapshots regulars per tenir còpies de seguretat.

- **Amazon Glacier** – Emmagatzematge d'arxiu (cost molt baix).

És un servei d'emmagatzematge al núvol de baix cost dissenyat per a arxiu i còpies de seguretat a llarg termini. Forma part de la família de serveis Amazon S3, però està optimitzat per a dades que no es consulten sovint i que poden tolerar un temps d'espera per a la recuperació.

Característiques principals d'Amazon S3 Glacier:

- Cost molt baix: és molt més barat que altres tipus d'emmagatzematge, ideal per a dades que gairebé no es consulten.
- Recuperació flexible: pots triar entre diferents velocitats de recuperació:
- Expedited (ràpida): segons disponibilitat, en pocs minuts.
- Standard: en poques hores.
- Bulk: la més barata, però pot trigar fins a 12 hores.
- Alta durabilitat: les dades es repliquen automàticament en múltiples ubicacions dins d'una regió AWS.
- Seguretat: suport per a xifratge i control d'accés detallat.

Casos d'ús típics:

- Arxiu de documents legals o mèdics.
- Còpies de seguretat de sistemes antics.
- Conservació de dades per a compliment normatiu (com GDPR o HIPAA).
- Emmagatzematge de dades científiques o investigació que no es consulta sovint.

**2.3. Bases de dades (Databases).** Per gestionar dades estructurades, NoSQL, o en memòria.

**- Amazon RDS – Bases de dades relacionals (MySQL, PostgreSQL...).**

És un servei gestionat d’AWS que facilita la configuració, operació i escalat d’una base de dades relacional al núvol. Està pensat per estalviar temps i esforç en tasques com la instal·lació, manteniment, còpies de seguretat i actualitzacions de bases de dades.

Característiques principals d’Amazon RDS:

- Gestió automatitzada: AWS s’encarrega de les còpies de seguretat, actualitzacions de programari, monitoratge i recuperació automàtica.
- Alta disponibilitat: pots activar la configuració Multi-AZ per tenir rèpliques en diferents zones de disponibilitat.
- Escalabilitat: pots augmentar o reduir la capacitat de la base de dades fàcilment.
- Seguretat: suport per a xifratge, control d’accés amb IAM i integració amb VPC.
- Còpies de seguretat i snapshots: automàtiques o manuals, amb possibilitat de restauració puntual.

Motors de base de dades compatibles:

- MySQL
- PostgreSQL
- MariaDB
- Oracle
- Microsoft SQL Server
- Amazon Aurora (una base de dades pròpia d’AWS compatible amb MySQL i PostgreSQL)

Diferència amb altres serveis:

- RDS és per bases de dades relacionals.
- DynamoDB és per bases de dades NoSQL.
- Redshift és per anàlisi de dades massives (data warehousing).

**- Amazon DynamoDB – NoSQL.**

És un servei de base de dades NoSQL completament gestionat per AWS, dissenyat per oferir un rendiment alt i una latència molt baixa, fins i tot a gran escala. És ideal per a aplicacions que necessiten accés ràpid i flexible a grans volums de dades.

Característiques principals de DynamoDB:

- NoSQL: no utilitza taules relacionals com MySQL o PostgreSQL. Emmagatzema dades en taules amb elements i atributs, de manera flexible.
- Escalabilitat automàtica: pot gestionar milions de consultes per segon sense que hagi de preocupar-te per la infraestructura.
- Latència baixa: resposta en mil·lisegons, ideal per a aplicacions en temps real.
- Gestió totalment automatitzada: AWS s'encarrega de la replicació, seguretat, còpies de seguretat i escalat.
- Integració amb altres serveis AWS: com Lambda, API Gateway, IAM, etc.

Com s'organitzen les dades a DynamoDB?

- Taula: com una base de dades.
- Element: com una fila.
- Atributs: com columnes, però poden variar entre elements.
- Clau primària: pot ser simple (un sol atribut) o composta (partició + ordenació).

Diferència amb Amazon RDS

Característica	Amazon RDS (SQL)	Amazon DynamoDB (NoSQL)
Model de dades	Relacional (taules, SQL)	No relacional (clau-valor, documents)
Escalabilitat	Manual o automàtica	Totalment automàtica
Casos d'ús típics	ERP, CRM, aplicacions empresarials	Jocs, IoT, apps mòbils

- Amazon Aurora – DB alt rendiment compatible amb MySQL/PostgreSQL.

És un servei de base de dades relacional altament rendible i escalable creat per AWS, que combina el millor de les bases de dades comercials (com Oracle o SQL Server) amb la simplicitat i el cost de les bases de dades de codi obert (com MySQL i PostgreSQL).

Característiques destacades d'Amazon Aurora:

- Compatibilitat: pots triar entre dues versions: Aurora MySQL-compatible i Aurora PostgreSQL-compatible
- Rendiment superior: fins a 5 vegades més ràpid que MySQL i 3 vegades més ràpid que PostgreSQL en entorns similars.
- Alta disponibilitat i durabilitat: repliques automàtiques en múltiples zones de disponibilitat (Multi-AZ), amb recuperació automàtica.
- Escalabilitat automàtica: pots escalar la capacitat de lectura i escriptura fàcilment.
- Còpies de seguretat contínues: automàtiques i sense impacte en el rendiment.
- Seguretat integrada: xifratge en repòs i en trànsit, integració amb IAM i VPC.

Casos d'ús típics:

- Aplicacions empresarials que necessiten alta disponibilitat i rendiment.

- Migració de bases de dades MySQL/PostgreSQL locals al núvol.
- Aplicacions SaaS (Software as a Service).
- Sistemes financers o de comerç electrònic.

#### - Amazon ElastiCache – Caches (Redis, Memcached).

És un servei gestionat d'Amazon Web Services (AWS) que permet desplegar, operar i escalar memòries cau (caches) a la memòria, altament disponibles i de baixíssima latència, al núvol. Està pensat per millorar el rendiment d'aplicacions web i mòbils accelerant l'accés a dades freqüentment consultades.

Característiques principals:

- Compatibilitat amb Redis i Memcached: ElastiCache suporta dues tecnologies de memòria cau molt populars:
- Redis: amb funcionalitats avançades com persistència, replicació, snapshots, pub/sub, etc.
- Memcached: més simple i lleuger, ideal per a casos d'ús bàsics de cache.
- Alt rendiment: Les dades es guarden a la memòria RAM, cosa que permet temps de resposta molt ràpids (mil·lisegons o menys).
- Escalabilitat: Pots escalar horitzontalment (afegint més nodes) o verticalment (amb instàncies més potents).
- Alta disponibilitat i recuperació automàtica: Amb suport per a clústers multi-AZ (zones de disponibilitat), failover automàtic i backups.
- Integració amb altres serveis AWS: Com ara Amazon RDS, Lambda, EC2, etc.

#### 2.4. Xarxa i CDN (Networking & Content Delivery).

Per a connectar i distribuir recursos.

#### - Amazon VPC – Xarxa privada virtual.

És un servei d'Amazon Web Services (AWS) que et permet crear una xarxa virtual privada dins del núvol d'AWS, de manera molt semblant a una xarxa tradicional que podries tenir en un centre de dades físic. Amazon VPC és com una xarxa privada i segura dins d'AWS on pots desplegar els teus recursos (com servidors, bases de dades, etc.) amb control total sobre la seva configuració de xarxa.

Característiques principals:

- Aïllament: Cada VPC està aïllada de la resta, com si fos una xarxa privada.
- Subxarxes (subnets): Pots dividir la VPC en subxarxes públiques i privades.
- Control de trànsit: Mitjançant taules de rutes, ACLs (l·listes de control d'accés) i grups de seguretat.

- Connexió amb Internet: Pots afegir una Internet Gateway per permetre accés públic, o una NAT Gateway per permetre que recursos privats accedeixin a Internet sense ser accessibles des de fora.
- Connexió amb la teua xarxa local: Mitjançant VPN o AWS Direct Connect.

Exemple pràctic: Suposa que tens una aplicació web. Pots crear una VPC amb:

- Una subxarxa pública per al servidor web (accessible des d'Internet).
- Una subxarxa privada per a la base de dades (no accessible des de fora).
- Regles de seguretat que només permetin connexions segures i controlades.

- **Amazon CloudFront** – Xarxa de distribució de continguts (CDN).

El seu objectiu és lliurar contingut (com pàgines web, vídeos, imatges, fitxers, etc.) de manera ràpida, segura i fiable als usuaris d'arreu del món. CloudFront accelera la càrrega de contingut web distribuint-lo a servidors pròxims als usuaris.

Com funciona? Distribució global: CloudFront utilitza una xarxa de punts de presència (PoPs) repartits per tot el món. Quan un usuari fa una petició (per exemple, per veure una imatge o un vídeo), si el contingut ja està a prop (en un PoP), es lliura immediatament. Si no, es recupera de l'origen (com S3, EC2 o un servidor web) i es guarda temporalment al PoP per a futures peticions. Amb açò, es millora el rendiment i es redueix la latència i la càrrega sobre els servidors d'origen.

Altres avantatges:

- Seguretat: Suporta HTTPS, integració amb AWS Shield i AWS WAF per protegir contra atacs.
- Control d'accés: Pots restringir qui pot veure el teu contingut.
- Integració amb altres serveis AWS: Com Amazon S3, EC2, Elastic Load Balancing, etc.

Casos d'ús típics:

- Lliurament de llocs web estàtics o dinàmics.
- Streaming de vídeo o àudio.
- Acceleració d'APIs.
- Distribució de programari o actualitzacions.

- **Elastic Load Balancing (ELB)** – Balanceig de càrrega.

Distribueix automàticament el trànsit entrant d'aplicacions entre múltiples instàncies (com EC2), per garantir alta disponibilitat, escalabilitat i tolerància a fallades. ELB actua com un "repartidor de trànsit": quan molts usuaris accedeixen a la teva aplicació, ELB reparteix les peticions entre diversos servidors perquè cap d'ells es col·lapse.

Tipus d'ELB:

### *Application Load Balancer (ALB)*

- Ideal per a aplicacions web (nivell 7 – HTTP/HTTPS).
- Pot fer routing basat en URL, capçaleres, cookies, etc.
- Ex: /fotos va a un servidor, /vídeos a un altre.

### *Network Load Balancer (NLB)*

- Per a trànsit de xarxa molt ràpid i de baix nivell (nivell 4 – TCP/UDP).
- Ideal per a aplicacions amb requisits de rendiment molt alts.

### *Gateway Load Balancer (GWLb)*

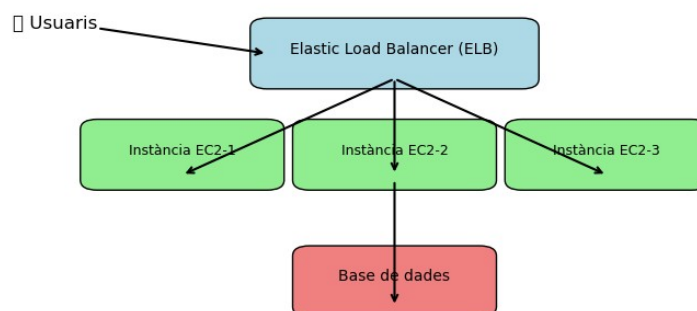
- Per a serveis de tercers com tallafocs, inspecció de trànsit, etc.

