

Universitat Autònoma de Barcelona
Facultat de Ciències



BUILDING VPCs AND LAUNCHING WEB SERVERS

Autors:

Gerard Lahuerta & Ona Sánchez
1601350 — 1601181

2 d' Abril de 2023

Contents

1	Introducció	3
2	Motivació del treball	3
3	Sessió 1: Testeig de la creació i gestió de les VPC	4
3.1	Objectius	4
3.2	Metodologia	4
3.3	Desenvolupament del treball	5
3.3.1	5
3.3.2	Creació de les <i>subnets</i> addicionals	7
3.3.3	Creació del grup de seguretat de la VPC	11
3.3.4	Llançament d'una <i>Web Server Instance</i>	13
3.4	Laboratori completat	15
3.5	Conclusions	15
4	Sessió 2: Llançament d'una Web server amb VPC	16
4.1	Objectius	16
4.2	Metodologia	16
4.3	Desenvolupament	18
4.3.1	Creació de la VPC i de les subxarxes	18
4.3.2	Llançament de les instàncies	19
4.3.3	Comprovacions d'accés a les instàncies	21
4.3.4	Modificació de les subxarxes privades	22
4.4	Conclusions	24

1 Introducció

Com a part de l'assignatura de *Sistemes distribuïts i el núvol*, s'ha proposat l'entrega d'un informe on es recull l'experiència i els passos que s'han seguit per a desenvolupar una xarxa VPC, juntament amb el llançament d'una instància *EC2* dins una subxarxa d'aquesta.

2 Motivació del treball

Practicar l'ús de la plataforma *Amazon Web Service (AWS)*, així com posar en pràctica els coneixements explicats en les classes de teoria sobre la creació de xarxes VPC i l'ús d'aquestes.

3 Sessió 1: Testeig de la creació i gestió de les VPC

3.1 Objectius

Els objectius plantejats en aquesta sessió són:

- Agafar agilitat de treball a la plataforma *AWS*.
- Crear una xarxa *VPC*.
- Configurar un grup de seguretat propi.
- Llançar una instància *EC2* a la *VPC*.
- Modificar les instàncies segons els requisits a complir.
- Crear la infraestructura de la *VPC* i les subxarxes d'aquesta segons les necessitats pròpies.

3.2 Metodologia

Per dur a terme la pràctica és seguiran els consells i passos del manual subministrat pel curs que otorga *AWS* :

Module-5 Networking and Content Delivery > Lab 2 - Build your VPC and Launch a Web Server.

A més, s'han seguit les indicacions del professor per a diverses qüestions i dubtes sorgits a l'hora de treballar en la instància.

Informar també, que la metodologia del treball ha estat basada en recopilar la informació necessària per redactar l'informe i poder analitzar els processos de gestió de la instància. S'ha subdividit l'explicació de treball en 4 etapes diferents:

1. Creació d'una xarxa *VPC*.
2. Adició de subxarxes.
3. Creació un grup de seguretat per la *VPC*.
4. Llançament d'una instància *Web Server*.

En cada subapartat es documentarà el procés i explicació del treball.

Es recomana que previ a llegir aquest informe s'hagi entés els procediment explicat a la pràctica anterior ([Pràctica 2](#)) ja que part del procés d'elaboració d'aquest treball és similar al fet en l'anterior.

3.3 Desenvolupament del treball

S'inicia doncs la pràctica engegant el terminal (imatge 1a) del *AWS* i, començant així la creació i gestió de la xarxa *VPC*.

Una vegada iniciat el terminal, apareix la pàgina inicial de la consola d'*AWS* (imatge 1b).

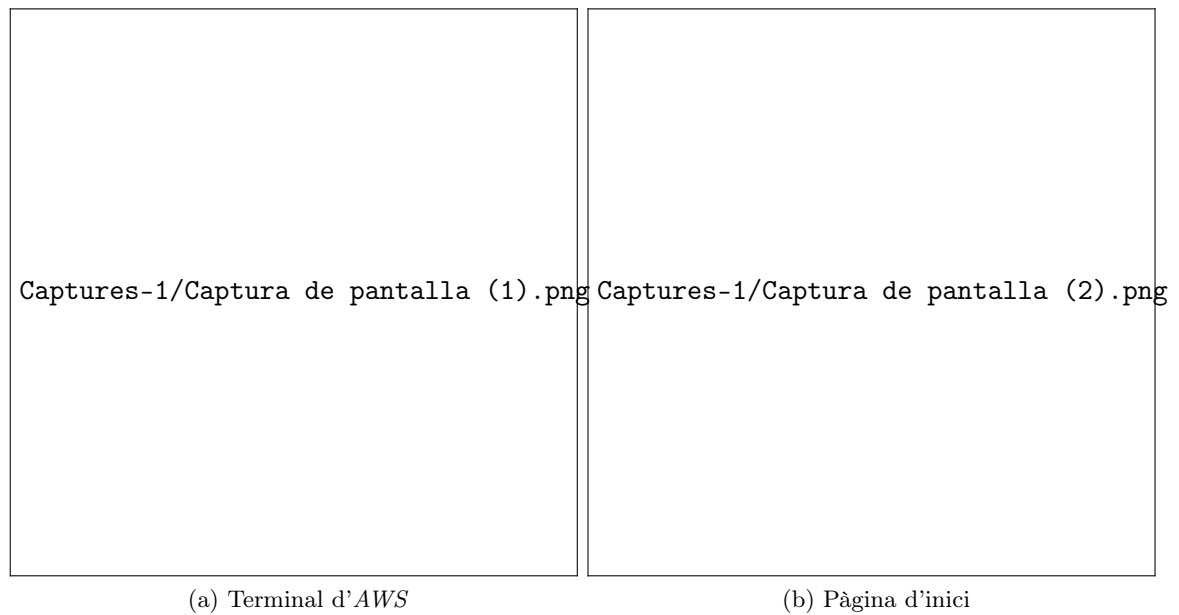


Figure 1: Inicialització de l'ambient de pràctiques

3.3.1

Una vegada inicialitzat l'ambient de pràctiques, es procedeix a la creació d'una *VPC* amb dues subxarxes, una pública i una privada.

Per tal de crear la *VPC*, cal cercar al menú *Services*, que permet obrir la consola que es mostra a continuació:

Per proseguir amb la creació de la *VPC*, cal seleccionar l'opció *Crear VPC*. D'aquesta manera, s'obren les opcions de configuració de la *VPC*, que permetran escollir la configuració que es necessiti per satisfer els requisits que demana un hipotètic client.

Es mostra a continuació la configuració utilitzada per a la creació de la *VPC* de la pràctica:

D'aquesta manera, s'ha creat una *VPC* amb dues subxarxes, una pública i una privada. Per confirmar la creació de la *VPC*, clicar *Create VPC* al final de la pràgina.

Un cop creada la *VPC*, seleccionant l'opció *View VPC*, *AWS* ens mostra de forma esquematitzada la xarxa que hem creat, tal i com s'observa a continuació:

Es confirma d'aquesta manera la correcta creació de la *VPC*, així com de les subxarxes pública i privada.

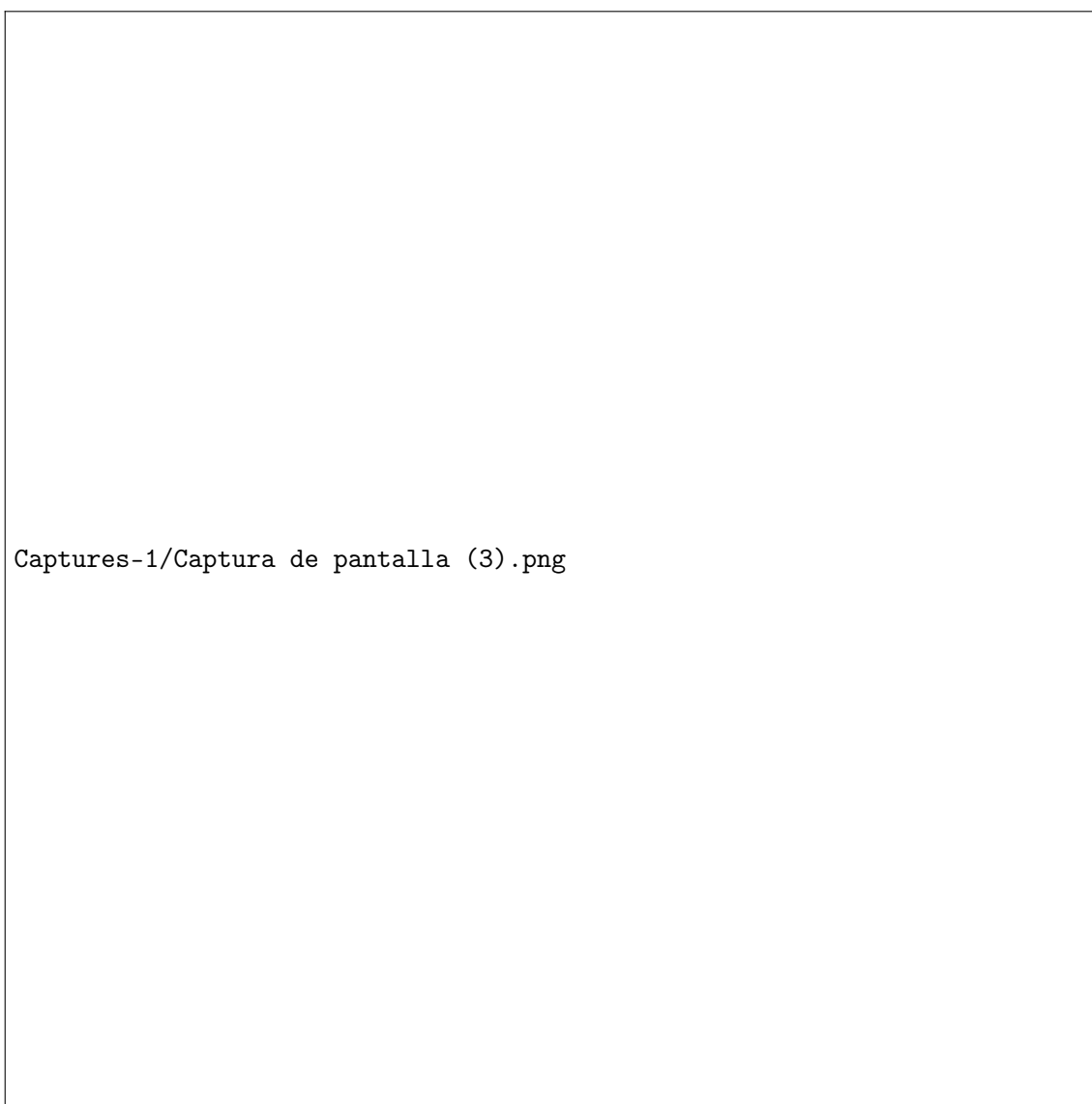


Figure 2: Consola *AWS* de creació d'una *VPC*

Per tal de veure els detalls de la xarxa, escollir l'opció *Subnets* seguit de *Route tables* per veure els detalls de la configuració de la xarxa.

