

Computació en Entorns Al Núvol

Pràctica 1 - Virtual Private Cloud

Grup 19

- Adrià Muro Gómez (1665191)
- David Morillo Massagué (1666540)

Data: 12/04/2025

Problema a resoldre.....	3
Diferències respecte el disseny inicial.....	3
Disseny principal a implementar.....	5
Descripció de connexions i adreces del sistema implementat.....	6
Xarxa VPC i Subxarxes.....	6
Internet Gateway i taula de rutes.....	7
Security Groups.....	8
Instàncies EC2.....	8
Connexions i validació.....	9
Funcionament en un esdeveniment de caiguda d'un servidor.....	10
Millores del disseny.....	11

Problema a resoldre

Plantejament del problema:

L'empresa ABC Inc vol implantar un nou **Servei Web** per tal d'assistir les peticions d'informació que vinguin de l'exterior. Es vol implementar un servei amb **redundància**, de forma que pugui continuar funcionant encara que es produeixi una caiguda en un dels servidors.

D'aquesta manera, ABC Inc vol implementar **un o varis servidors** Web accessibles des de l'exterior a través dels ports estàndards **http i https**.

Alhora, es requeriran diversos **Serveis** pendents de definir però que ja se sap que seran **locals** a cada servidor web però **no accessibles des de l'exterior**, s'haurà de deixar preparat tot l'escenari per aquest Serveis i altres que puguin venir.

Per seguretat, als servidors web es podrà accedir des de qualsevol lloc per **HTTP/HTTPS** però per administració per **SSH**, només es podrà accedir des de la **xarxa privada local**.

Diferències respecte el disseny inicial

Disseny de la infraestructura i justificació de les decisions tècniques

Durant la primera sessió de treball, vam dissenyar una arquitectura inicial basada en el laboratori del **Mòdul 5 – Lab 2 d'AWS Academy**. No obstant això, després d'una revisió amb el professorat, vam incorporar diversos canvis importants per millorar la resiliència, la seguretat i l'escalabilitat de la infraestructura. A continuació es detallen les decisions tècniques preses i la seva justificació.

1. Duplicació dels servidors web

Per millorar la disponibilitat i la fiabilitat del sistema, vam configurar diversos servidors web. Aquesta duplicació garanteix que, si un servidor fallés, els altres puguin continuar oferint el servei sense interrupcions, millorant així la tolerància a fallades i assegurant la continuïtat del servei.

2. Creació de dues subxarxes públiques i privades distribuïdes en dues AZ

Per augmentar l'alta disponibilitat de la infraestructura, vam distribuir els recursos en dues zones de disponibilitat (AZ) diferents dins de la VPC. Cada zona de disponibilitat disposa de dues subxarxes: una pública i una privada. Aquesta distribució ajuda a mitigar els riscos derivats d'una possible fallada d'una única zona de disponibilitat. Si una AZ experimenta una caiguda, els recursos de l'altra zona poden continuar oferint el servei, assegurant la disponibilitat contínua de la infraestructura.

3. Configuració de l'Internet Gateway

Per tal que les instàncies EC2 allotjades a les subxarxes públiques puguin comunicar-se amb l'exterior (Internet), s'ha configurat un Internet Gateway i s'ha associat a la VPC principal. Aquesta passarel·la és imprescindible per proporcionar accés públic a serveis com ara aplicacions web i per permetre que les instàncies puguin descarregar actualitzacions o paquets durant la seva inicialització. A més, s'ha creat i associat una taula de rutes a les subxarxes públiques que redirigeix tot el trànsit sortint (0.0.0.0/0) cap a l'Internet Gateway. Sense aquesta configuració, tot i tenir IP pública assignada, les instàncies no podrien establir connexions externes.