### *Classic Load Balancer (CLB)*

- Versió més antiga, suporta trànsit HTTP/HTTPS i TCP.
- Encara es fa servir en sistemes antics, però es recomana usar ALB o NLB.

#### Beneficis:

- Alta disponibilitat: Si un servidor falla, ELB redirigeix el trànsit a altres que funcionin.
- Escalabilitat automàtica: Funciona bé amb Auto Scaling.
- Monitoratge i seguretat: Integració amb CloudWatch, certificats SSL, i grups de seguretat.



#### Explicació del diagrama:

- Usuaris: Fan peticions a la teua aplicació des tot el món.

- Elastic Load Balancer (ELB): Rep les peticions i les distribueix de manera intel·ligent entre les instàncies disponibles.
- Instàncies EC2: Són els servidors que processen les peticions. ELB reparteix la càrrega entre elles.
- Base de dades: Les instàncies EC2 poden consultar o escriure dades a la base de dades, que normalment està en una subxarxa privada.

*2. 5. Seguretat, identitat i compliment (Security, Identity & Compliance).* Per a gestionar l'accés i seguretat.

- **AWS IAM** – Control d'accés d'usuaris i rols.

És un servei d'Amazon Web Services que et permet gestionar de manera segura l'accés als recursos d'AWS. Amb IAM pots controlar qui pot fer què dins del teu entorn AWS. IAM és el sistema de permisos d'AWS. Et permet definir qui pot accedir als teus serveis i què poden fer.

Què pots fer amb IAM?

- Crear usuaris i grups: Per a persones o aplicacions que necessiten accedir a AWS.
- Assignar permisos: Mitjançant polítiques que defineixen accions permeses (com llegir un fitxer S3, iniciar una instància EC2, etc.).
- Controlar l'accés a serveis específics: Per exemple, pots permetre que un usuari només pugui veure informes a CloudWatch, però no modificar res.
- Autenticació multifactor (MFA): Per afegir una capa extra de seguretat.
- Rols IAM: Per permetre que serveis d'AWS (com Lambda o EC2) actuïn amb permisos específics.

Exemple pràctic:

Suposa que tens un desenvolupador que només ha de gestionar instàncies EC2. Pots crear un usuari IAM per ell i assignar-li una política que només li permeti accedir a EC2, però no a S3, RDS, etc.

Beneficis:

- Seguretat millorada: Control detallat sobre qui pot accedir a què.
- Gestió centralitzada: Tot l'accés es controla des d'un sol lloc.
- Compliment normatiu: Ajuda a seguir bones pràctiques i regulacions.

- **AWS KMS** – Gestió de claus criptogràfiques.

És un servei que permet crear i gestionar de manera centralitzada les claus de xifratge utilitzades per a protegir les dades. Amb AWS KMS, pots generar, importar, rotar i administrar claus de xifratge per a garantir la confidencialitat i integritat de la informació emmagatzemada en el núvol.

Funcionalitats clau d'AWS KMS:

- Creació de claus: Permet generar claus mestres i claus de dades per protegir recursos.
- Gestió centralitzada: Facilita l'administració de claus i l'aplicació de polítiques de seguretat.
- Integració amb altres serveis: Es pot utilitzar amb serveis com S3, EBS, RDS i Redshift per xifrar dades en repòs i en trànsit

- **AWS Shield & WAF** – Protecció contra atacs (DDoS, etc.).

Són serveis de seguretat que protegeixen les aplicacions web contra amenaces en línia.

AWS Shield és un servei de protecció contra atacs de denegació de servei distribuïts (DDoS). Té dues versions: AWS Shield Standard i Advanced.

AWS WAF (Web Application Firewall)

AWS WAF és un firewall d'aplicacions web que permet supervisar i controlar el trànsit HTTP/HTTPS cap a les aplicacions. Protegeix contra amenaces com:

- Injecció SQL
- Cross-site scripting (XSS)
- Bloqueig d'IP sospitoses
- Protecció contra bots maliciosos

AWS WAF es pot integrar amb serveis com Amazon CloudFront, Application Load Balancer i API Gateway per reforçar la seguretat de les aplicacions web.

**2.6. Monitoratge i gestió (Monitoring & Management).** Per supervisar, automatitzar i controlar els recursos.

- **Amazon CloudWatch** – Logs, mètriques i alarmes.

És un servei de supervisió i observabilitat que permet monitoritzar recursos i aplicacions en temps real. Amb CloudWatch, pots recopilar i analitzar mètriques, configurar alarmes i automatitzar accions per optimitzar el rendiment dels teus sistemes.

Funcionalitats principals d'Amazon CloudWatch

- Supervisió en temps real: Recull dades sobre el rendiment de les aplicacions i recursos d'AWS.
- Configuració d'alarmes: Permet establir alertes per respondre a canvis en el sistema.
- Automatització d'accions: Pot activar accions automàtiques quan es detecten anomalies.
- Anàlisi de registres: Facilita la detecció de problemes mitjançant l'anàlisi de logs.

CloudWatch és útil per a DevOps, administradors de sistemes i desenvolupadors que necessiten una visió clara del rendiment i estat operatiu dels seus serveis en AWS.



## - AWS CloudTrail – Registre d'activitats i auditories.

És un servei que permet registrar i supervisar l'activitat dels usuaris i l'ús de les API dins d'AWS. És essencial per a la governança, auditoria, seguretat i compliment normatiu en entorns AWS.

- Funcionalitats principals d'AWS CloudTrail
- Registre d'activitat: Captura accions realitzades per usuaris, rols i serveis dins d'AWS.
- Historial d'esdeveniments: Permet consultar els últims 90 dies d'activitat sense cost addicional.
- Integració amb Amazon Athena: Facilita l'anàlisi de registres amb SQL per detectar activitats sospitoses.

### Beneficis d'AWS CloudTrail

- Millora la seguretat: Identifica accessos no autoritzats i activitats inusuals.
- Facilita el compliment normatiu: Ajuda a demostrar la conformitat amb regulacions com SOC, PCI i HIPAA.
- Optimitza les operacions: Permet depurar problemes i investigar incidències operatives.

- **CloudTrail Lake**: Emmagatzema i analitza esdeveniments per a auditories i investigacions de seguretat.

És una funcionalitat avançada dins d'AWS CloudTrail que permet emmagatzemar, analitzar i auditar esdeveniments de manera eficient. Aquesta eina converteix els esdeveniments en un format optimitzat per a consultes ràpides i permet executar SQL-based queries per analitzar l'activitat dins d'AWS.

### Característiques principals de CloudTrail Lake

- Emmagatzematge a llarg termini: Permet conservar esdeveniments fins a 10 anys per a auditories i anàlisis de seguretat.
- Format optimitzat: Converteix els esdeveniments en Apache ORC, un format columnar que millora la velocitat de recuperació de dades.
- Selecció avançada d'esdeveniments: Permet definir criteris per emmagatzemar només els esdeveniments rellevants.
- Execució de consultes SQL: Facilita la cerca i anàlisi de registres per detectar anomalies o investigar incidents de seguretat.
- Integració amb AWS Glue i Amazon Athena: Permet federar dades i executar consultes avançades.

CloudTrail Lake és especialment útil per a auditories de seguretat, compliment normatiu i detecció de comportaments sospitosos dins d'AWS.

## - AWS Config – Historial i conformitat de configuracions.

Services (AWS) que permet supervisar, auditar i avaluar les configuracions dels recursos dins d'AWS. Ajuda a gestionar els canvis en la configuració, garantir el compliment de les polítiques i simplificar la resolució de problemes operatius.

### Funcionalitats principals d'AWS Config

- Monitorització contínua: Registra canvis en la configuració dels recursos AWS.
- Auditoria i compliment: Avalua si els recursos compleixen les polítiques de seguretat i governança.
- Historial de configuració: Permet veure com han canviat les configuracions al llarg del temps.
- Integració amb altres serveis: Es complementa amb AWS CloudTrail per correlacionar canvis amb accions d'usuaris.

### Beneficis d'AWS Config

- Millora la seguretat: Detecta configuracions incorrectes que podrien comprometre la infraestructura.
- Facilita el compliment normatiu: Ajuda a complir regulacions com GDPR, HIPAA i PCI-DSS.
- Optimitza la gestió de recursos: Permet entendre la relació entre diferents recursos i la seva configuració.

## 2.7. Machine Learning i IA.

Serveis per crear i entrenar models d'intel·ligència artificial.

## - Amazon SageMaker – Desenvolupament de models ML.

Permet crear, entrenar i desplegar models de machine learning (ML) de manera ràpida i segura. És una plataforma unificada per a dades, anàlisi i intel·ligència artificial (IA), dissenyada per simplificar el procés de desenvolupament de models d'aprenentatge automàtic.

### Funcionalitats principals d'Amazon SageMaker

- Entrenament i desplegament de models ML: Permet entrenar models amb grans volums de dades i desplegar-los en entorns escalables.
- Automatització del machine learning: Inclou eines com SageMaker Autopilot, que automatitza la selecció d'algoritmes i l'entrenament de models.
- Preparació de dades: Amb SageMaker Data Wrangler, facilita la neteja i transformació de dades per a l'entrenament de models.
- Inferència optimitzada: Permet desplegar models amb costos reduïts i alta eficiència.

- Integració amb altres serveis AWS: Es connecta amb Amazon S3, AWS Lambda, Amazon Redshift, entre altres.

#### Beneficis d'Amazon SageMaker

- Redueix la complexitat del ML: Automatitza tasques repetitives i simplifica el flux de treball.
- Escalabilitat i flexibilitat: Permet entrenar models amb grans volums de dades i desplegar-los en entorns distribuïts.
- Seguretat i governança: Ofereix eines per gestionar l'accés i la protecció de dades.

#### - Amazon Rekognition – Anàlisi d'imatges i vídeos.

És un servei d'Amazon Web Services (AWS) que utilitza intel·ligència artificial (IA) i machine learning (ML) per analitzar imatges i vídeos. Permet reconèixer objectes, persones, text, activitats i contingut inadequat de manera automatitzada.

#### Funcionalitats principals d'Amazon Rekognition

- Detecció de rostres: Identifica i analitza característiques facials com ulls oberts, ulleres o expressions.
- Comparació de rostres: Compara imatges per verificar identitats.
- Detecció d'objectes i escenes: Identifica elements com vehicles, animals, edificis, etc.
- Reconeixement de text: Extreu text de cartells, publicacions en xarxes socials i embalatges.
- Moderació de contingut: Detecta imatges i vídeos amb contingut inadequat.
- Reconeixement de celebritats: Identifica persones conegudes en imatges i vídeos.
- Anàlisi de vídeos: Detecta segments clau com crèdits, fotogrames negres i transicions.

#### Beneficis d'Amazon Rekognition

- Automatització de processos: Redueix el temps i el cost de l'anàlisi manual.
- Escalabilitat: Processa milions d'imatges i vídeos en segons.
- Integració amb altres serveis AWS: Compatible amb Amazon S3, Lambda, i altres serveis.

#### - Amazon Comprehend – Processament de llenguatge natural.

Processament de llenguatge natural (NLP) i machine learning (ML) per analitzar i extreure informació de textos no estructurats.

#### Funcionalitats principals d'Amazon Comprehend

- Anàlisi de sentiments: Detecta si un text té un to positiu, negatiu, neutre o mixt.