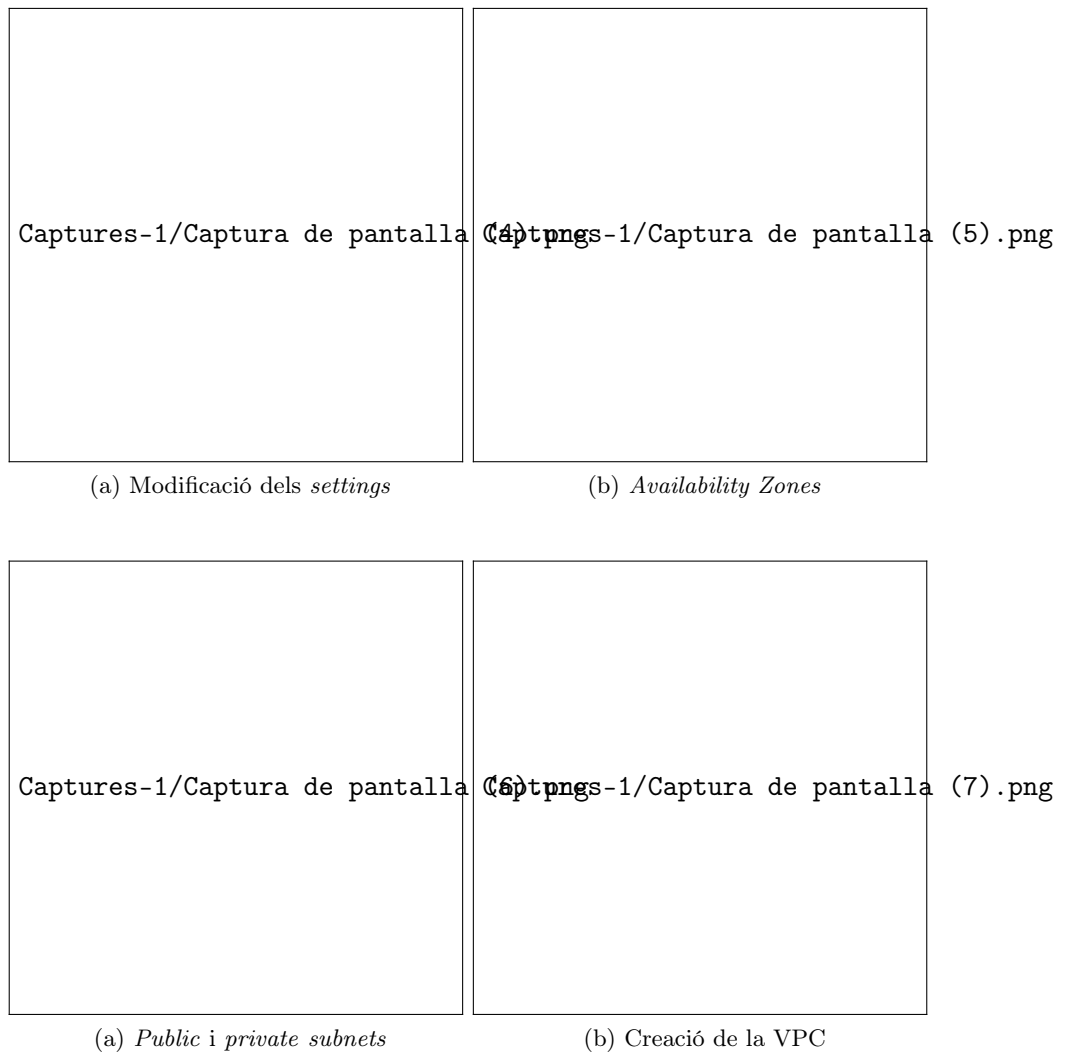


Figure 3: Configuració de la *VPC*

3.3.2 Creació de les *subnets* addicionals

Per tal d'obtenir una millor viabilitat del nostre *Web Server*, es procedeix a crear unes *subnets* addicionals en diferents zones de disponibilitat.

En el nostre cas s'ha decidit crear dos subxarxes addicionals (una pública i una privada).

Per a crear aquestes *subnets* cal accedir a la secció *subnets* situada a la part esquerra en el panell de navegació (tal i com és mostra a 6).

Una vegada situats allà, seleccionarem el botó *create subnet* per a introduir les característiques de la subxarxa.

El procés per a la creació d'una xarxa privada o pública és similar però no idèntic. Mostrem a continuació les dades a introduir per crear ambdues subxarxes:

- **Creació de *subnet* pública:**

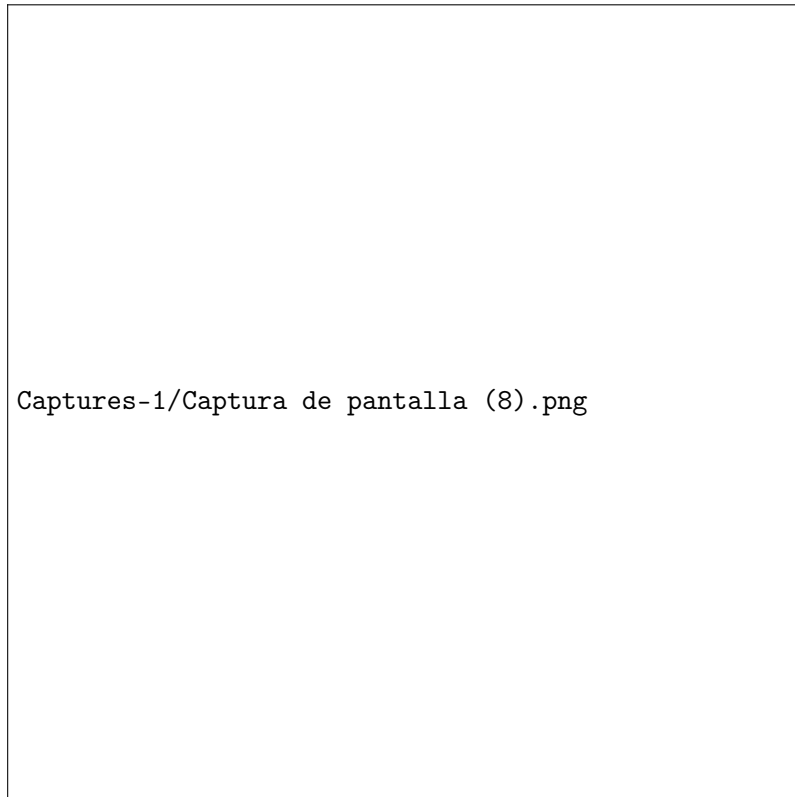


Figure 4: Esquema de la *VPC* creada

◦ **Creació de *subnet* privada:**

Un cop creades les subxarxes *public* i *private*, es configura la nova subxarxa privada creada per tal que es pugui connectar a internet, mantenint els recursos privats. Per poder fer-ho s'han de seguir els següents passos:

1. Escollir l'opció *Route tables*, seleccionant la subxarxa privada.
2. Al panell inferior, triar la pestanya *Routes*.

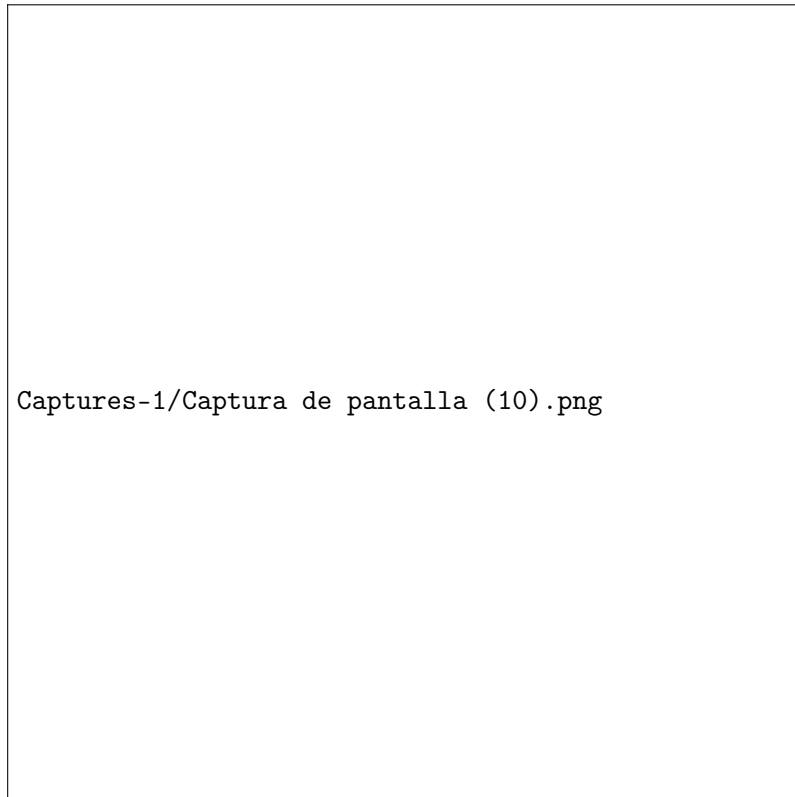
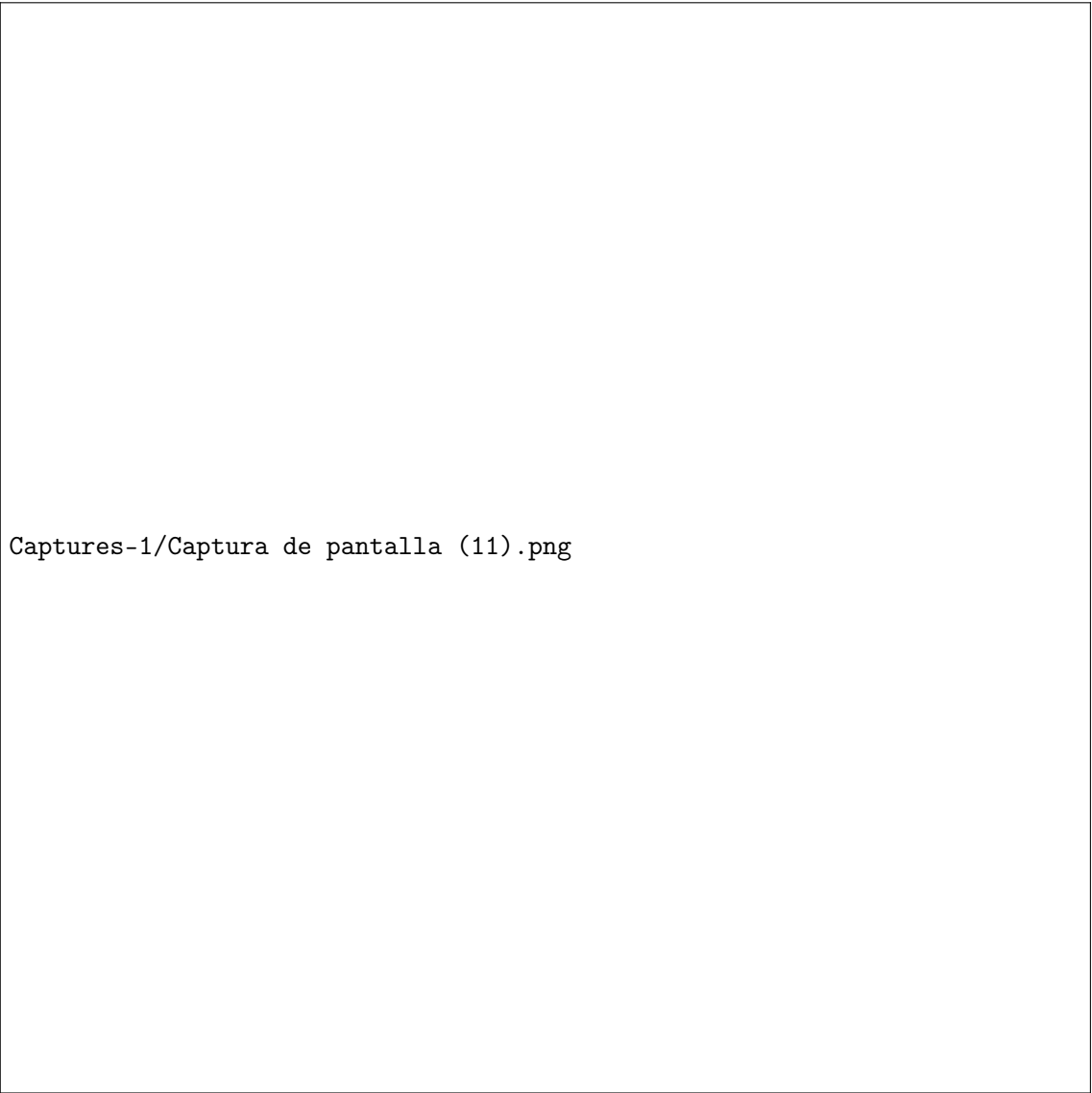


Figure 5: Detalls avançats de la xarxa

3. Triar la pestanya *Subnet associations* i Escollir *Edit subnet associations*.
4. Seleccionar tant la subxarxa privada 1, com la subxarxa privada 2 i clicar *Save associations*.
5. Confirmació d'èxit mitjançant el següent missatge:

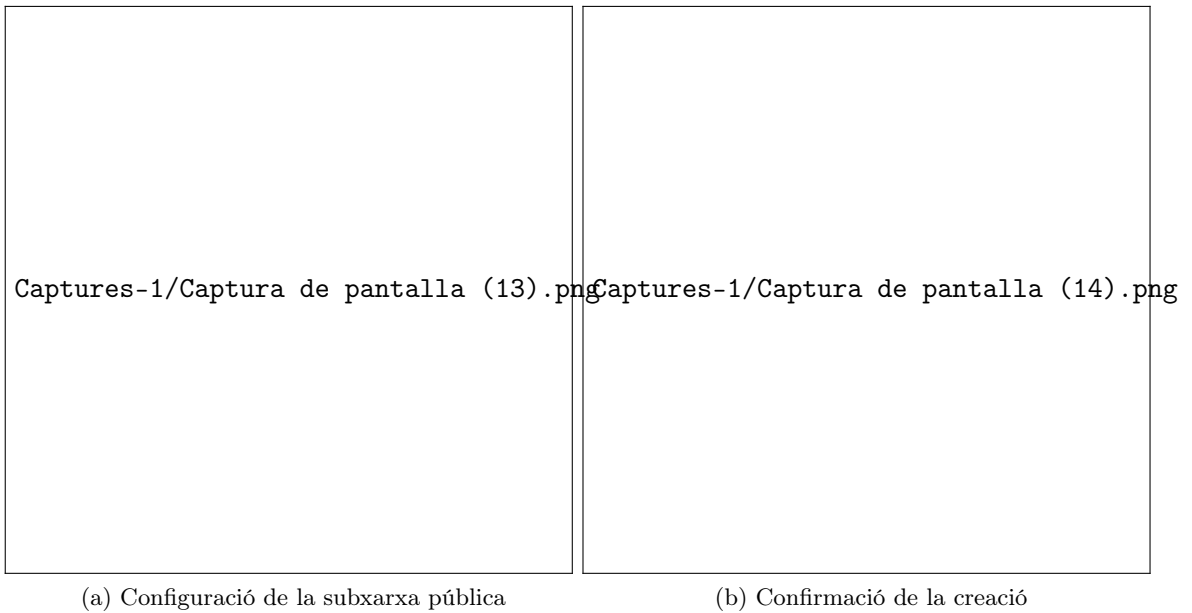


Captures-1/Captura de pantalla (11).png

Figure 6: Pantalla de gestió i creació de subnets

A continuació, es farà l'equivalent per a les subxarxes públiques, seguint els següents passos:

1. Escollir l'opció *Route tables*, seleccionant la subxarxa pública.
2. Triar la pestanya *Subnet associations* i Escollir *Edit subnet associations*.
3. Seleccionar tant la subxarxa pública 1, com la subxarxa pública 2 i clicar *Save associations*.