4. Seguretat i accés restringit als servidors web

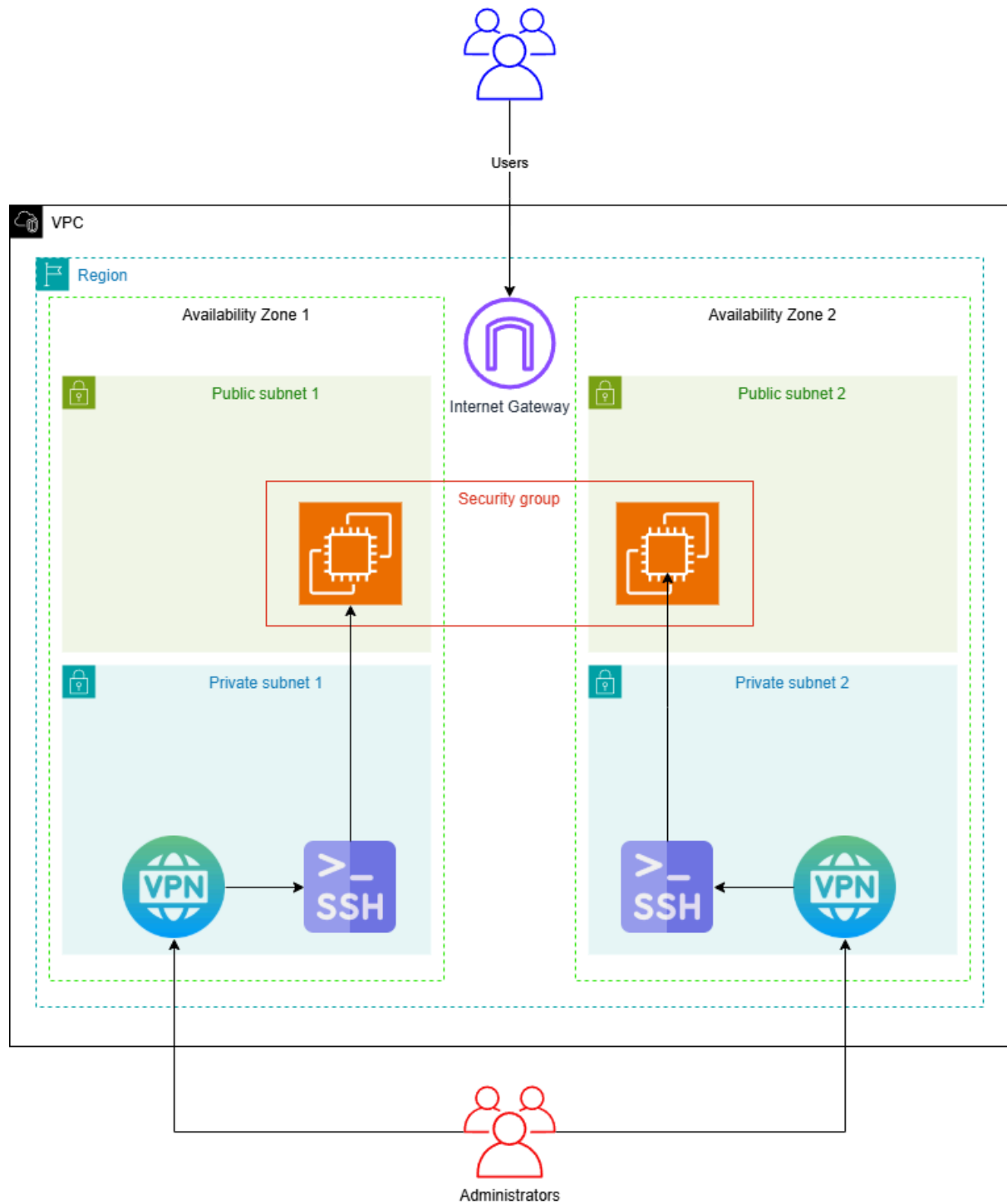
Per garantir la seguretat del servei web i complir amb els requisits de seguretat establerts per l'empresa ABC Inc, s'ha configurat un Security Group específic per als servidors web. Les regles de seguretat permeten:

- **Accés públic per HTTP (port 80) i HTTPS (port 443) des de qualsevol origen (Internet):** Aquesta configuració permet l'accés públic a la plataforma web per a usuaris externs, garantint que el servei sigui accessible des de qualsevol ubicació mitjançant HTTP i HTTPS.
- **Accés restringit per SSH (port 22) exclusivament des de la xarxa privada:** Per evitar l'exposició del port SSH a l'Internet i protegir els servidors d'atacs externs, hem configurat l'accés SSH perquè només sigui permès des de la xarxa privada. Aquesta mesura millora la seguretat de l'infraestructura, ja que limita l'accés administratiu a les màquines només als dispositius autoritzats dins de la VPC.

Per a accedir a aquest servei SSH, en el diagrama s'ha inclòs un servei VPN que permetrà als administradors gestionar les aplicacions al VPC. Aquest servidor no s'implementarà al nostre VPC però creiem necessari mencionar-ho per a justificar l'ús del SSH des de la subxarxa privada.

Aquest conjunt de decisions tècniques assegura que la infraestructura sigui robusta, escalable i segura, complint amb els requisits de disponibilitat i seguretat establerts per l'empresa i seguint les millors pràctiques de AWS.

Disseny principal a implementar



Descripció de connexions i adreces del sistema implementat

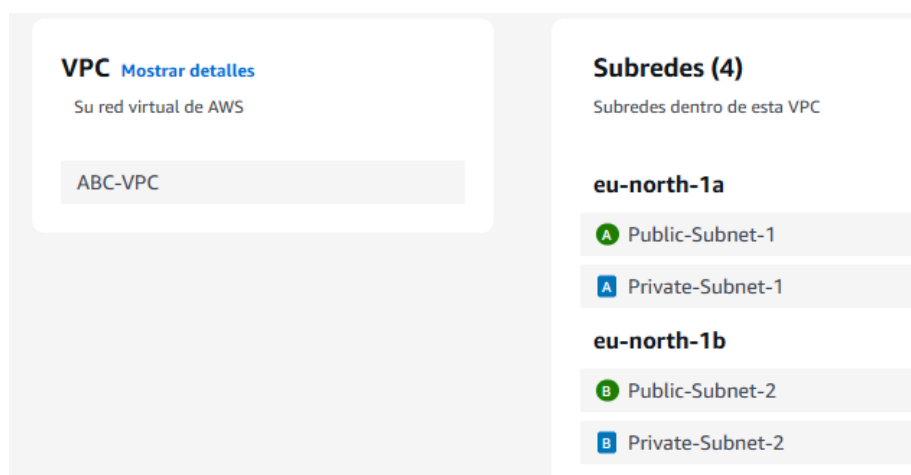
A continuació es detalla cada part del sistema així com les connexions entre components i el mecanisme d'accés a les instàncies virtuals.

Xarxa VPC i Subxarxes

En primer lloc, s'ha creat una VPC anomenada ABC-VPC amb el CIDR bloc 10.0.0.0/16, que proporciona un ampli rang d'adreces IP internes. Dins d'aquesta VPC, s'han creat quatre subxarxes:

- **Public-Subnet-1** amb CIDR 10.0.1.0/24 a la zona de disponibilitat *eu-north-1a*.
- **Public-Subnet-2** amb CIDR 10.0.2.0/24 a la zona de disponibilitat *eu-north-1b*.
- **Private-Subnet-1** amb CIDR 10.0.11.0/24 a la zona de disponibilitat *eu-north-1a*.
- **Private-Subnet-2** amb CIDR 10.0.12.0/24 a la zona de disponibilitat *eu-north-1b*.

Public-Subnet-2	subnet-0fee9f72679ebe9b5	10.0.2.0/24
Public-Subnet-1	subnet-025d6f139b6b97f2c	10.0.1.0/24
Private-Subnet-2	subnet-09f97042de5db96a5	10.0.12.0/24
Private-Subnet-1	subnet-01d97f9798a94d4ff	10.0.11.0/24



Les subxarxes **públiques** s'utilitzen per allotjar les instàncies que han de tenir accés a internet, mentre que les **privades** es reserven per futurs serveis interns que no han d'estar exposats directament. Aquests serveis poden ser, per exemple, bases de dades per a l'aplicació web.