- **Reconeixement d'entitats:** Identifica noms de persones, llocs, organitzacions i dates en un text.
- **Extracció de frases clau:** Detecta conceptes rellevants dins d'un document.
- **Identificació de l'idioma:** Determina l'idioma predominant en un text.
- **Classificació de documents:** Categoritza textos segons temes predefinits o personalitzats.
- **Detecció de relacions entre paraules:** Analitza connexions entre termes dins d'un document.

#### Beneficis d'Amazon Comprehend

- **Automatització de l'anàlisi de textos:** Redueix el temps i l'esforç necessari per processar grans volums de dades textuais.
- **Escalabilitat:** Pot analitzar milions de documents de manera eficient.
- **Integració amb altres serveis AWS:** Compatible amb Amazon S3, Lambda, DynamoDB, entre altres.

Amazon Comprehend és útil per a atenció al client, anàlisi de xarxes socials, processament de documents legals i financers, entre altres aplicacions.

### *2.8. DevOps i eines de desenvolupament.*

- **AWS CodePipeline, CodeBuild, CodeDeploy** – Integració i desplegament continu.

AWS ofereix tres serveis clau per a la integració i desplegament continu (CI/CD): AWS CodePipeline, AWS CodeBuild i AWS CodeDeploy. Aquests serveis automatitzen el procés de desenvolupament, prova i desplegament d'aplicacions.

#### *AWS CodePipeline*

- És un servei de gestió de flux de treball per a CI/CD.
- Automatitza el procés de compilació, prova i desplegament de codi.
- Permet integrar-se amb serveis com GitHub, AWS CodeCommit i Jenkins.
- Facilita la implementació de canvis de codi de manera ràpida i segura.

#### *AWS CodeBuild*

- És un servei de compilació de codi completament gestionat.
- Compila el codi font, executa proves i genera paquets de programari llestos per al desplegament.
- No requereix la gestió de servidors de compilació.
- Escala automàticament per satisfer les necessitats de compilació.

#### *AWS CodeDeploy*

- Automatitza el desplegament d'aplicacions en Amazon EC2, AWS Fargate, AWS Lambda i servidors locals.
- Admet estratègies de desplegament com blue/green i rolling updates.
- Redueix el temps d'inactivitat i minimitza errors en el desplegament.

Aquests serveis treballen junts per oferir una pipeline CI/CD completa, millorant l'eficiència i la seguretat en el desenvolupament d'aplicacions en AWS. Pots trobar més informació a

- **CloudFormation** – Infraestructura com a codi (IaC).

Permet modelar, aprovisionar i gestionar recursos d'infraestructura com a codi (IaC). Amb CloudFormation, pots definir tota la teva infraestructura en plantilles JSON o YAML, facilitant la creació i gestió de recursos de manera automatitzada

Funcionalitats principals d'AWS CloudFormation

- Infraestructura com a codi (IaC): Permet definir i desplegar recursos AWS mitjançant plantilles.
- Automatització del desplegament: Redueix errors manuals i accelera la configuració de sistemes.
- Gestió de dependències: Administra la creació i eliminació de recursos en l'ordre correcte.
- Escalabilitat i replicació: Facilita la replicació d'infraestructures en diferents regions AWS.

Beneficis d'AWS CloudFormation

- Simplificació de la gestió: Permet administrar múltiples recursos com una sola unitat.
- Reutilització de plantilles: Facilita la replicació d'entorns amb configuracions consistents.
- Control de versions: Permet rastrejar i revertir canvis en la infraestructura.

Taula resum:

<b>Categoria</b>	<b>Exemple destacat</b>	<b>Funció principal</b>
Càlcul	EC2, Lambda	Executar aplicacions i serveis
Emmagatzematge	S3, EBS, Glacier	Guardar fitxers i dades
Bases de dades	RDS, DynamoDB	Gestió de dades estructurades
Xarxa i CDN	VPC, CloudFront	Connexió i distribució global
Seguretat	IAM, KMS, Shield	Control i protecció d'accés
Monitoratge	CloudWatch, CloudTrail	Seguiment i alarmes
Machine Learning	SageMaker, Rekognition	IA i anàlisi avançada

Categoria	Exemple destacat	Funció principal
DevOps	CodePipeline, IaC	Automatització i desplegament

I un video explicatiu: <https://youtu.be/8OKfNHciBNg?si=w9mCspzbKOrbtouE>

### 3. Exploració de la Consola d'Administració

En el cas d'AWS la consola d'administració és la interfície web que permet accedir i gestionar els serveis AWS.

Mira aquest vídeo: <https://youtu.be/mvvsTKidGgM?si=fX8KvSrJHHh8jZum>

Però, què és la Consola d'Administració d'AWS? És una plataforma basada en web on pots:

- Crear i administrar instàncies de servidors virtuals (EC2)
- Emmagatzemar dades (S3)
- Configurar bases de dades (RDS, DynamoDB)
- Controlar usuaris i permisos (IAM)
- Fer seguiment del consum i costos
- Automatitzar desplegaments i molt més

#### Exploració pas a pas de la consola

1. Inici de sessió

2. Panell principal (Dashboard). Un cop dins, veuràs:

- Barra de cerca: Serveix per trobar ràpidament serveis com "EC2", "S3", etc.
- Recentment utilitzats: Mostra serveis que has usat últimament.
- Accés ràpid a serveis destacats.

3. Serveis clau que pots explorar

Ací tens alguns serveis que pots investigar dins la consola:

Servei	Descripció	Ús típic
<b>EC2</b>	Servidors virtuals	Hosting de webs o aplicacions
<b>S3</b>	Emmagatzematge d'objectes	Guardar fitxers, backups
<b>RDS</b>	Bases de dades relacionals	MySQL, PostgreSQL gestionats
<b>Lambda</b>	Funcions serverless	Executar codi sense servidors

Servei	Descripció	Ús típic
<b>IAM</b>	Gestió d'usuaris i permisos	Seguretat i accés controlat
<b>CloudWatch</b>	Monitorització i alertes	Seguiment del rendiment
<b>CloudFormation</b>	Infraestructura com a codi	Automatitzar entorns

#### 4. Funcionalitats útils

- Billing (Facturació): per controlar els costos mensuals.
  - Regions: pots canviar la regió des del menú superior dret (important per disponibilitat i latència).
  - Support: accés al centre de suport d'AWS.
-

## Tema 4: Mesures bàsiques de seguretat al núvol

---



- 
1. *Justificació*
  2. *Model de responsabilitat compartida*
  3. *Gestió d'accessos (IAM – Identity & Access Management)*
  4. *Protecció de dades*
  5. *Conformitat*
  6. *Gestió d'accessos*



## 1. Justificació

Són essencials per garantir la confidencialitat, integritat i disponibilitat de les dades i serveis. Aquestes mesures parteixen del model de responsabilitat compartida, i es basen en bones pràctiques com la gestió d'accessos i la protecció de dades.

## 2. Model de responsabilitat compartida

El Model de Responsabilitat Compartida d'AWS és un principi fonamental que defineix qui és responsable de què en termes de seguretat i compliment normatiu quan utilitzes els serveis en el núvol d'AWS.

En què consisteix? AWS és responsable de la "Seguretat del Núvol" (Security of the Cloud). AWS gestiona i protegeix la infraestructura física i la capa d'infraestructura:

- Centres de dades
- Servidors
- Xarxes
- Hardware
- Virtualització

El client (tu) és responsable de la "Seguretat en el Núvol" (Security in the Cloud). Tu, com a usuari d'AWS, has de protegir i gestionar els teus recursos i dades a nivell lògic i d'aplicacions:

- Configuració dels serveis (ex. VPC, Security Groups)
- Gestió d'usuaris i permisos (IAM)
- Xifrat de dades
- Monitorització i auditoria
- Seguretat d'aplicacions i sistemes operatius
- Compliment de polítiques internes

Aspecte	AWS (Proveïdor)	Client (Usuari)
Infraestructura física	Centre de dades, servidors, xarxa	No la gestiona
Hardware i virtualització	Gestió i manteniment	No la gestiona
Sistemes operatius	Gestió per serveis gestionats (ex. Lambda)	Gestió quan s'usen serveis autogestionats
Configuració de xarxa	No	VPC, subxarxes, taules de rutes, SG
Control d'identitat	No	IAM, polítiques, MFA
Dades i aplicacions	No	Emmagatzematge, còpia de

Entendre aquest model t'ajuda a:

- Saber quines parts depenen d'AWS i quines d'ara en endavant tu has de gestionar
- Evitar problemes de seguretat per configuracions errònies o falta de control
- Complir amb normatives i bones pràctiques

El Model de Responsabilitat Compartida és un concepte extensible a altres proveïdors de núvol, no només a AWS. Tot i que cada proveïdor pot tenir matisos o variacions en la seua implementació, però la idea bàsica és la mateixa.

### 3 Gestió d'accessos (IAM – Identity & Access Management)

És un sistema de gestió d'identitats i permisos que et permet:

- Crear usuaris, grups i rols amb permisos específics
- Assignar polítiques (permissions) que defineixen exactament quins recursos poden accedir i amb quins drets (lectura, escriptura, administració, etc.)
- Gestionar l'autenticació i autorització dins d'AWS
- Integrar amb serveis d'identitat externs (ex: Active Directory, SAML, OpenID Connect)

Components principals:

Component	Descripció
<b>Usuari IAM</b>	Identitat d'una persona o aplicació que accedeix a AWS
<b>Grup IAM</b>	Conjunt de usuaris amb permisos comuns
<b>Rol IAM</b>	Identitat amb permisos, per ser assumida per usuaris o serveis
<b>Política</b>	Document JSON que especifica permisos detallats (qui pot fer què)
<b>MFA</b>	Autenticació de múltiples factors per més seguretat

Per què és important IAM?

- Aplica el principi de mínim privilegi: només dones els permisos necessaris
- Protegeix recursos crítics evitant accessos no autoritzats
- Permet auditar i controlar l'activitat dins del teu entorn AWS
- És la base per a la seguretat en la gestió de recursos i dades

Exemple pràctic: Suposa que tens un equip de desenvolupament

- Crea un grup “Desenvolupadors” amb permisos per desplegar i modificar recursos dins d’una VPC
- Dona a cada desenvolupador un usuari IAM amb MFA activat
- Si necessiten executar un servei específic que accedeix a S3, els dones un rol que poden “assumir” per accedir-hi amb permisos restringits

Exemples de serveis IAM en altres núvols

- AWS IAM,
- Azure Active Directory (Azure AD)
- Google Cloud IAM

## 4. Protecció de dades

La protecció de comptes i dades a AWS és essencial per mantenir la teua infraestructura segura i resilient. AWS proporciona moltes eines i bones pràctiques per evitar accessos no autoritzats, pèrdues de dades i vulnerabilitats.