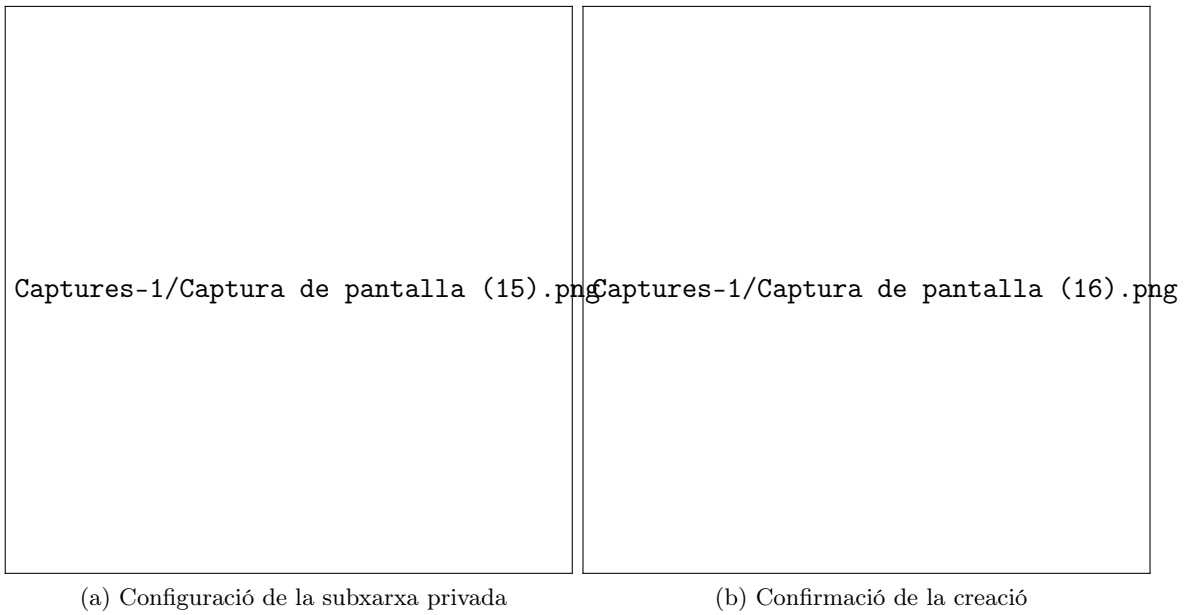


4. Confirmació d'èxit mitjançant el següent missatge:

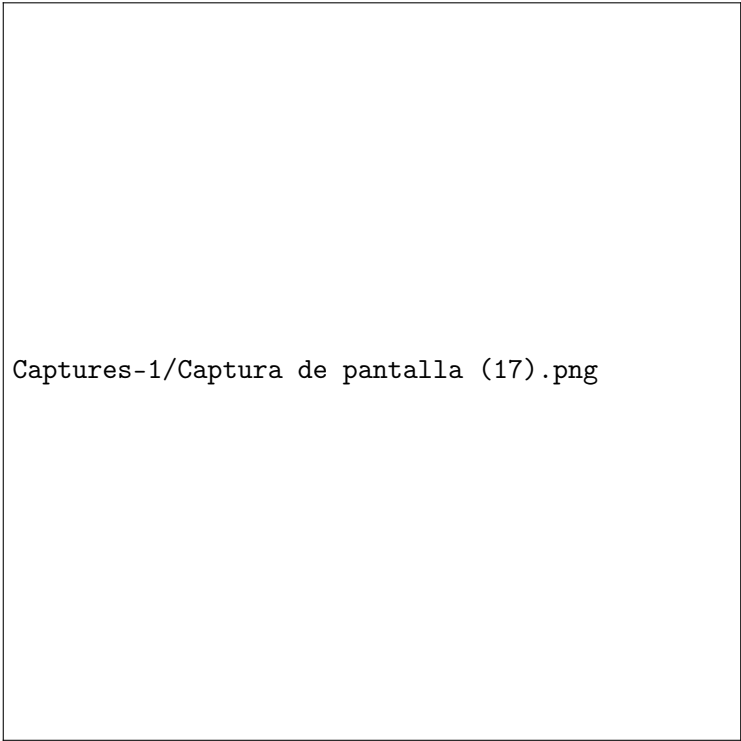
3.3.3 Creació del grup de seguretat de la VPC

Un cop creada la *VPC* i les subxarxes associades, es crea un grup de seguretat, que actuarà com un *firewall* virtual. Aquest grup de seguretat es llançarà juntament amb les instàncies que el tinguin associat, i seguirà unes certes normes segons les necessitats que es tinguin.

El primer pas és trobar l'apartat *Security groups* al panell de l'esquerra, i escollir l'opció *Create security group*, que es situa a la part superior dreta de la consola, tal com es mostra a la imatge 7:



A continuació, es crearà el grup de seguretat amb les següents característiques:
 Es mostrarà a continuació un missatge d'èxit com el de la imatge [9](#) conforme el grup de seguretat de la *VPC* ha sigut creat correctament, i el grup podrà ser utilitzat a l'apartat [3.3.4](#) quan llancem una instància *EC2*.



Captures-1/Captura de pantalla (17).png

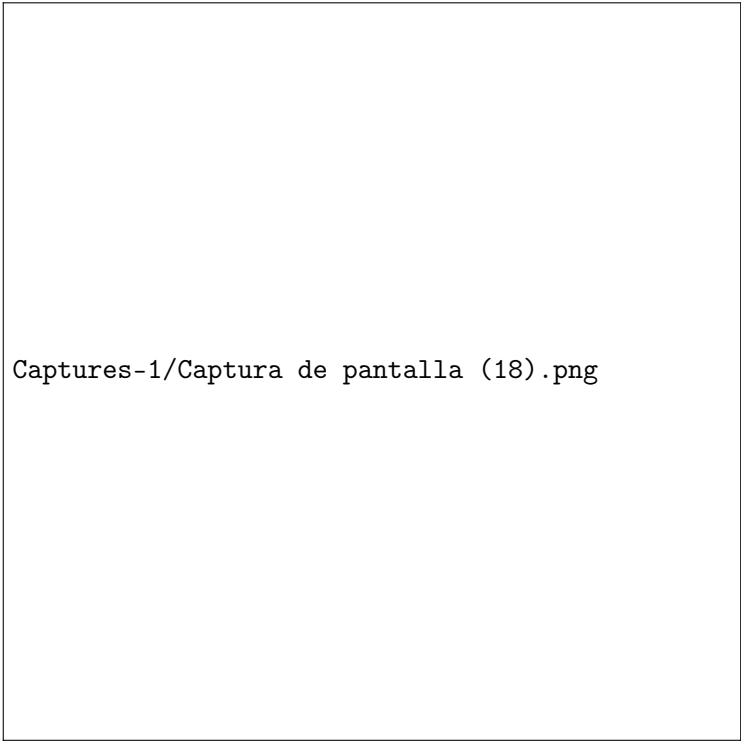
3.3.4 Llançament d'una *Web Server Instance*

En aquest apartat, l'objectiu és llançar una instància *EC2* dins la nova *VPC* creada a l'apartat ?? i configurar la instància de manera que es comporti com un servidor web.

Per tal de crear la instància cal cercar al panell *Services*, triar *EC2* i obrir la consola *EC2*, com es mostra a la imatge 10. Un cop posicionats a la consola, cal triar *Launch instance*:

A continuació es mostra la configuració escollida pel llançament de la instància pas per pas:

1. Posar *Web Server 1* com a nom de la instància i seleccionar *Amazon Linux* com a *AMI* per crear la instància.
2. Mantenir el tipus d'instància com *t2.micro*.
3. Escollir l'opció *vockey* del menú *Key pair name*.
4. Configurar la xarxa usant el grup de seguretat creat prèviament a l'apartat 3.3.3



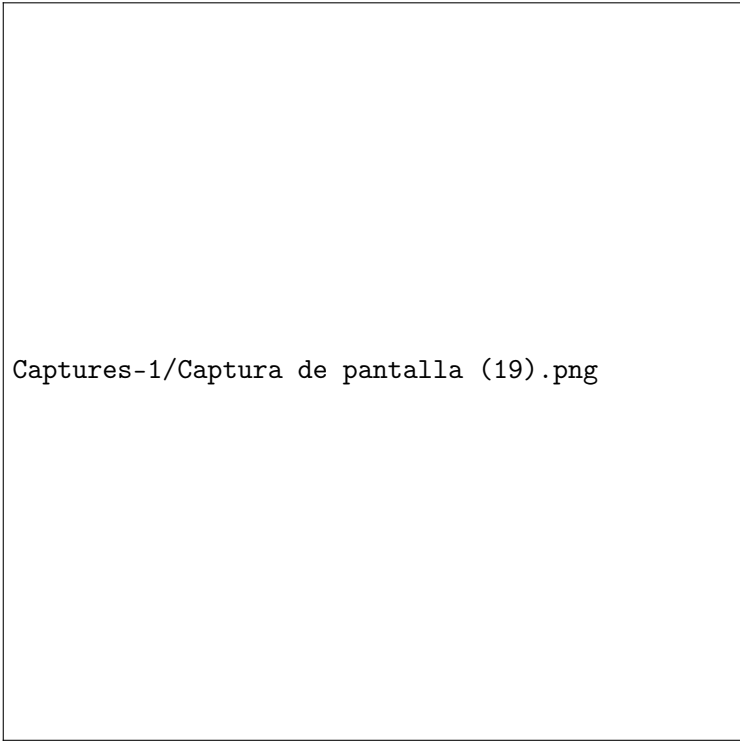
Captures-1/Captura de pantalla (18).png

5. Mantenir la configuració per defecte de la secció *Configure storage* i afegir el codi mostrat a continuació a l'apartat *User data* de la secció *Advanced details*.
6. Seleccionar *Launch instance* i confirmar que la instància ha sigut llançada correctament mitjançant un missatge d'èxit a la part superior de la consola.

Una vegada la instància *EC2* ha sigut llançada correctament, escollir *View all instances*. S'observa a la imatge [11a](#) com la instància encara està pendent de passar l'*Status check*, mentre que a la imatge [11b](#) es veu com ja està en correcte funcionament.

Per tal de comprovar que tant la instància com la VPC funcionen correctament i es pot accedir des de internet, cal seleccionar la instància creada, *Web Server 1* i copiar la *Public IPv4 DNS* mostrada a la secció *Details*, a la part inferior de la pàgina, tal i com es veu marcat a la imatge [11](#).

Per finalitzar, s'obre una nova pestanya del navegador, on s'enganxa la *Public DNS* de la instància creada, i es comprova que es pot accedir correctament, com es pot observar a la imatge [12](#).



Captures-1/Captura de pantalla (19).png

3.4 Laboratori completat

Una vegada s'ha completat el laboratori, ja es pot tancar escollint l'opció *End lab* a la part superior de la pàgina i prement el botó *Yes* per confirmar. Apareixerà a la pantalla la següent imatge:

3.5 Conclusions

Es finalitza l'informe afirmant que s'han assolit els objectius plantejats a [3.1](#), seguint els passos del laboratori.