Internet Gateway i taula de rutes

Per proporcionar accés a Internet a les instàncies dins de les subxarxes públiques, s’ha creat un **Internet Gateway** (ABC-IGW) que s’ha adjuntat a la VPC. Aquest component actua com a passarel·la cap a l’exterior.

igw-06e80ee1ea3e11c5f / ABC-IGW

Acciones

Detalles

Información

ID de gateway de Internet

igw-06e80ee1ea3e11c5f

Estado

Attached

ID de la VPC

vpc-0589d247ae2b62c81 | ABC-VPC

Propietario

194357582553

Etiquetas

Buscar etiquetas

Clave

Valor

Name

ABC-IGW

Administrar etiquetas

Gateways de Internet (2)

Información

Buscar

	Name	ID de gateway de Internet	Estado	ID de la VPC	Propietario
<input type="checkbox"/>	-	igw-05c4ed36068d84f5d	Attached	vpc-0676ec89432ba8a52	194357582553
<input type="checkbox"/>	ABC-IGW	igw-06e80ee1ea3e11c5f	Attached	vpc-0589d247ae2b62c81 ABC-VPC	194357582553

A més, s’ha configurat una **taula de rutes** (Public-RT) associada a les subxarxes públiques amb una regla que envia tot el tràfic (0.0.0.0/0) cap a l’Internet Gateway.

rtb-01dcebef8ed1540f2 / Public-RT

Detalles

Información

ID de tabla de enrutamiento

rtb-01dcebef8ed1540f2

VPC

vpc-0589d247ae2b62c81 | ABC-VPC

Principal

No

ID de propietario

194357582553

Rutas

Asociaciones de subredes

Asociaciones de borde

Propagación de rutas

Rutas (2)

Filtrar rutas

Destino	Destino
0.0.0.0/0	igw-06e80ee1ea3e11c5f
10.0.0.0/16	local

Les subxarxes privades no tenen accés directe a Internet, per tant, la seva taula de rutes no inclou cap sortida cap a l’exterior.

Rutas	Asociaciones de subredes	Asociaciones de borde	Propagación de rutas	Etiquetas
Asociaciones de subredes explícitas (2)				
Q Buscar asociación de subredes				
Nombre	ID de subred	CIDR IPv4	CIDR IPv6	
Public-Subnet-2	subnet-0fee9f72679ebe9b5	10.0.2.0/24	-	
Public-Subnet-1	subnet-025d6f139b6b97f2c	10.0.1.0/24	-	
Subredes sin asociaciones explícitas (2)				
Las siguientes subredes no se han asociado explícitamente con ninguna tabla de enrutamiento y, por lo tanto, están asociadas a la tabla de enrutamiento principal:				
Q Buscar asociación de subredes				
Nombre	ID de subred	CIDR IPv4	CIDR IPv6	
Private-Subnet-2	subnet-09f97042de5db96a5	10.0.12.0/24	-	
Private-Subnet-1	subnet-01d97f9798a94d4ff	10.0.11.0/24	-	

Security Groups

S'ha creat un grup de seguretat per complir amb les exigències de l'enunciat:

Web-SG: assignat a les instàncies EC2 allotjades a les subxarxes públiques. Aquest grup permet:

- Tràfic entrant al port **80 (HTTP)** des de qualsevol IP (0.0.0.0/0), per permetre l'accés a la web Apache des d'internet a partir d'HTTP.
- Tràfic entrant al port **443 (HTTPS)** des de qualsevol IP (0.0.0.0/0), per permetre l'accés a la web Apache des d'internet a partir d'HTTP.
- Tràfic entrant al port **22 (SSH)** únicament des de les **subxarxes privades** (en el nostre cas 10.0.11.0/24 i 10.0.12.0/24), per tal de garantir que només es pot accedir a nivell administratiu via una màquina dins la pròpia xarxa privada.