### ***Protecció del compte AWS***

1. No utilitzis el compte root per al dia a dia. El compte root és el compte principal que es crea quan configures AWS. Només hauria de fer servir per a tasques crítiques (ex: configuració inicial, recuperació de compte). Activa MFA (Multi-Factor Authentication) immediatament per aquest compte.
2. Activa MFA per a tots els usuaris IAM. MFA afegeix una capa extra de seguretat (com Google Authenticator, clau física, etc.).
3. Utilitza IAM per crear usuaris i rols. Assigna només els privilegis mínims necessaris (principi de least privilege). Usa grups IAM per facilitar la gestió de permisos
4. Revisa i gestiona l'accés regularment. Utilitza IAM Access Analyzer i AWS Trusted Advisor per identificar permisos excessius o mal configurats. Desactiva comptes inactius o claus d'accés antigues

### ***Protecció de les dades***

5. Xifra les dades en repòs i en trànsit.

A AWS, pots xifrar:

- Dades en repòs a S3, EBS, RDS, DynamoDB, etc.
- Dades en trànsit amb HTTPS/TLS

Utilitza AWS KMS (Key Management Service) per gestionar les claus de xifrat

## 6. Restringeix l'accés a buckets S3

- Evita fer-los públics tret que siga necessari
- Utilitza bucket policies i IAM policies per controlar qui pot llegir/escriure
- Activa S3 Block Public Access

## 7. Fes còpies de seguretat regulars

- Automatitza backups amb AWS Backup, Snapshots o funcions pròpies del servei (RDS, DynamoDB...)
- Revisa polítiques de retenció i recuperació de dades

## 8. Utilitza serveis de seguretat gestionats

- AWS Shield: defensa contra atacs DDoS
- AWS WAF: firewall d'aplicacions web per filtrar trànsit maliciós
- AWS GuardDuty: monitorització d'amenaques basada en IA
- AWS Macie: detecció de dades sensibles (com NIFs, correus, etc.)

## ***Monitorització i resposta***

### 9. Registra l'activitat amb AWS CloudTrail

- Registra totes les accions (API calls) que es fan al compte
- És clau per fer auditories, detecció d'anomalies o resposta a incidents

### 10. Configura alertes amb Amazon CloudWatch

- Monitora esdeveniments inusuals (ex: accés des de IPs desconegudes)
- Actua automàticament (ex: deshabilita un accés, envia notificació, etc.)

## **5. Conformitat**

Conformitat (Compliance). Si parlem d'AWS podem dir que té un ampli catàleg de certificacions de seguretat i conformitat que poden ajudar la teva organització a complir amb requisits legals, normatius i industrials.

Exemples de marcs i certificacions que AWS compleix:

- ISO 27001, 27017, 27018 – Gestió de seguretat de la informació i privadesa al núvol
- SOC 1, SOC 2, SOC 3 – Controls sobre serveis (seguretat, disponibilitat, confidencialitat)
- GDPR (UE) – Protecció de dades personals
- HIPAA (EUA) – Protecció de dades mèdiques

- PCI DSS – Seguretat per pagaments amb targeta
- FedRAMP, ENS, C5, etc. – Compliment amb normatives governamentals

Pots consultar totes les certificacions actuals a AWS Artifact, un servei que et permet accedir als informes i certificacions oficials.

## 6. Gestió d'accessos

La gestió d'accessos a AWS és el conjunt d'eines i pràctiques que et permeten controlar qui pot accedir als teus recursos a AWS, amb quins permisos, i en quines condicions. És un dels pilars fonamentals de la seguretat al núvol.

Objectius de la gestió d'accessos

- Autenticar correctament qui entra al teu compte (usuari, aplicació, servei)
- Autoritzar què pot fer dins d'AWS (ex: llegir dades, crear recursos, esborrar)
- Auditar i monitoritzar els accessos
- Assegurar-te que s'aplica el principi de mínim privilegi

Components clau a AWS

1. IAM (Identity and Access Management)

2. AWS Organizations. Permet gestionar múltiples comptes AWS de manera centralitzada.

Inclou:

- Polítiques de servei (SCPs) que limiten els permisos a nivell d'organització
- Consolidació de facturació i gestió de permisos transversals

3. Control d'accés basat en recursos. Molts serveis (ex: S3, Lambda, SNS, etc.) permeten afegir polítiques directament al recurs. Per exemple: una política de bucket S3 pot permetre només l'accés des d'una VPC específica o des d'un rol determinat.

4. Autenticació multifactor (MFA)

- Es pot requerir MFA per a l'accés a la consola
- També pots exigir-la per a accions crítiques (com esborrar recursos)

5. Federació d'identitat

Integra usuaris d'un sistema extern (com Microsoft AD, Google Workspace, Okta, etc.)

Usuaris federats poden obtenir accés temporal mitjançant rols IAM i SAML o OIDC

### ***Millors pràctiques***

- No utilitzis el compte root per a tasques habituals
  - Assigna només els permisos necessaris
  - Revisa els permisos amb IAM Access Analyzer
  - Activa CloudTrail per registrar qui fa què
  - Usa tags (etiquetes) per aplicar permisos per projectes, departaments o entorns
-

## Tema 5: Xarxes i lliurament de continguts

---



- 
1. Xarxes en AWS
  2. Configuració de Xarxa Virtual (VPC a AWS)
  3. Seguretat a les xarxes i disseny d'arquitectures
  4. Serveis d'encaminament i distribució de contingut
    - 4.1. Amazon Route 53 – Servei de DNS altament disponible
    - 4.2. Amazon CloudFront – Content Delivery Network (CDN)
    - 4.3. Elastic Load Balancing (ELB) – Repartiment del tràfic
    - 4.4. AWS Global Accelerator
    - 4.5. Altres serveis relacionats
    - 4.6. Tot això, combinat, assegura

## 1. Xarxes en AWS

Les xarxes en AWS són fonamentals per connectar, protegir i escalar aplicacions al núvol. AWS ofereix una infraestructura de xarxa molt configurable mitjançant Amazon VPC (Virtual Private Cloud) i diversos serveis relacionats. VPC és un servei d'AWS que et permet crear una xarxa virtual privada dins del núvol d'AWS. Aquesta xarxa està aïllada lògicament de la resta de la infraestructura de núvol d'AWS, i pots configurar-la com si fora una xarxa pròpia dins del teu centre de dades.

Imagina que tens una aplicació web. Pots configurar una subxarxa pública per als servidors web accessibles des d'internet. Una subxarxa privada per a la base de dades o serveis interns, sense accés directe des de fora. Tot això passa dins de la teva VPC, amb les configuracions de seguretat i xarxa que tu necessites.

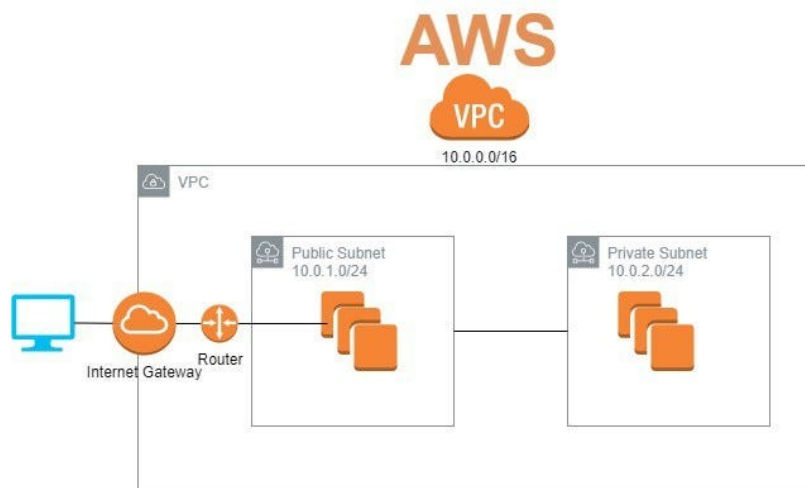
## 2. Configuració de Xarxa Virtual (VPC a AWS)

Una VPC (Virtual Private Cloud) és una xarxa virtual que pots configurar dins d'AWS, aïllada lògicament.

Elements clau d'una VPC:

- **Subxarxes** (Subnets):

- Públiques: tenen accés directe a Internet.
- Privades: no tenen accés directe a Internet.



- **Internet Gateway** (IGW): És la porta d'enllaç d'internet. Permet connexions entre instàncies de la VPC i Internet.

- **Route Tables** (taules de rutes): En una VPC (Virtual Private Cloud) d'AWS són un component clau que controla com es dirigeix el trànsit de xarxa dins de la VPC i cap a fora (com Internet, altres VPCs, xarxes locals, etc.).

Una route table és una llista de regles de routing (anomenades rutes) que indiquen on ha d'anar el trànsit de xarxa segons l'adreça IP de destinació. Cada Route Table conté:



- Rutes → Cada ruta defineix: Un rang de destinació (ex: 0.0.0.0/0, 10.0.1.0/24, etc.)
- Un objectiu (target) cap on s'ha d'enviar el trànsit (ex: Internet Gateway, NAT Gateway, instància, peering connection...)
- Subxarxes associades → Cada subxarxa d'una VPC ha d'estar associada a una Route Table (implícita o explícita)

Exemples de rutes habituals:

Destinació	Objectiu	Significat
10.0.0.0/16	local	Trànsit dins la VPC
0.0.0.0/0	Internet Gateway	Eixida a Internet
0.0.0.0/0	NAT Gateway	Eixida a Internet des d'una subxarxa privada

- **NAT Gateway:** permet que les instàncies en subxarxes privades puguin accedir a Internet (per exemple, per actualitzar-se) sense exposar-se públicament.

- **Security Groups i NACLs:** Llistes de control d'accés a la xarxa. Controlen el tràfic a nivell d'instància i subxarxa, respectivament.

Les NACL són com agents de duanes, contolen qui entra i que ix contstant paquets i llistes.

Per altra banda, a nivell d'instància EC2 tenim grups de seguretat. Són com el porter d'una finca. Controlen qui pot entrar i deixen eixir a tothom.

### 3. Seguretat a les xarxes i disseny d'arquitectures

La seguretat en xarxes es basa en segmentació, xifratge, control d'accés i monitorització.

Podem establir, amb caràcter general, recomanacions o bones pràctiques:

- Dividir recursos entre subxarxes públiques i privades.
- Ús de Security Groups per filtrar tràfic a nivell d'instància.
- Activar logs de tràfic (VPC Flow Logs).
- Xifratge de dades en trànsit (TLS) i en repòs.
- Utilitzar IAM i polítiques de mínim privilegi.
- Integració amb AWS WAF (Web Application Firewall) per protegir aplicacions web.

#### Exemple d'arquitectura segura:

- Frontend en subxarxa pública (amb un Load Balancer).

- Backend i base de dades en subxarxes privades.
- Comunicació entre capes restringida per Security Groups.
- Monitoratge amb CloudWatch, VPC Flow Logs, i AWS GuardDuty.

## 4. Serveis d'encaminament i distribució de contingut

Els serveis d'encaminament i distribució de contingut en AWS són eines que permeten dirigir el trànsit de xarxa de manera intel·ligent i lliurar contingut (com fitxers, webs, vídeos, etc.) de forma ràpida, segura i eficient als usuaris finals arreu del món.

A AWS, els serveis d'encaminament i distribució de continguts són fonamentals per oferir aplicacions amb alta disponibilitat, rendiment i escalabilitat global. Ací tens els principals serveis que cobreixen aquestes funcionalitats, explicats amb detall:

### 4.1. Amazon Route 53 – Servei de DNS altament disponible

Funció: Servei gestionat de DNS (Domain Name System) que tradueix noms de domini en adreces IP.