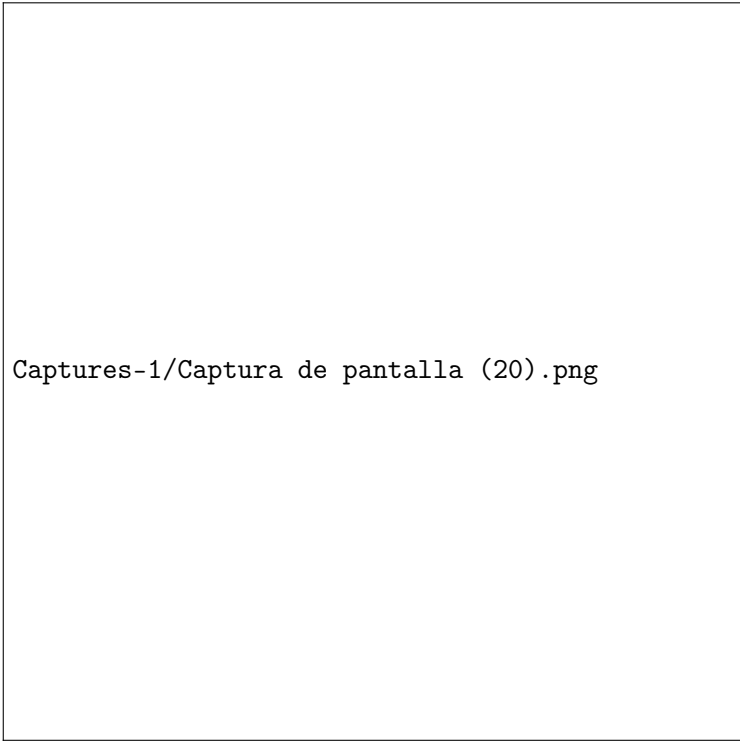
S'acaba la pràctica amb la confirmació de que s'ha millorat l'agilitat a l'hora de crear i modificar instàncies *EC2*.

S'ha entès com crear grups de seguretat que s'adaptin a les necessitats de la *VPC*, i com aplicar-los a una instància *EC2* creada posteriorment.

S'ha millorat la comprensió sobre les *VPC* aplicant la teoria feta a classe a un exemple pràctic, i s'ha provat la creació de subxarxes tant privades com públiques.

S'ha après a visualitzar les xarxes i subxarxes creades mitjançant detalls avançats.

S'ha vist també que *AWS* usa reiteradament missatges d'èxit per tal de confirmar les accions que es realitzen a la consola, i s'ha entès la importància d'aquests per tal d'avançar correctament en la creació de xarxes i instàncies.



Captures-1/Captura de pantalla (20).png

4 Sessió 2: Llençament d'una Web server amb VPC

4.1 Objectius

Els objectius plantejats en aquesta sessió són:

- Ser capaços de crear una *VPC* amb diverses subxarxes, sense seguir el manual.
- Modificar les característiques de les xarxes privades, per tal de poder accedir a elles des del navegador.
- Crear instàncies de tipus Ubuntu.
- Aplicar la teoria i la pràctica apreses en les sessions anteriors.

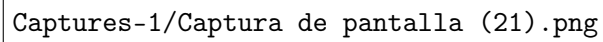
4.2 Metodologia

Per tal d'assolir els objectius proposats a la sessió, s'ha usat el *Sandbox* subministrat pel curs que otorga *AWS*.

A més, s'ha utilitzat el coneixement assolit prèviament a la sessió 1 i s'han seguit les indicacions del professor per a diverses qüestions i dubtes surgits, sobretot a l'hora de llançar les instàncies.

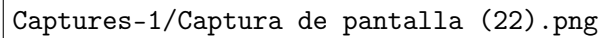
Mencionar també, que la metodologia del treball s'ha basat en recopilar imatges i informació dels passos realitzats pel llançament de 4 *Web Servers*, 2 públics i 2 privats, per facilitar la redacció de l'informe i poder analitzar el procés.

S'ha subdividit el treball en 4 etapes diferents:



Captures-1/Captura de pantalla (21).png

- Creació de la *VPC* amb 4 subxarxes.
- Llançament d'una instància *EC2* a cada subxarxa.
- Comprovació d'accés a les instàncies.
- Modificació de les subxarxes privades per poder accedir al servidor des del navegador.



4.3 Desenvolupament

4.3.1 Creació de la VPC i de les subxarxes

Seguint el procediment de la sessió 1 explicat anteriorment, creem la VPC de forma similar.

Per altra banda, decidim directament indicar a la VPC en el moment de creació que hi dispondrem de dos subxarxes públiques i privades (que estaran repartides uniformament en dos zones de disponibilitat per tal de donar així una millor seguretat del servidor web).

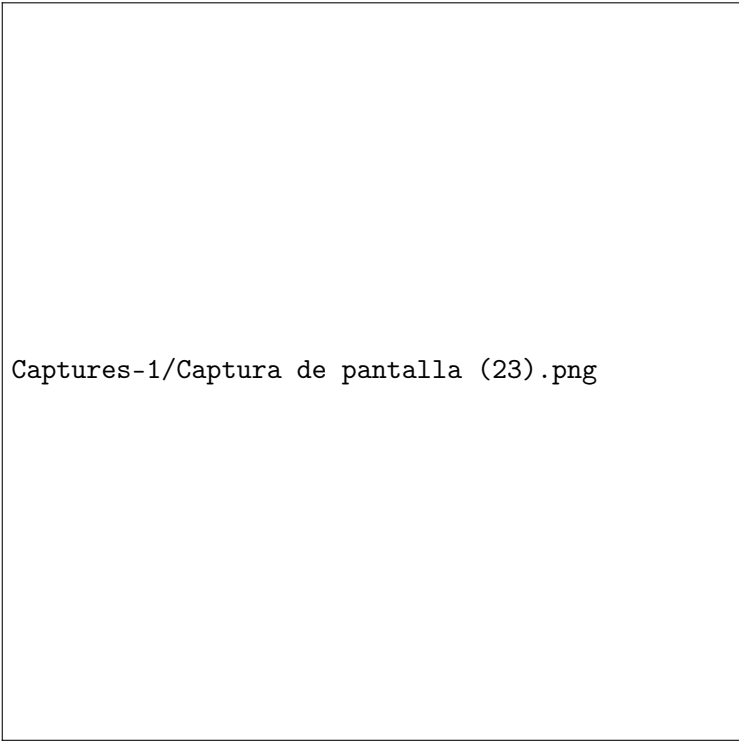
Procedim indicant també que introduïrem una *NAT-Gateway* en cada zona de disponibilitat i, finalment, no introduïm cap punt d'enllaç a la VPC.

Comentar també s'han modificat certs paràmetres de les subxarxes creades; concretament s'ha modificat la direcció IP de les mateixes de la següent forma:

Subxarxa (<i>etiqueta</i>)	IPv
go-subnet-public1-us-east-1a	10.0.0.0/24
go-subnet-private1-us-east-1a	10.0.1.0/24
go-subnet-public2-us-east-1b	10.0.2.0/24
go-subnet-private2-us-east-1b	10.0.3.0/24

Table 1: Direccions IP de les diferents subxarxes

Finalment, la *VPC* segueix el següent esquema:



Captures-1/Captura de pantalla (23).png

4.3.2 Llençament de les instàncies

El plantejament següent és similar al ja explicat. Anomenem a les instàncies (que en el nostre cas seràn instàncies *EC2*) com *Server i* (o *Server i privada* en cas de tractar-se d'una instància que estarà associada a una subxarxa de la VPC privada) on $i \in \{1, 2\}$ que indica si està a la zona 1 o la zona 2 (*us-east-1a* o *us-east-1b* respectivament).

Indiquem quina mida desitgem (que en el nostre cas es tracta d'una *t2 micro*), sel·leccionem també com a màquina virtual la distribuïdora *Ubuntu*¹ i sel·leccionem com a clau d'accés la *vockey*.

Modifiquem la configuració de xarxa per configurar la instància a la VPC creada per a la sessió i introduïnt-li la subxarxa corresponent a la instància.

També, es sel·lecciona la regla de seguretat que s'utilitzarà per accedir-hi (la de la VPC).

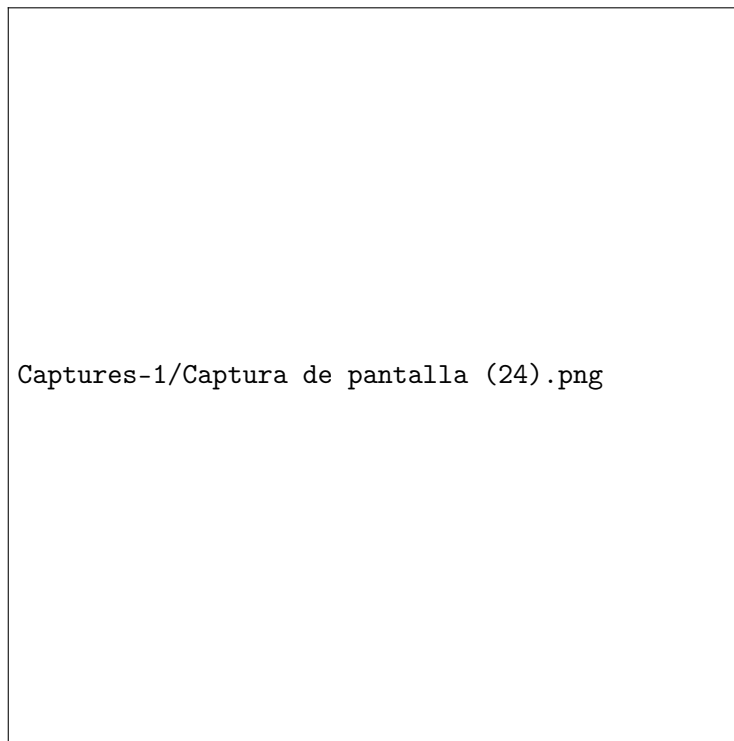
En el nostre cas, com no s'ha creat inicialment la regla de seguretat, a l'hora de crear la primera instància s'ha aprofitat per a fer la seva declaració.

Hem anomenat aquesta regla de seguretat de la forma per defecte (ja que no es declararan més regles i les creades per l'ambient de proves Sandbox del *AWS* són clarament identificables), *launch-wizard-1*.

La regla declarada permet l'accés a una pàgina web sezilla que mostra un missatge per pantalla des de qualsevol IP mitjançant el protocol HTTP.