Reglas de entrada (4)									
Q Buscar									
<input type="checkbox"/>	Name	ID de la regla del gr...	Versión de IP	Tipo	Protocolo	Intervalo de puertos	Origen		
<input type="checkbox"/>	-	sgr-0bcb37bb3d1d760fe	IPv4	HTTPS	TCP	443	0.0.0.0/0		
<input type="checkbox"/>	-	sgr-0dbd9eab5153bfdcf	IPv4	SSH	TCP	22	10.0.11.0/24		
<input type="checkbox"/>	-	sgr-0212fad22430c28e4	IPv4	HTTP	TCP	80	0.0.0.0/0		
<input type="checkbox"/>	-	sgr-0e83280562229bd6c	IPv4	SSH	TCP	22	10.0.12.0/24		

Instàncies EC2

S'han llançat dues instàncies EC2, una en cada subxarxa pública, fent ús de la imatge **Amazon Linux 2 AMI**. Les característiques de les instàncies són:

- Tipus: **t3.micro** (t2.micro no estava disponible en aquell moment)
- VPC: ABC-VPC

- Subnet: **Public-Subnet-1** / **Public-Subnet-2**
- Assignació automàtica d'IP pública: **activada**
- Zona de disponibilitat: una instància per AZ (alta disponibilitat geogràfica)
- Security Group assignat: **Web-SG**

Resumen de instancia de i-005347be5e2c934e7 (Web Server 1) Información

Se ha actualizado hace less than a minute

ID de la instancia
 i-005347be5e2c934e7

Dirección IPv6
-

Tipo de nombre de anfitrión
Nombre de IP: ip-10-0-1-245.eu-north-1.compute.internal

Responder al nombre DNS de recurso privado
-

Dirección IP asignada automáticamente
 16.170.143.51 [IP pública]

Rol de IAM
-

IMDSv2
Required

Dirección IPv4 pública
 16.170.143.51 | [dirección abierta](#) 

Estado de la instancia
 En ejecución

Nombre DNS de IP privada (solo IPv4)
 ip-10-0-1-245.eu-north-1.compute.internal

Tipo de instancia
t3.micro







ID de VPC
 vpc-0589d247ae2b62c81 (ABC-VPC) 

ID de subred
 subnet-025d6f139b6b97f2c (Public-Subnet-1) 

ARN de instancia
 arn:aws:ec2:eu-north-1:194357582553:instance/i-005347be5e2c934e7

Les instàncies s'inicialitzen automàticament mitjançant un script de **user data**, que instal·la el servidor Apache i crea un fitxer HTML simple per verificar la seva funcionalitat. L'script utilitzat és el mateix que l'utilitzat al laboratori d'VPC.

Aquest mecanisme permet tenir una pàgina funcional disponible immediatament després del llançament de la instància.

Name 	ID de la instancia	Estado de la i... 	Tipo de inst... 	Comprobación de	Estado de la al...	Zona de dispon... 	DNS de IPv4 pública 	Dirección IP... 
Web Server 1	i-005347be5e2c934e7	 En ejecución  	t3.micro	 3/3 comprobaci... Ver alarmas 		eu-north-1a	-	16.170.143.51
Web Server 2	i-0f87633b25ffc492c	 En ejecución  	t3.micro	 3/3 comprobaci... Ver alarmas 		eu-north-1b	-	16.170.211.248