Característiques destacades:

- Alta disponibilitat i escalabilitat global.
- Routing basat en geografia: envia els usuaris a la regió més propera.
- Routing per pes: distribueix tràfic entre múltiples recursos segons percentatges.
- Failover DNS: redirigeix automàticament si un endpoint falla.
- Verificació de salut (health checks): monitoritza recursos i els elimina del DNS si fallen.
- Integra amb CloudFront, ELB, S3, i més.

### 4.2. Amazon CloudFront – Content Delivery Network (CDN)

Funció: Distribueix contingut (web, vídeo, apps, APIs) a través d'una xarxa global de punts de presència (Edge Locations).

**Beneficis:**

- Redueix latència i millora rendiment al servir contingut des del node més proper a l'usuari.
- Compatible amb contingut estàtic (HTML, imatges, CSS) i dinàmic (APIs).
- Protecció integrada amb:
  - AWS Shield (protecció contra DDoS)

- AWS WAF (Web Application Firewall)
- TLS/HTTPS i polítiques de seguretat (com HSTS)

- Integració amb Lambda@Edge per executar codi personalitzat en punts de presència.

**Un cas d'ús típic:** Servir un lloc web estàtic allotjat a S3 amb distribució global via CloudFront.

### 4.3. Elastic Load Balancing (ELB) – Repartiment del tràfic

Funció: Distribueix automàticament el tràfic entrant entre múltiples instàncies EC2, containers o serveis.

Tipus:

Tipus	Ús principal	Protocols	Característiques
<b>ALB (Application Load Balancer)</b>	Aplicacions web (nivell 7)	HTTP/HTTPS	Path-based routing, WebSocket, target groups
<b>NLB (Network Load Balancer)</b>	Tràfic a baixa latència (nivell 4)	TCP, UDP	Rendiment elevat, IPs estàtiques
<b>CLB (Classic Load Balancer)</b>	Usos antics	TCP/HTTP	Menys flexible

Funcions:

- Alta disponibilitat i escalabilitat automàtica
- Integració amb Auto Scaling
- Permet SSL termination per descarregar la càrrega criptogràfica

### 4.4. AWS Global Accelerator

Funció: Optimitza el rendiment global d'aplicacions millorant la latència i disponibilitat utilitzant la xarxa global d'AWS.

**Com funciona:**

- Assigna una IP global única.
- El tràfic s'encamina per la xarxa d'alta velocitat d'AWS fins a la regió ideal.
- Utilitza múltiples zones de disponibilitat per oferir alta tolerància a errors.

### Diferències amb CloudFront:

Global Accelerator	CloudFront
Millora rendiment de <b>tràfic dinàmic</b>	CDN per <b>tràfic estàtic i dinàmic</b>
IP global única	Dominis personalitzats (ex. d1234.cloudfront.net)
Apte per jocs, APIs, aplicacions interactives	Apte per llocs web, vídeo, fitxers

#### *4.5. Altres serveis relacionats*

##### AWS PrivateLink

- Publica serveis de manera privada dins AWS, sense exposar-los a Internet.
- Evita el tràfic entre VPCs via IP pública.

##### VPC Endpoints

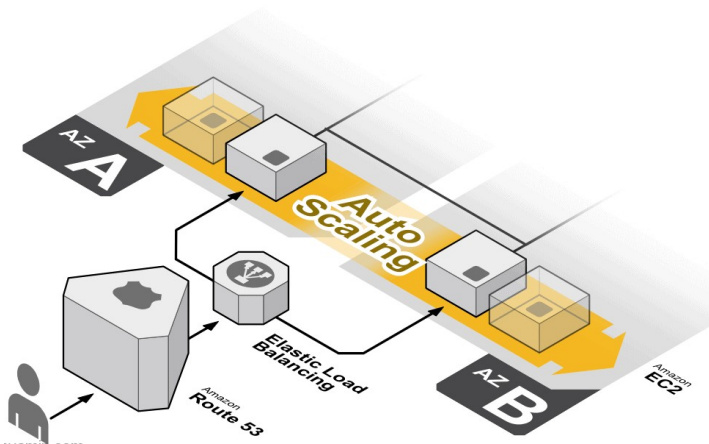
- Accés segur i privat a serveis com S3 i DynamoDB sense sortir a Internet.
- Millora la seguretat i rendiment.

#### *4.6. Tot això, combinat, assegura:*

- Resposta ràpida a escala global.
  - Distribució intel·ligent del tràfic.
  - Alta disponibilitat i seguretat.
-

## Tema 6: Computació en el núvol i escalat automàtic

---



1. Introducció als Serveis de Càlcul
2. Ús de Màquines Virtuals i funcions serverless
3. Escalat automàtic (Auto Scaling)
4. Balanceig de Càrrega
5. Integració entre balanceig i escalat

## 1. Introducció als Serveis de Càlcul

Els serveis de càlcul són la base fonamental de qualsevol infraestructura al núvol. Proporcionen la potència de processament necessària per executar aplicacions, analitzar dades, allotjar llocs web, i molt més, sense necessitat de mantenir servidors físics propis.

Són els substituïts dels servidors propis, no els tens físicament, els llogues. Parlem d'Infraestructura com a Servei (IaaS).

### Què són els serveis de càlcul?

Són recursos digitals que permeten executar codi, processos i aplicacions. Aquests serveis poden adaptar-se a les necessitats de cada usuari o empresa, des de xicotetes aplicacions personals fins a sistemes empresarials complexos.

Tu tens el control però tu tens la responsabilitat.

### Tipus principals de serveis de càlcul:

- **Màquines Virtuals (Vms)**. Són entorns virtualitzats que funcionen com un ordinador complet. Exemples: Amazon EC2, Google Compute Engine, Azure VMs.

En el cas de Google, tenim: **Google Compute Engine**. És un servei d'Infraestructura com a Servei (IaaS) ofert per Google Cloud Platform (GCP) que et permet crear i executar màquines virtuals (VMs) a la infraestructura de Google.

Famílies de màquines de Google Compute Engine:

1. General-purpose (ús general). Equilibri entre CPU, memòria i cost. Ideals per a aplicacions web, bases de dades petites, desenvolupament, etc.

- E2: Econòmiques i flexibles, amb rendiment variable.
- N2 / N2D: Més rendiment i estabilitat que E2. (N2D usa AMD EPYC)
- C3-standard / C2-standard: Alt rendiment, més potents pel que fa a la CPU que N2/E2.
- A3 / A2 (amb GPU): Pensades per a IA/ML però poden fer servir-se com màquines generals potents.

2. Memory-optimized (optimitzades per memòria). Per a aplicacions que requereixen molta RAM (bases de dades grans, anàlisi en memòria, etc.). M2 / M3: Ofereixen fins a 12 TB de RAM. Tenim una alta relació RAM/CPU.

3. Compute-optimized (optimitzades per càlcul). Per a càrregues intensives de CPU (simulacions, jocs, anàlisi científic, etc.). C2 / C2D: Alta freqüència de CPU, amb processadors Intel o AMD.

4. Accelerator-optimized (amb GPU per IA o gràfics). Pensades per a machine learning, simulacions o renderització gràfica. A2 (NVIDIA A100 GPUs)

5. Instàncies personalitzades (Custom VM types). Pots definir exactament quant de CPU i quanta memòria vols. Ideal per quan cap màquina predeterminada s'ajusta als teus requisits.

- **Contenidors.** Lleugers i ràpids d'arrencar, com Docker, sovint gestionats amb Kubernetes. Permeten desplegar aplicacions de forma més eficient i portable.

Parlem de Docker. Els contenidors de Docker corrent en el núvol són una forma lleugera i eficient d'executar aplicacions empaquetades amb totes les seues dependències, utilitzant serveis d'infraestructura o plataformes en el núvol com Google Cloud, AWS o Azure.

Un contenidor Docker és una unitat lleugera i aïllada que conté:

- L'aplicació
- Les biblioteques i dependències necessàries
- El sistema operatiu mínim per a executar-la

Pensa en un contenidor com una caixa portàtil que pots moure i executar en qualsevol sistema que tinga Docker instal·lat, sense preocupar-te de les configuracions del sistema amfitrió.

- **Còmput Serverless.** El Còmput Serverless (o computació sense servidors) és un model de programació en què no cal gestionar directament els servidors. El proveïdor de núvol (com Google Cloud, AWS o Azure) s'encarrega automàticament de tot el backend d'infraestructura, com la provisió, escalat, manteniment i monitoratge de servidors.

Tot i el nom, els servidors sí que existeixen, però tu no els veus ni els administres. En el escenari de Còmput Serverless, només escrius el teu codi. El núvol s'encarrega de la resta.

### Objectius dels serveis de còmput:

- **Escalabilitat:** adaptar-se automàticament a l'augment o reducció de la demanda.
- **Alta disponibilitat:** garantir que les aplicacions estiguin sempre disponibles.
- **Eficiència de costos:** pagar només pels recursos utilitzats.
- **Gestió simplificada:** menys responsabilitat sobre la infraestructura física.

### Exemples d'ús:

- Allotjament de llocs web i aplicacions.
- Execució de processos de dades i machine learning.
- Suport a APIs i microserveis.
- Automatització de tasques i respostes a esdeveniments

## 2. Ús de Màquines Virtuals i funcions serverless

Els serveis de còmput al núvol ofereixen diferents models d'execució. Els dos més utilitzats són les màquines virtuals (VMs) i les funcions serverless com AWS Lambda. Tots dos tenen avantatges i casos d'ús específics.

### Màquines Virtuals (VMs)

Les màquines virtuals simulen ordinadors físics. Ofereixen un entorn complet amb sistema operatiu i configuració pròpia.

Casos d'ús habituals:

- Aplicacions monolítiques o antigues que necessiten entorns personalitzats.
- Sistemes que requereixen accés a baixos nivells del sistema.
- Serveis que necessiten persistència o processos de llarga durada.

Avantatges:

- Control total del sistema (instal·lació de software, seguretat, etc.).
- Alta flexibilitat per a qualsevol tipus d'aplicació.
- Potent escalabilitat vertical (afegir CPU, RAM, etc.).

Limitacions:

- Necessiten manteniment (actualitzacions, seguretat, etc.).
- Temps de posada en marxa més lent.
- Costos més alts si no s'optimitza l'ús.

### Funcions serverless

Per exemple, AWS Lambda i serveis equivalents executen funcions menudes i independents que responen a esdeveniments. No cal gestionar cap servidor.

Casos d'ús habituals:

- Automatització de tasques (com processar imatges, enviar correus, etc.).
- Backend per a APIs REST.
- Processament de dades en temps real (streaming).
- Integracions entre serveis (webhooks, triggers).

Avantatges:

- Escalabilitat automàtica i immediata.
- Cap gestió de servidors.
- Pagament per ús (només quan la funció s'executa).
- Alta disponibilitat i tolerància a errors.

Limitacions:

- Temps d'execució limitat (ex: 15 minuts a AWS Lambda).
- No apte per a aplicacions amb estat (stateful).
- Pot ser més car a llarg termini si es fan servir de manera contínua.

Fem una comparativa. Ací tens una taula:

Característica	Màquines Virtuals (VMs)	Lambda (Serverless)
Control del sistema	Alt	Limitat



Característica	Màquines Virtuals (VMs)	Lambda (Serverless)
Escalat automàtic	Configurable	Automàtic
Cost	Fins i tot en repòs	Només per ús
Casos d'ús	Apps grans o personalitzades	Funcions breus i reactives
Temps de desplegament	Minuts	Millisegons

### 3. Escalat Automàtic (Auto Scaling)

L'escalat automàtic és una tècnica que permet adaptar els recursos computacionals automàticament en funció de la càrrega o demanda del sistema. Això assegura un rendiment constant i una millor eficiència de costos.