Una vegada indicada la regla de seguretat de la VPC, s'introdueix el codi que execu-

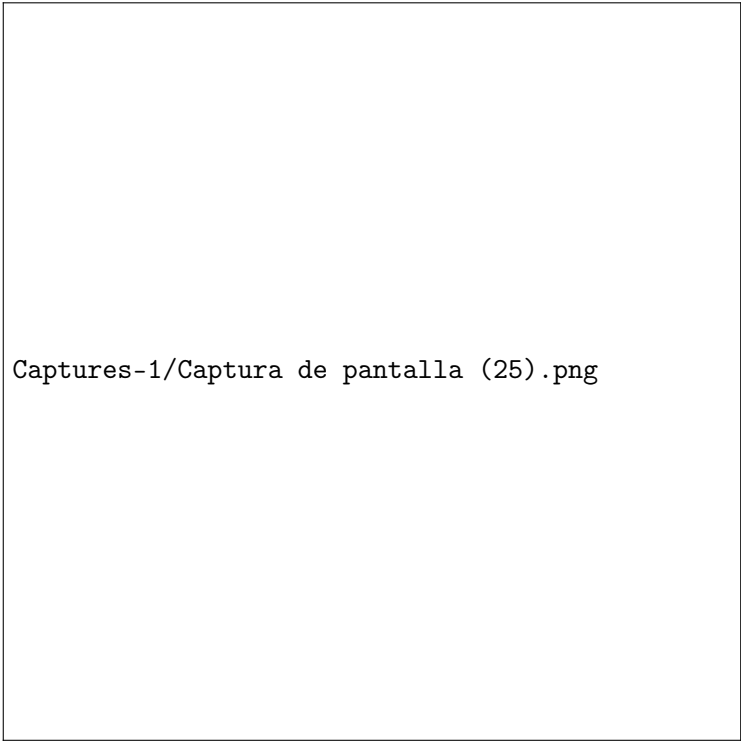
¹S'ha escollit la màquina virtual Ubuntu per un problema en el llançament de l'última versió de la màquina virtual d'Amazon Linux.



tarà per la màquina virtual al iniciar-se.

Mostrem ara el codi introduït a una de les instàncies com a exemple:

```
#!/bin/bash
apt update
apt -y install apache2
echo "<html>My web page</html>" > /var/www/html/index.html
```



Captures-1/Captura de pantalla (25).png

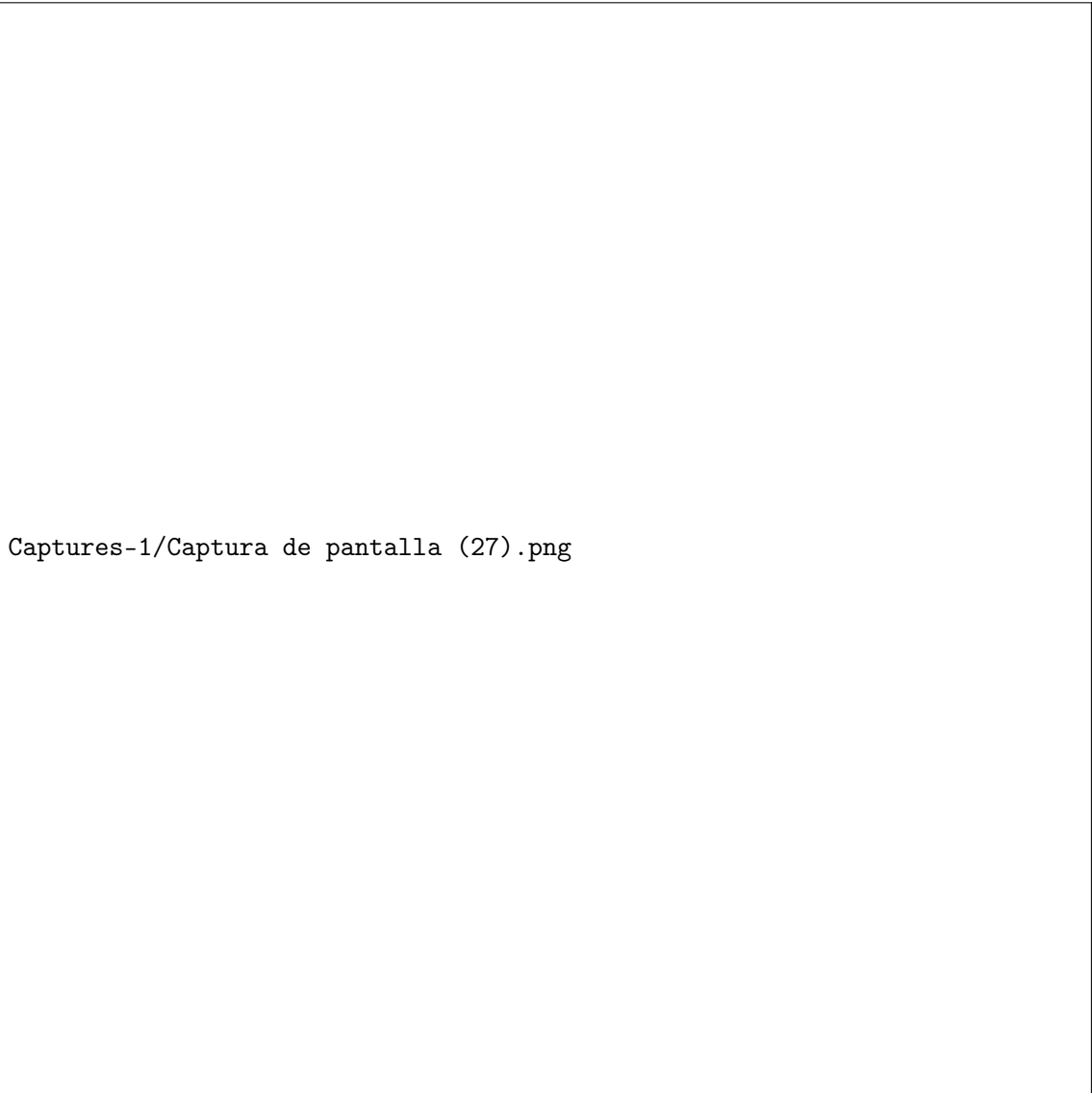
4.3.3 Comprovacions d'accés a les instàncies

Posteriorment a la creació de les instàncies es decideix provar la connexió amb aquestes, inserim ara els resultats obtinguts:

Observem com a les subxarxes públiques l'accés es permet per contra de les privades que deneguen l'accés.

Com a part de la sessió s'ha proposat modificar les característiques de les subxarxes privades per tal de tornar-les públiques (capaces d'acceptar l'accés des de internet).

Es mostra en la següent secció les modificacions fetes a les subxarxes privades i els resultats obtinguts per a tornar-les públiques.



Captures-1/Captura de pantalla (27).png

Figure 7: Creació del grup de seguretat

4.3.4 Modificació de les subxarxes privades

Per tal de "transformar" les subxarxes privades en públiques s'ha probat varies coses, expliquem el nostre primer intent i l'últim (que és el que va donar els resultats que esperàvem).

Primer intent: Habilitar clau pública

El nostre primer intent va ser, des de l'apartat de subxarxes en el panell de l'VPC, sel·leccionar la red privada a modificar i en el panell que s'obria al clicar s'obre *acciones*, entrar en el apartat *habilitar configuración de subred*.

D'aquesta forma apareixia una pantalla per a modificar paràmetres de la subxarxa.

Un dels paràmetres era una casella que habilitava l'assignació automàtica de la IP.

Al no trobar-se inicialment sel·leccionada, assumíem que aquest requisit havia d'estar acti-

1. Modificar el nom, descripció i VPC del grup de seguretat.
2. Escollir l'opció *Add rule*, del panell *Inbound rules*.
3. Configurar el Type, Source i Description del grup de seguretat.
4. Baixar al final de la pàgina i clicar *Create security group*.

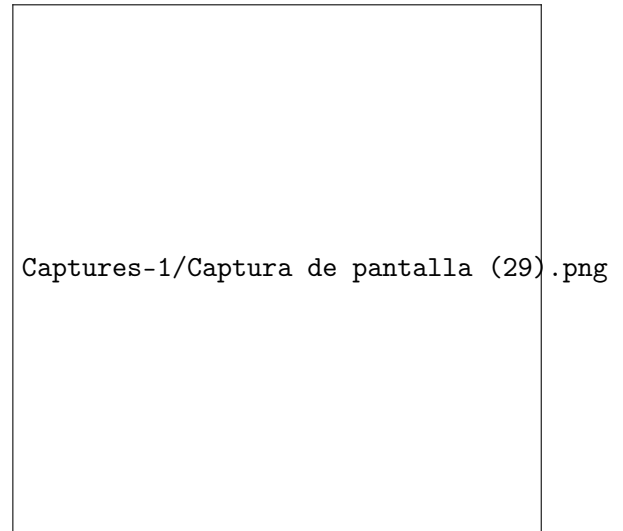


Figure 8: Creació d'un grup de seguretat

vat per a ser una xarxa pública.

Els resultats no van ser els esperats (òbviamment).

Al no obtenir resultat vam interpretar l'esquema que estabem fent del servidor web (l'arquitectura de la VPC); d'on vam intuïr que el que feia que una xarxa fos pública o privada era que devia accedir mitjançant una *NAT-Gateway*.

Per aquest motiu ens vam enfocar en modificar la ruta d'accés de la subxarxa.