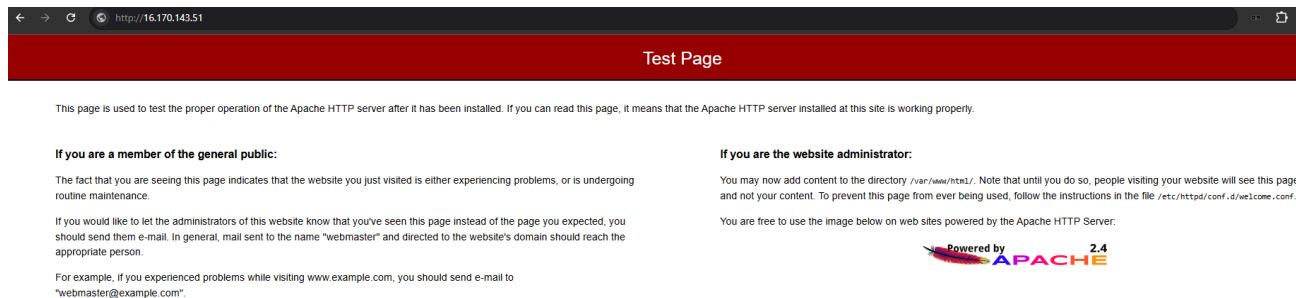
Les IP's de les nostres instàncies van ser les següents:

- **Web Server 1** → 16.170.145.51
- **Web Server 2** → 16.170.211.248

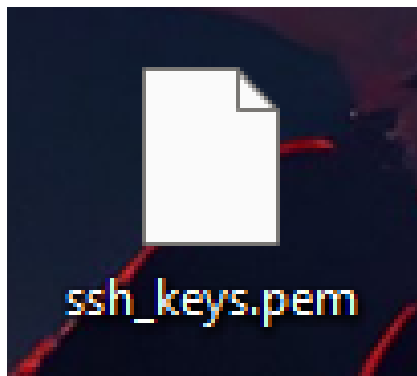
Connexions i validació

Per validar la infraestructura desplegada, s'han dut a terme dues comprovacions principals:

Accés públic via HTTP: A través del navegador, s'ha accedit a la IP pública de les instàncies EC2, verificant que el servidor Apache està operatiu i retorna la pàgina HTML esperada.



Accés SSH restringit: Tot i que les instàncies tenen IP pública, el port 22 (SSH) està restringit a les subxarxes privades. Per aquest motiu, per tal de fer accés SSH caldria disposar d'una instància bastion o una VPN interna que resideixi a la VPC privada. En el nostre cas, s'ha preparat l'accés amb una clau privada anomenada `ssh_keys.pem`, que ha estat descarregada durant el procés de creació de la instància.



Funcionament en un esdeveniment de caiguda d'un servidor

El sistema ha estat dissenyat per ser resilient davant la caiguda d'un dels servidors:

- **Redundància per zones de disponibilitat (AZ):** Els dos servidors web estan allotjats a zones de disponibilitat diferents, evitant la caiguda simultània per errors físics, elèctrics o de xarxa dins d'una única regió. Aquesta arquitectura assegura que si una AZ deixa de funcionar, el tràfic es redirigeix automàticament cap als servidors actius d'una altra zona.
- **Replicació de serveis locals:** Els serveis locals essencials estan replicats a cada servidor per garantir la continuïtat de les funcions internes sense dependre de la

comunicació entre zones.

- **Temps de tornada al funcionament d'una AZ:** En cas de caiguda d'una zona de disponibilitat, AWS treballa per restablir el servei al més aviat possible. Normalment les AZs tornen a estar operatives en un període que va de minuts a poques hores. No obstant això, gràcies a la redundància implementada, el servei continua operatiu en tot moment des de la zona alternativa.

Milliores del disseny

En el futur es poden aplicar diverses millores per fer el sistema més robust i millorar l'experiència dels usuaris:

- **Afegir Auto Scaling:** Per adaptar-se automàticament a pics de trànsit i estalviar recursos quan la càrrega és baixa.
- **Monitorització (Amazon CloudWatch):** Per veure què està passant en tot moment i rebre alertes si hi ha problemes o anomalies.
- **Base de dades en xarxa privada (Amazon RDS):** Per guardar dades de manera segura i fiable, sense exposar-les a internet.
- **Backups i estratègia de recuperació:** Fer còpies de seguretat automàtiques i tenir un pla per recuperar el sistema ràpidament si hi ha una fallada greu. Es podrien fer snapshots automàtics amb Amazon RDS o Amazon EBS.