Per a màquines virtuals (Vms), plataformes com Amazon EC2, Google Compute Engine o Azure VMs permeten configurar grups d'escalat automàtic, els quals:

- Afegeixen instàncies quan augmenta la càrrega (CPU, tràfic de xarxa, etc.).
- Eliminen instàncies quan la demanda disminueix, optimitzant recursos i costos.

Per a serveis serverless (Lambda), els serveis com AWS Lambda escalen de manera totalment automàtica i transparent per a l'usuari:

- S'executen en paral·lel, segons el nombre d'esdeveniments rebuts.
- No requereixen configuració prèvia d'escalat.
- Ideal per a càrregues variables i esdeveniments intermitents.

Avantatges de l'escalat automàtic:

- Estalvi de costos. Pagues només pels recursos utilitzats realment.
- Rendiment òptim. Manté una resposta ràpida fins i tot durant pics de trànsit.
- Millor experiència d'usuari. Evita saturacions i errors per falta de recursos.

### 4. Balanceig de Càrrega

Els sistemes moderns han de ser resilents, escalables i eficients. Ho vorem més endavant amb la Well-Architected Framework. El balanceig de càrrega i l'escalat automàtic són tècniques clau per assolir aquests objectius en entorns cloud.

#### Balanceig de càrrega (Load Balancing)

El balancejador de càrrega distribueix el trànsit d'entrada entre múltiples instàncies o serveis per assegurar:

- Repartiment equitatiu de la càrrega
- Alta disponibilitat
- Rendiment consistent

Exemples de balancejadors:

- AWS Elastic Load Balancer (ELB)
- Google Cloud Load Balancing

Per exemple, AWS Elastic Load Balancer (ELB) és un servei gestionat d'equilibri de càrrega (load balancing) que distribueix automàticament el trànsit d'entrada entre diversos recursos, com ara EC2 instances, contenidors o adreces IP.

Tenim diversos tipus de ELB en AWS:

Tipus	Descripció breu	Casos d'ús típics
<b>Application Load Balancer (ALB)</b>	Load balancing a nivell de capa 7 (HTTP/HTTPS)	Web apps, microserveis, APIs REST
<b>Network Load Balancer (NLB)</b>	Load balancing a nivell de capa 4 (TCP/UDP)	Trànsit alt i baixíssima latència
<b>Gateway Load Balancer (GWLB)</b>	Especial per a integrar appliances de seguretat (firewalls, inspecció)	Inspecció de trànsit en xarxa
<b>Classic Load Balancer (CLB)</b>	Versió antiga, capa 4 i 7, recomanada només per sistemes antics	Migracions des de sistemes antics

## 5. Integració entre balanceig i escalat

El balancejador de càrrega treballa conjuntament amb l'escalat automàtic:

- Quan l'escalador afegeix noves instàncies, el balancejador les detecta i hi envia trànsit.
- Quan la càrrega baixa, es poden eliminar instàncies i el balancejador les exclou.

Això garanteix:

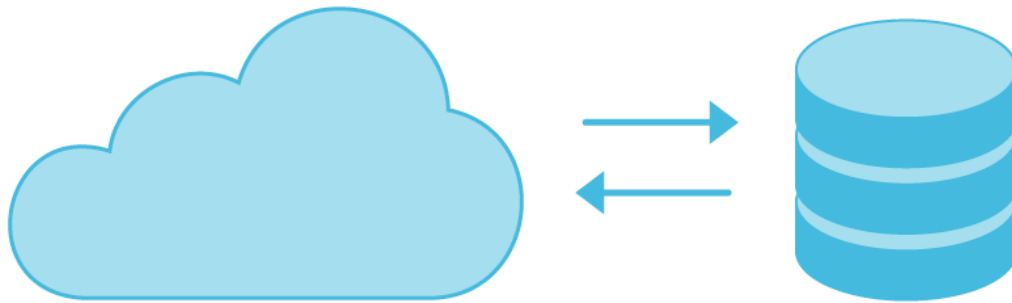
- Capacitat adaptativa
- Mínima latència
- Alta eficiència

Beneficis combinats

- Alta disponibilitat: cap instància individual esdevé un punt de fallida.
- Rendiment optimitzat: evita saturacions durant pics de trànsit.
- Eficiència de costos: s'ajusten els recursos segons necessitat real.

## Tema 7: Bases de dades al núvol

---



- 
1. Serveis d'Emmagatzematge al Núvol
    - 1.1. Disc dur al núvol (Bloc Storage).
    - 1.2. Emmagatzematge d'objectes
    - 1.3. Emmagatzematge de fitxers (File Storage)
  2. Bases de Dades al Núvol
    - 2.1. Bases de dades relacionals (SQL)
    - 2.2. Bases de dades NoSQL
    - 2.3. Altres serveis relacionats
  3. Creació i Gestió d'una Base de Dades a AWS
  4. El problema de la migració

## 1. Serveis d'Emmagatzematge al Núvol

Els serveis d'emmagatzematge permeten desar, accedir i gestionar dades de forma segura i escalable des d'infraestructures al núvol. Són essencials per a aplicacions, sistemes i bases de dades. Anem a veure 3 emmagatzematges diferents.

### 1.1. Disc dur al núvol (Block Storage).

Tenim un problema, o potset no. El problema és que una instància d'EC2 té CPU, RAM i storage (disc dur). Però si atures una instància i després la relances, les dades del disc dur es perden perquè la màquina es crea físicament en altre servidor, només s'ha desat el context. Suficient per a relançar la instància d'EC2 però el que contenia l'emmagatzament es perd.

Si volen un disc dur associat a una màquina virtual que siga persistent necessitem: Block Storage que simula un disc dur físic i s'utilitza per muntar-lo en una màquina virtual.

Exemples: **Amazon EBS (Elastic Block Store)** i **Azure Managed Disks**

Usos típics: sistemes operatius, aplicacions que necessiten accés directe al disc. Amb block storage tenim:

- Persistència de dades
- Alta velocitat d'accés
- Compatible amb bases de dades i aplicacions

### 1.2. Emmagatzematge d'objectes

Permet desar fitxers com imatges, vídeos o documents com a objectes amb metadades i identificadors únics. Guardarem objectes sense més. De distints tipus. De distints tamanyos. Només guardar-los.

Exemples: **Amazon S3**, **Google Cloud Storage** o **Azure Blob Storage**

Usos típics: còpies de seguretat, contingut multimèdia, data lakes, llocs web estàtics...

Avantatges:

- Escalabilitat massiva
- Baix cost per GB
- Accés des de web i APIs

### 1.3. Emmagatzematge de fitxers (File Storage)

Servei per a compartir fitxers entre múltiples màquines, com un sistema de fitxers en xarxa.

Un exemple és **Amazon EFS (Elastic File System)**. És un servei que proporciona un sistema de fitxers elàstic, escalable i compartit, accessible des de múltiples instàncies EC2 alhora.

És un sistema de fitxers basat en NFS (Network File System), que permet que diverses instàncies EC2 (fins i tot de diferents zones de disponibilitat dins una mateixa regió) puguin compartir un mateix sistema de fitxers com si fora un disc de xarxa. Tenim:

- Sistema de fitxers compartit: Permet que múltiples instàncies EC2 accedisquen i modifiquen simultàniament els mateixos fitxers.
- Escalat automàtic: El sistema creix i decreix automàticament segons la quantitat de dades emmagatzemades (fins a petabytes).
- Alt rendiment i baixa latència: Ideal per a aplicacions que necessiten accés simultani a fitxers amb rendiment consistent.
- Altament disponible i durador: Emmagatzema dades de manera redundant a múltiples zones de disponibilitat (AZs) dins una regió.
- Xifratge integrat: Xifra dades en repòs i en trànsit, compatible amb AWS KMS.
- Compatible amb POSIX: Suporta permisos, propietaris, i comandes típiques de sistemes UNIX/Linux.

Usos típics: entorns compartits, aplicacions distribuïdes o servidor de fitxers

Mentre que EBS és un recurs de zona i no és escalable, en EFS tenim escalabilitat horitzontal i vertical i diverses instàncies EC2 accedint-hi i és un recurs de zona. És un disc dur per a una EC2, però millor que EBS.

En Azure es diu **Azure Files** i en GCP es diu **Filestore**

## 2. Bases de Dades al Núvol

Una base de dades és un sistema per a desar, organitzar i recuperar dades de manera eficient. Els serveis al núvol ofereixen bases de dades gestionades, que no requereixen manteniment manual. Distingim entre SQL i noSQL.

### 2.1. Bases de dades relacionals (SQL)

Dades organitzades en taules amb relacions definides. Fan servir el llenguatge SQL.

Parlem d'un servei gestionat de bases de dades relacionals ofert pel nostre operador de núvol. Permet configurar, operar i escalar bases de dades al núvol de manera senzilla i eficient, sense haver-te de preocupar per la gestió de la infraestructura.

Avantatges de bases de dades SQL al núvol:

1. Gestió completament o parcialment automatitzada
  - Instal·lació i configuració inicial
  - Còpies de seguretat automàtiques
  - Actualitzacions de seguretat
  - Monitoratge i alertes

- Recuperació davant errors (failover)
2. Alta disponibilitat i tolerància a errors
    - Amb l'opció Multi-AZ, Amazon RDS pot replicar la base de dades en una altra zona de disponibilitat.
    - Si una zona cau, la base de dades es reassigna automàticament a la rèplica sense pèrdua de dades.
  3. Escalabilitat vertical i horitzontal
    - Pots canviar de mida (més CPU, RAM o emmagatzematge) fàcilment.
    - Alguns motors (com Aurora) també permeten llegides escalables mitjançant rèpliques de lectura.
  4. Seguretat integrada. Suport per a:
    - Encriptació en repòs (KMS) i en trànsit (TLS)
    - Autenticació amb IAM
    - Control de xarxa amb VPC i grups de seguretat
  5. Pagament per ús. Pagues pel que utilitzes: hores de computació, emmagatzematge, transferència... Pots utilitzar opcions com:
    - On-Demand (pagament per hora)
    - Reserved Instances (contractes de 1-3 anys amb descompte)
  6. Monitoratge i alertes integrades. Amb Amazon CloudWatch i la consola RDS pots:
    - Vigilar el rendiment (CPU, IOPS, connexions...)
    - Crear alertes automàtiques
  7. Compatibilitat amb motors populars. Per exemple, Amazon RDS és compatible amb:
    - MySQL
    - PostgreSQL
    - MariaDB
    - Oracle
    - Microsoft SQL Server
  8. Còpies de seguretat i restauració puntual. Per exemple, RDS fa snapshots automàtics i et permet:
    - Tornar a un estat concret ("point-in-time recovery")
    - Clonar bases de dades fàcilment per proves o desenvolupament
  9. Fàcil desplegament i gestió. Amb la consola AWS o eines com Terraform, CloudFormation o AWS CLI, pots desplegar una base de dades en minuts.