Últim intent: Modificar la ruta d'accés

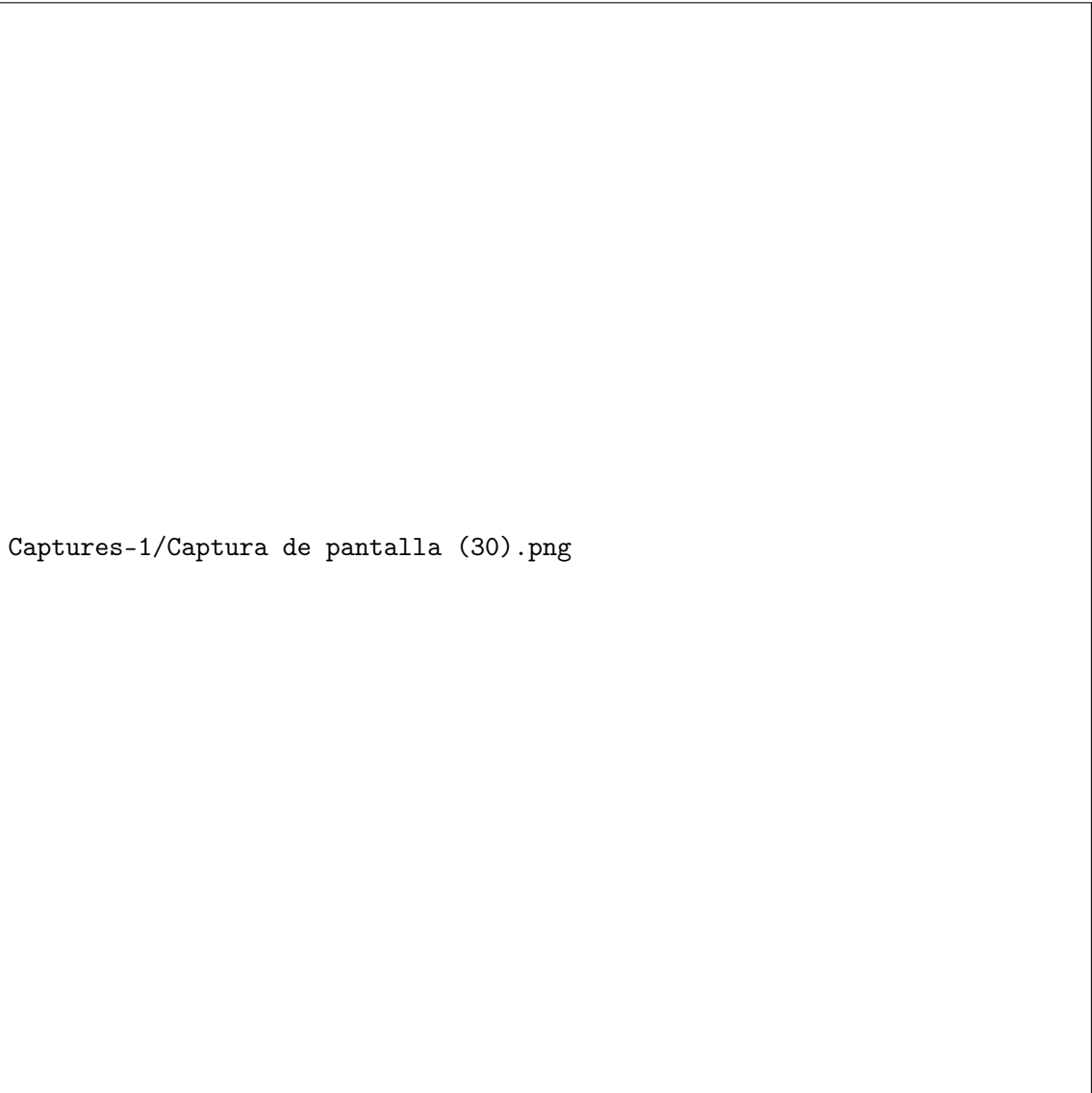
Similar al procediment anterior, sel·leccionem la subxarxa a modificar i anem a l'apartat de rutes ubicat al panell inferior que apareix al sel·leccionar una subxarxa.

Una vegada allà cliquem al botó: editar rutes.

En el destí 0.0.0.0/0 (que indica que tothom pot accedir-hi), eliminem el destí (que es tracta de la *NAT-Gateway*) i el substituïm per el *igw-0b6918a4a72ddc65f*.

Aquest canvi fa que des de internet qualsevol persona pugui accedir al *web server* que abans era privat.

Mostrem ara els resultats de la modificació:



Captures-1/Captura de pantalla (30).png

Figure 9: Missatge d'èxit del *Security Group*

4.4 Conclusions

Es finalitza l'informe de la segona sessió confirmant l'assoliment dels objectius plantejats a 4.1, afirmant que s'ha sigut capaç de crear una VPC amb 4 subxarxes, 2 de públiques i 2 de privades, i llançar instàncies a cada una d'elles, sense la necessitat de consultar els passos del laboratori anterior.

Mitjançant les diverses proves fetes, s'han descobert noves formes de fer algunes parts del procés, com per exemple la creació d'un grup de seguretat mentre es crea la instància enlloc de fer-ho abans a l'apartat especialitzat.

S'han descobert algunes de les limitacions del Sandbox, i per evitar errors s'ha après com llançar una imatge de tipus Ubuntu.

S'ha millorat la comprensió dels missatges d'error que proporciona *AWS*, i s'ha guanyat

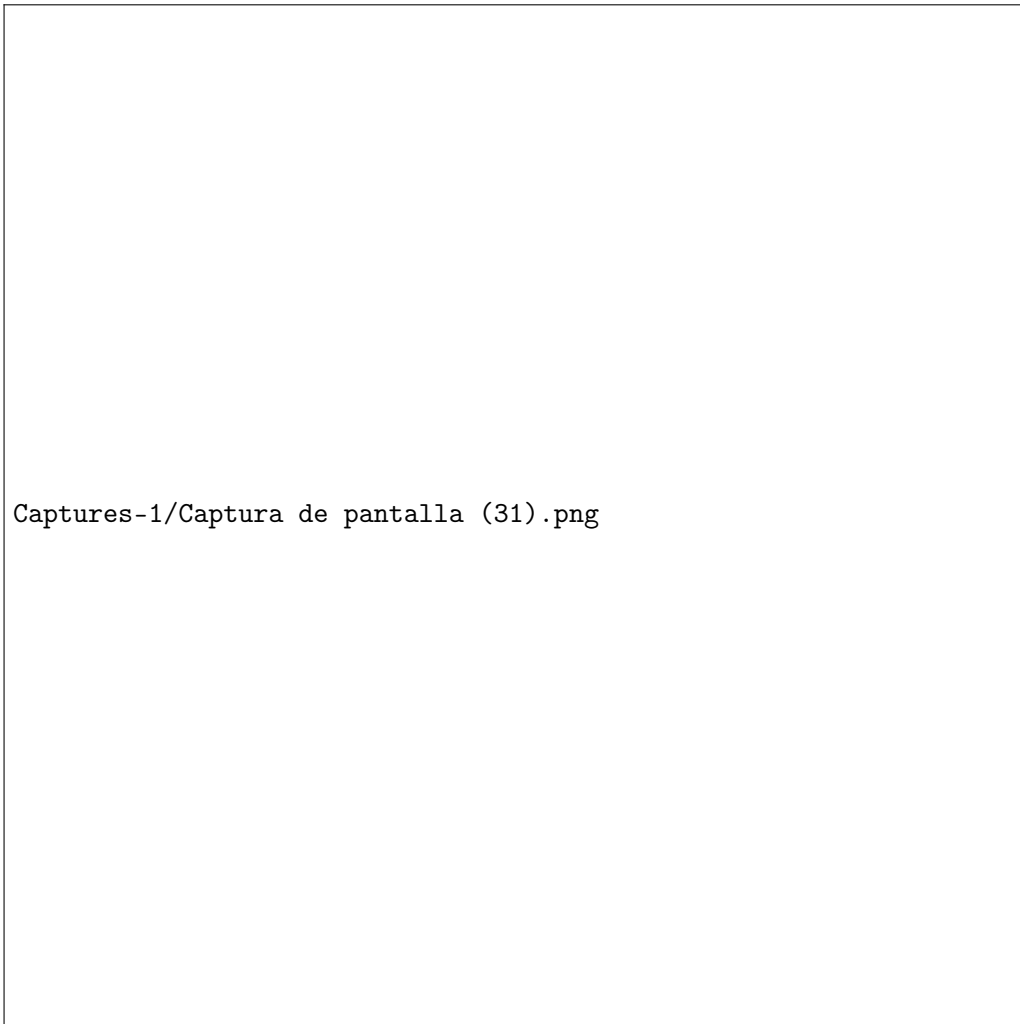
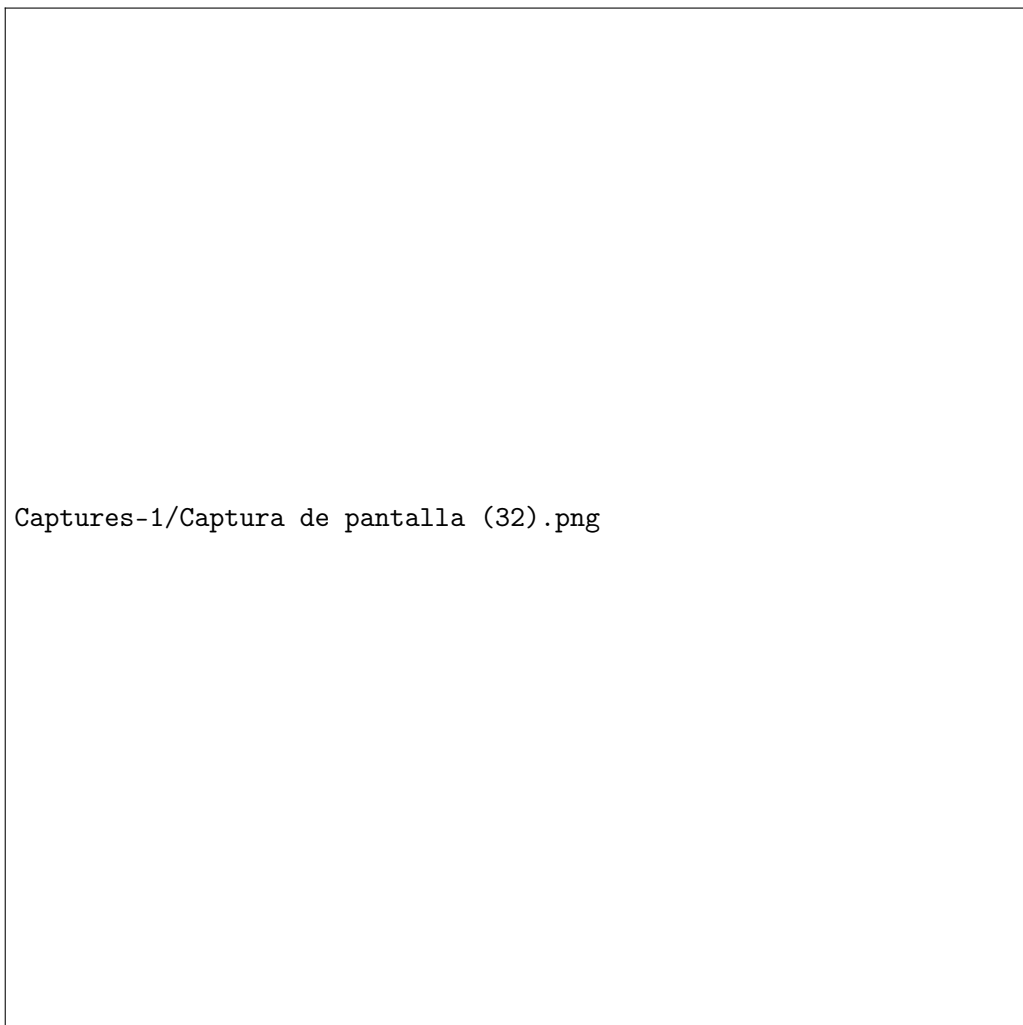