Exemple: **Amazon RDS** (MySQL, PostgreSQL, MariaDB), **Azure SQL Database**

Usos: aplicacions web, sistemes empresarials, ERP, CRM

## *2.2. Bases de dades NoSQL*

Dissenyades per a dades no estructurades o semi-estructurades. Tenim bases de dades més flexibles i escalables que les tradicionals SQL. Un bon exemple es DynamoDB.

**Amazon DynamoDB** és un servei de base de dades NoSQL completament gestionat, ofert per AWS, dissenyat per a oferir un alt rendiment, baixa latència i escalabilitat automàtica. És ideal per a aplicacions que necessiten accés ràpid a grans volums de dades.

Les característiques principals són:

- NoSQL: Emmagatzema dades en format clau-valor i documents (JSON).
- Escalabilitat automàtica: S'ajusta automàticament segons la càrrega.
- Alt rendiment: Mil·lisegons de latència, fins i tot a escala massiva.
- Sense servidor (serverless): No cal gestionar cap infraestructura.
- Alta disponibilitat: Dades replicades en múltiples zones (Multi-AZ).
- Integració amb Lambda: Ideal per arquitectures sense servidor (serverless).
- Control d'accés avançat: Amb IAM i etiquetes de recursos.

Com s'estructura DynamoDB? Com una taula, és l'equivalent a una "taula" tradicional, però flexible. És de tipus clau-valor.

**MongoDB** és una base de dades **NoSQL orientada a documents**, de codi obert, que emmagatzema les dades en format JSON. És molt flexible, escalable i ideal per a aplicacions modernes com webs, mòbils i serveis al núvol.

Característiques clau:

- Documents JSON: Les dades s'emmagatzemen com documents que poden tenir estructures complexes i jeràrquiques.
- Sense esquema fix: No cal definir un esquema previ, els documents poden tenir diferents camps.
- Escalabilitat horitzontal: Suport per a particionament automàtic (sharding).
- Alta disponibilitat: Amb rèpliques automàtiques (replica sets).
- Consultes riques: Potents operacions de lectura i escriptura, amb filtres, agregacions, indexació...
- Integració fàcil amb molts llenguatges: JavaScript, Python, Java, Node.js, etc.
- Suport per transaccions multi-document (des de MongoDB 4.0).

Pel que fa a l'estructura de MongoDB:

- Base de dades (Database) → Conté diverses colleccions.
- Col·lecció (Collection) → L'equivalent a una "taula" però sense esquema fix.
- Document → L'equivalent a una "fila"; format JSON o BSON.
- Camp (Field) → Clau dins d'un document (semblant a una "columna").

Si parlem d'AWS tenim **Amazon DocumentDB**.

Parlem ara d'**Amazon Keyspaces** que imita el comportament d'**Apache Cassandra**. És una base de dades NoSQL de columnes distribuïdes (column-family). Compatible amb Apache Cassandra i el seu llenguatge de consulta: CQL (Cassandra Query Language)

Característiques:

- Serverless: no cal gestionar servidors.

- Escalabilitat automàtica: pot manejar petabytes de dades.
- Alta disponibilitat: dissenyada per ser tolerable a fallades.
- Integració amb IAM, CloudWatch, VPC, etc.
- Ús típic: IoT, catàlegs de productes, dades de registre, sistemes de recomanació, etc.

És ideal si necessites una base de dades de columnes escalable i sense manteniment manual.

Què vol dir “base de dades de columnes”? A diferència d’una base de dades relacional (taules amb files i columnes tradicionals), les bases de dades de columnes (column-family stores):

- Emmagatzemen les dades per columnes, no per files.
- Són eficients per consultes sobre grans volums de dades d’una o poques columnes.

Per últim Amazon Neptune, és un servei de base de dades gestionat per AWS dissenyat especialment per emmagatzemar i consultar dades en forma de gràfics (graphs), no com a taules ni columnes.

Què és una base de dades de gràfics? Una base de dades de gràfics emmagatzema: nodes (els objectes, per exemple una persona, un llibre, un producte...) i les arestes (les relacions entre aquests objectes, per exemple: "coneix", "ha comprat", "és amic de"...)

Aquest tipus de base de dades és ideal per explorar relacions complexes entre entitats, com en xarxes socials, recomanacions, gestió de coneixement, etc.

### 2.3. Altres serveis relacionats

- Cache de dades: **Amazon ElastiCache** (Redis, Memcached) → per millorar rendiment
- Bases de dades de fluxos: **Amazon Kinesis, Azure Stream Analytics**
- Enginys d’anàlisi massiva: **BigQuery, Redshift, Snowflake**

## 3. Creació i Gestió d’una Base de Dades a AWS

Amazon Web Services (AWS) ofereix diversos serveis per a crear, gestionar i escalar bases de dades segons les necessitats de la teva aplicació.

### *Passos per crear una base de dades a AWS*

◆ Pas 1: Seleccionar el tipus de base de dades segons les necessitats del teu projecte:

Relacional (SQL): per aplicacions tradicionals, ERP, etc.

NoSQL: per aplicacions escalables, mòbils, IoT.

In-Memory: per a cache i temps real.

Analítica: per anàlisi de grans volums de dades.

◆ Pas 2: Triar el servei adequat --> Necessitat | Servei AWS



<b>Necessitat</b>	<b>Servei AWS</b>
SQL gestionat	<b>Amazon RDS</b> (MySQL, PostgreSQL, etc.)
NoSQL clau-valor	<b>Amazon DynamoDB</b>
Documents JSON	<b>Amazon DocumentDB</b> (compatible amb MongoDB)
Gràfics	<b>Amazon Neptune</b>
Memòria cau	<b>Amazon ElastiCache</b> (Redis, Memcached)
Data warehouse	<b>Amazon Redshift</b>

#### ◆ Pas 3: Crear la base de dades

- Entra al panell d’AWS Management Console.
- Ves a RDS o el servei corresponent.
- Prem “Create Database”.
- Tria el motor (MySQL, PostgreSQL, etc.).
- Defineix:
  - Nom de la BD
  - Usuari i contrasenya
  - Tipus d’instància (rendiment i cost)
  - Emmagatzematge (EBS: SSD o magnètic)
  - Xarxa i seguretat (VPC, ports, backups, etc.)

#### ◆ Pas 4: Connectar-se a la BD

- Usa eines com DBeaver, MySQL Workbench, psql o drivers JDBC/ODBC.
- Connecta’t amb l’endpoint, usuari i contrasenya.

## 4. El problema de la migració

AWS DMS (AWS Database Migration Service) és un servei gestionat per a migrar bases de dades cap a AWS o entre diferents motors de base de dades, de manera ràpida, segura i amb molt poca interrupció.

És un servei que et permet moure dades entre:

- Bases de dades on-premises → AWS
- Bases de dades entre serveis AWS (ex: RDS → Aurora)
- Diferents motors de bases de dades (ex: Oracle → PostgreSQL)

Pot fer:

- Migracions únicament de dades
- Sincronització contínua (replicació en temps real)
- Transformació lleugera de dades (amb AWS Schema Conversion Tool)

<b>Característica</b>	<b>Descripció</b>
<b>Migració heterogènia</b>	Pots migrar entre motors diferents (ex: SQL Server → MySQL)
<b>Migració en línia</b>	Les bases de dades poden continuar en ús mentre es fa la migració
<b>Replicació contínua</b>	Pots mantenir la base de dades sincronitzada (per migracions

## Característica

## Descripció

<b>Seguretat</b>	amb downtime zero)
<b>Schema Conversion Tool (SCT)</b>	Compatible amb IAM, VPC, TLS i KMS
	Per convertir l'esquema quan es migra entre motors diferents

Quan fer servir AWS DMS?

- ✓ Vols migrar una base de dades a AWS sense gaire interrupció
  - ✓ Tens motors de base de dades diferents (heterogeni)
  - ✓ Necessites replicació en temps real mentre fas la migració
  - ✓ Vols evitar migracions manuals lentes i complexes
-

## Tema 8: Marc de treball Well-Architected

---

---

---

- 1. Marc de treball Well-Architected*
- 2. Principis bàsics del marc Well-Architected*
- 3. Monitorització en un entorn Well-Architected*
- 4. Eines recomanades*
- 5. Disseny d'Arquitectures Resilients i Escalables*
- 6. Interpretació de Recomanacions d'Optimització*

## 1. Marc de treball Well-Architected

**AWS Well-Architected framework** (desenvolupat per AWS, però amb principis aplicables a altres entorns cloud) ofereix bones pràctiques per dissenyar, implementar i operar sistemes eficients, segurs i escalables. Aquests principis es complementen amb una monitorització efectiva per garantir l'operativitat i el rendiment del sistema.

El marc de treball Well-Architected Framework (WAF) va ser creat originalment per AWS, però els seus principis es poden aplicar també a altres núvols, com ara Microsoft Azure o Google Cloud Platform (GCP).

Podem dir que els principis són generals, el WAF es basa en 6 pilars fonamentals que són vàlids per a qualsevol arquitectura cloud. Aquests pilars es poden traduir a pràctiques equivalents en Azure, GCP, o altres entorns.

Well-Architected Framework d'AWS és propietari d'AWS, però els principis arquitectònics són aplicables a qualsevol entorn cloud, sempre que els adaptes a la tecnologia i serveis del núvol que utilitzes.

## 2. Principis bàsics del marc Well-Architected

En total són 6 pilars:

### 1. Excel·lència operacional

- Automatització de processos (CI/CD, IaC).
- Monitorització contínua i gestió d'incidències.
- Millora contínua mitjançant mètriques i logs.

### 2. Seguretat

- Principi de mínim privilegi (IAM).
- Protecció de dades (encriptació, backups).
- Detecció i resposta a amenaces (SIEM, AWS GuardDuty).

### 3. Fiabilitat

- Tolerància a fallades (multi-AZ, redundància).
- Recuperació davant errors (backups, DRP).
- Proves de càrrega i chaos engineering.

### 4. Eficiència de rendiment

- Optimització de recursos (autoescalat, caches).
- Monitorització de mètriques clau (latència, throughput).
- Elecció de serveis adequats per a cada càrrega.

### 5. Optimització de costos

- Anàlisi d'ús i desprovisionament de recursos inutilitzats.
- Ús d'instàncies reservades o spot i són instàncies de baix cost.

- Monitorització de costos amb eines com AWS Cost Explorer.

## 6. Sostenibilitat

També tenim **AWS Well-Architected Tool** que és una eina gratuïta proporcionada per Amazon Web Services (AWS) que ajuda arquitectes de solucions i equips tècnics a avaluar, revisar i millorar les seves càrregues de treball al núvol, basant-se en les bones pràctiques del Marc de Referència Well-Architected d'AWS (Well-Architected Framework).

## 3. Monitorització en un entorn Well-Architected

La monitorització és clau per garantir el compliment d'aquests 6 principis:

### Mètriques en temps real:

- CPU, memòria, latència, errors (**AWS CloudWatch**)

- SLA/SLO:

**SLA** (Service Level Agreement) – Acord de Nivell de Servei és un contracte formal entre un proveïdor de serveis (com AWS, Google Cloud o una empresa de TI) i el client. Defineix quin nivell de servei es garanteix. Normalment inclou:

- \* Disponibilitat mínima (% uptime garantit, ex. 99.9%).

- \* Temps de resposta màxim.

- \* Penalitzacions si no es compleix (com compensacions econòmiques).

Per exemple, el nostre SLA garanteix un 99,9% de disponibilitat mensual. Si es baixa d'això, es farà un descompte del 10% al client afectat.

**SLO** (Service Level Objective) – Objectiu de Nivell de Servei. És un objectiu intern mesurable que indica el nivell desitjat de servei. S'utilitza internament per a mesurar la qualitat del servei abans de comprometre's formalment. No és un contracte, però sí una meta quantificable.

Exemple: El nostre SLO intern és que l'API responga en menys de 200 ms el 95% del temps.

### Logs i traces:

- Centralització i anàlisi **AWS CloudTrail**

- Detecció d'anomalies. Per exemple **Amazon Lookout**, que és una família de serveis d'AWS basats en Machine Learning (ML) dissenyats per ajudar empreses a detectar anomalies i problemes de manera proactiva en diferents àmbits operacionals.

### Alertes i automatització:

- Configuració d'alertes per llindars. A AWS es pot fer de forma eficaç amb **Amazon CloudWatch**, que permet monitorar recursos i enviar alertes automàtiques quan es superen certs valors (llindars) en mètriques.

- Accions automàtiques (autoescalat, reinicis). A AWS, pots configurar accions automàtiques com ara autoescalat, reinicis, aturades o inici de recursos com a resposta a esdeveniments del sistema o a condicions de monitoratge (com alarmes de **CloudWatch**).

Accions més habituals:

1. Autoescalat (Auto Scaling). Permet augmentar o reduir automàticament el nombre d'instàncies EC2 (o altres serveis escalables com ECS, DynamoDB...) segons la càrrega. Afegir instàncies EC2 si la CPU > 70% durant 5 min.
2. Reinicis automàtics d'instàncies EC2. **CloudWatch** pot fer accions automàtiques sobre EC2 segons condicions de mètriques com ara reiniciar una EC2 si la memòria cau per baix d'un valor. Aturar-la si no respon.
3. Autoescalat per ECS, Lambda, DynamoDB... ECS (Fargate / EC2): pots escalar serveis segons ús de CPU o nombre de peticions. Lambda: escalat automàtic nadiu (no cal configurar-lo, però pots limitar-lo). DynamoDB: pot escalar capacitat de lectura/escriptura automàticament. Aurora Serverless v2: escalat de capacitat automàtic.
4. Automatització via AWS Systems Manager. Permet definir runbooks (procediments automatitzats) per a executar accions com: reiniciar serveis, executar scripts a instàncies o fer snapshots abans d'apagar.
5. Activadors via **EventBridge**. Pots configurar accions automàtiques basades en esdeveniments del sistema, per exemple: quan una instància EC2 es crea o es para, quan es detecta un canvi de configuració o quan una Lambda falla.

#### Seguretat proactiva:

- Detecció de comportaments sospitosos (**AWS Security Hub**). És un servei centralitzat de seguretat i compliment normatiu que ajuda a agrupar, organitzar i automatitzar la gestió de seguretat a tot el teu entorn AWS.
- Auditoria contínua de configuracions (**AWS Config**). És un servei que et permet monitorar, registrar i avaluar la configuració dels recursos d'AWS al llarg del temps. És ideal per a compliment normatiu, auditoria, detecció de desviacions i resposta automatitzada a canvis de configuració.

#### 4. Eines recomanades

Per a complir amb els principis del Well-Architected Framework (WAF), es recomanen diverses eines natives d'AWS que cobreixen cadascun dels 6 pilars (Excellència operativa, Seguretat, Fiabilitat, Eficiència del rendiment, Optimització de costos i Sostenibilitat).

Ací tens una taula resum per pilar i les eines principals recomanades:

Pilar	Eines principals
Excellència operativa	CloudFormation, CloudTrail, CloudWatch, Config, Systems Manager
Seguretat	IAM, KMS, GuardDuty, Security Hub, Macie, Inspector
Fiabilitat	Auto Scaling, Route 53, ELB, S3 Backups, CloudWatch

Pilar	Eines principals
Eficiència del rendiment	Compute Optimizer, CloudFront, Aurora, Lambda, Fargate
Optimització de costos	Cost Explorer, Budgets, Trusted Advisor, Savings Plans
Sostenibilitat	Carbon Footprint Tool, Graviton, Lifecycle policies, Serverless

## 5. Disseny d'Arquitectures Resilients i Escalables

Dissenyar arquitectures resilients i escalables a AWS és clau per aprofitar els avantatges del núvol: disponibilitat contínua, recuperació davant fallades, i adaptabilitat a càrrega variable. AWS ofereix un ampli conjunt de serveis i bones pràctiques per fer-ho segons el Well-Architected Framework, especialment en els pilars de Fiabilitat (Reliability) i Eficiència del Rendiment (Performance Efficiency).

Que quede clar, entenem per:

**Resiliència:** Capacitat de l'arquitectura per recuperar-se automàticament d'errades (hardware, software, xarxa o errors humans).

**Escalabilitat:** Capacitat de créixer o reduir-se automàticament segons la càrrega de treball, mantenint el rendiment i l'eficiència.

Pràctiques recomanades:

1. Zones de disponibilitat i regions. Dissenya per alta disponibilitat distribuint recursos entre zones de disponibilitat (Azs). Per a serveis crítics globals, considera una arquitectura multi-regió.
2. Equilibri de càrrega (Load Balancing). Utilitza **Elastic Load Balancing (ELB)** per distribuir tràfic entre instàncies de diverses AZs.
3. Autoescalat (Auto Scaling). **Auto Scaling Groups (ASG)** per instàncies EC2 segons CPU, memòria, o peticions. Disseny dinàmic per escalar serveis com: Lambda (escalat automàtic), ECS / Fargate (task scaling) o DynamoDB Auto Scaling
4. Arquitectura desacoblada. Evita dependències rígides entre components: usa **Amazon SQS o SNS** per comunicació asíncrona o **Amazon EventBridge** per esdeveniments desacoblats.
5. Persistència resilient: Amazon S3 per emmagatzematge durador, Amazon RDS amb Multi-AZ i backups automàtics, Aurora Global Database per replicació multi-regió o DynamoDB amb replicació global i tolerància a errades.
6. Recuperació davant fallades: configura estratègies de backup i restauració (snapshots, Amazon Backup, S3 versioning)
7. Supervisió i automació: **Amazon CloudWatch** per logs, mètriques i alarmes, **AWS CloudTrail** per auditories o **AWS Config** per detectar desviacions. Pel que fa a automatitzar gestió i resposta podem aplicar **AWS Systems Manager**.




## 6. Interpretació de Recomanacions d'Optimització

Els assistents d'infraestructura a AWS, com **Trusted Advisor**, **Compute Optimizer**, **Well-Architected Tool**, i **Cost Explorer**, generen recomanacions automàtiques d'optimització. Per a interpretar-les correctament tindrem en compte:

1. Comprendre la font de la recomanació. Cada assistent enfoca un tipus d'optimització diferent:

Assistents	Recomanacions sobre...
<b>Trusted Advisor</b>	Bones pràctiques (seguretat, costos, rendiment, límits de servei)
<b>Compute Optimizer</b>	Escalat d'EC2, Lambda, EBS (rendiment vs. cost)
<b>Cost Explorer + Budgets</b>	Ús i estalvi econòmic
<b>Well-Architected Tool</b>	Riscos per pilar (resiliència, cost, seguretat, etc.)
<b>Security Hub</b>	Configuracions insegures o exposades

2. Prioritzar l'acció segons impacte i risc

Recomanació	Exemple	Acció típica
 Crítica (seguretat)	Bucket S3 és públic sense raó	Tancar accés immediatament
 Rendiment infrautilitzat	EC2 amb CPU < 20% durant 30 dies	Reduir mida / parar
 Informativa / optimització	Savings Plans disponibles	Analitzar si convé comprar

3. Verificar el context tècnic real. Abans d'aplicar cap recomanació. Parla amb els equips tècnics (ex: potser una instància està sobredimensionada per motius temporals), revisa l'arquitectura (hi ha dependències? Estàs en entorns prod o test?) o consulta les mètriques **CloudWatch** per confirmar el que diu la recomanació.

4. Decidir si actuar, ajustar o descartar. Pots:

- Aplicar el canvi recomanat
- Fer proves primer en entorns no crítics
- Anotar com "acceptat amb excepció" si no és viable
- Automatitzar-lo amb Lambda o Systems Manager si és recurrent



## ANNEX: RESULTATS DE L'APRENTATGE I CRITERIS D'AVALUACIÓ

**RA1.** Comprèn els fonaments de la computació al núvol, els seus avantatges davant de sistemes tradicionals, el marc d'adopció, els principis de migració i els aspectes clau de facturació, com ara estimació i optimització de costos. S'han comprès els conceptes fonamentals de la computació al núvol. S'ha demostrat la capacitat per explicar els avantatges del núvol davant de sistemes tradicionals. S'ha participat en activitats relacionades amb l'ecosistema de serveis al núvol. S'han identificat els principis bàsics de la facturació i els costos al núvol. S'ha fet un ús correcte d'eines per estimar i gestionar pressupostos. S'han participat a activitats pràctiques sobre gestió de costos.

**RA2.** Identifica els components clau de la infraestructura global del núvol, diferenciant serveis principals, regions, zones de disponibilitat i aplicant mesures bàsiques de seguretat com ara el model de responsabilitat compartida, gestió d'accessos i protecció de dades. S'ha adquirit coneixement dels components d'una infraestructura global al núvol. S'ha demostrat la capacitat per a explorar i descriure les categories de serveis principals disponibles. S'ha realitzat una avaluació de l'ús adequat de serveis bàsics en exercicis pràctics. S'ha comprès el model de responsabilitat compartida al núvol. S'han aplicat mesures de seguretat bàsiques mitjançant eines de gestió d'accés. S'han fet exercicis sobre gestió d'usuaris i polítiques de seguretat.

**RA3.** Dissenya i configura xarxes virtuals i serveis de còmput al núvol, aplicant bones pràctiques de seguretat, estratègies de balanceig de càrrega, escalat automàtic i aprofitant tecnologies serverless, contenidors i màquines virtuals segons casos d'ús específics. S'ha realitzat el disseny i la configuració de xarxes virtuals privades. S'han aplicat bones pràctiques de seguretat en xarxes i arquitectures. S'ha participat activament en la creació i la configuració d'una xarxa funcional. S'ha realitzat la selecció de serveis de computació adequats segons els casos d'ús. S'ha dut a terme la configuració i gestió de balanceig de càrrega i escalat automàtic. S'han desenvolupat pràctiques relacionades amb l'optimització de recursos computacionals.

**RA4.** Gestiona serveis d'emmagatzematge i bases de dades al núvol, seleccionant tecnologies adequades per a casos específics, i dissenya arquitectures escalables i resilient utilitzant eines de monitorització i optimització per millorar-ne el rendiment. S'ha fet la diferenciació entre tecnologies d'emmagatzematge al núvol. S'ha dut a terme la configuració i la gestió de bases de dades en un entorn de núvol. S'ha treballat per resoldre problemes pràctics sobre emmagatzematge i bases de dades. S'han dissenyat arquitectures escalables i resilient basades en les millors pràctiques. S'han fet servir eines de monitorització i recomanacions d'optimització. S'ha participat en activitats que simulen l'anàlisi i la millora d'arquitectures existents.