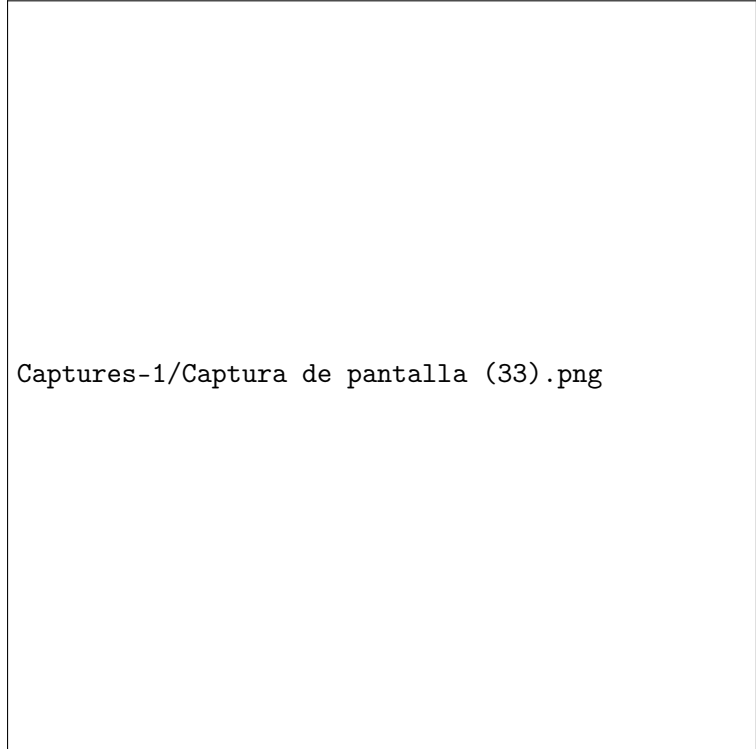
Figure 10: Llançament d'una instància *EC2*

agilitat a l'hora d'investigar com solucionar-los.

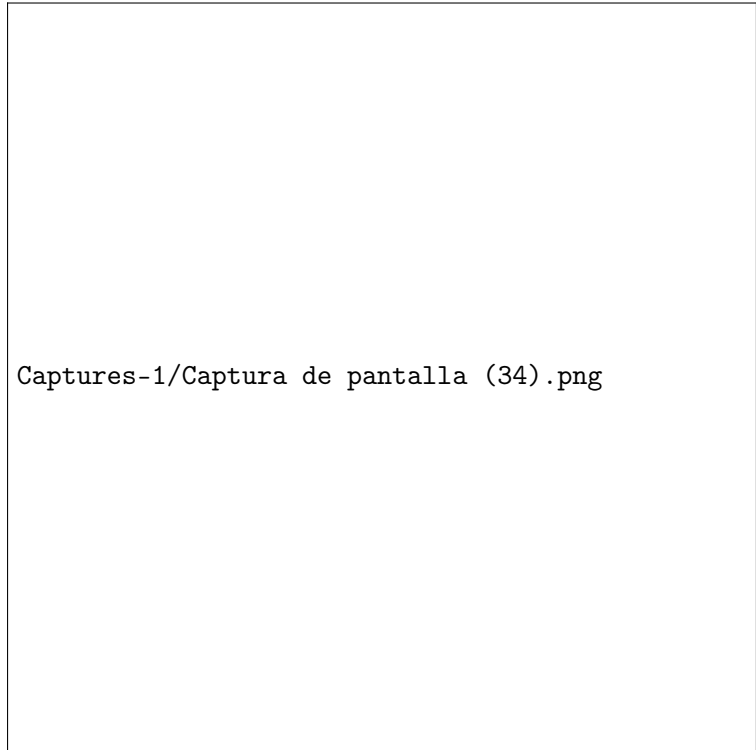
S'ha guanyat agilitat a l'hora de moure's per l'entorn *AWS*, i s'han posat en pràctica de forma autònoma la creació de subxarxes, instàncies i la modificació de les subxarxes privades.



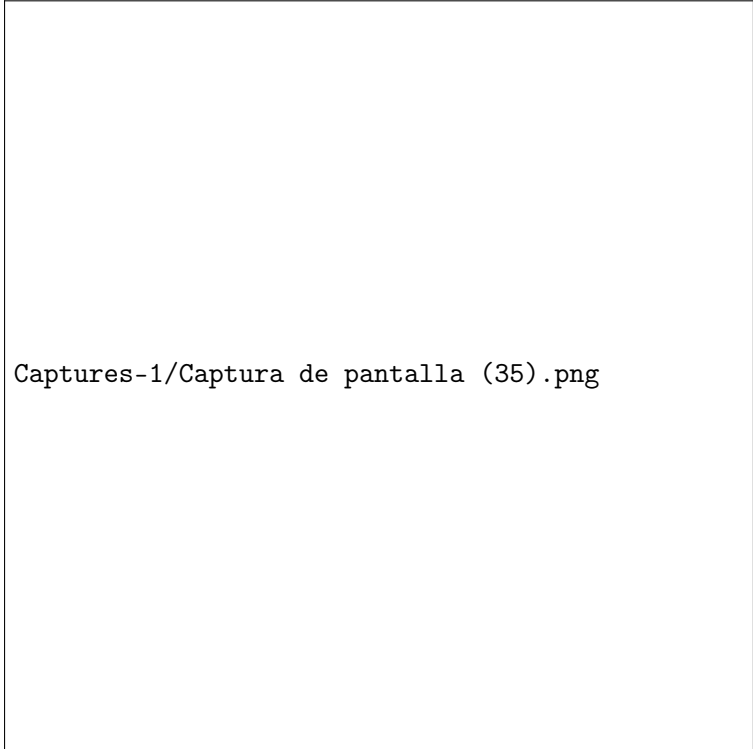
Captures-1/Captura de pantalla (32).png



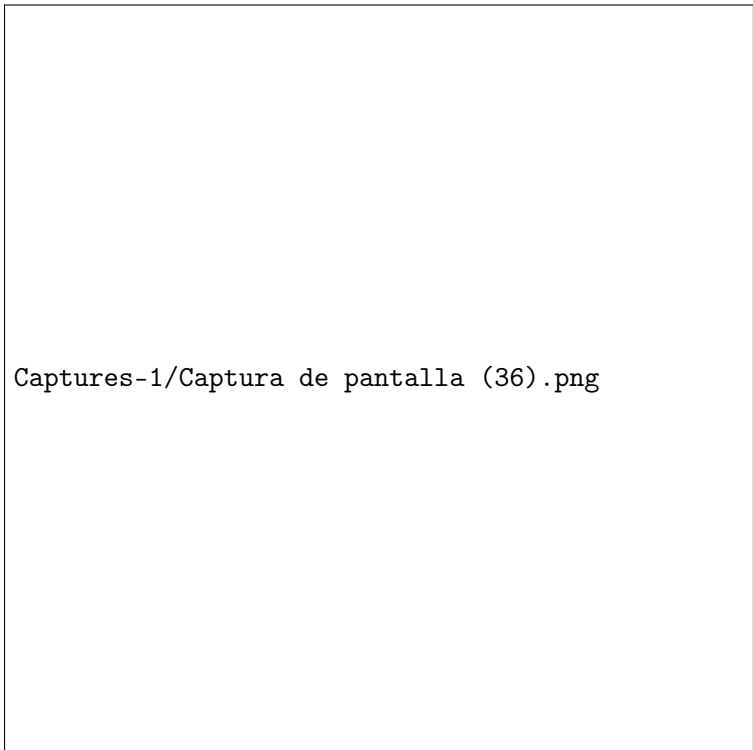
Captures-1/Captura de pantalla (33).png



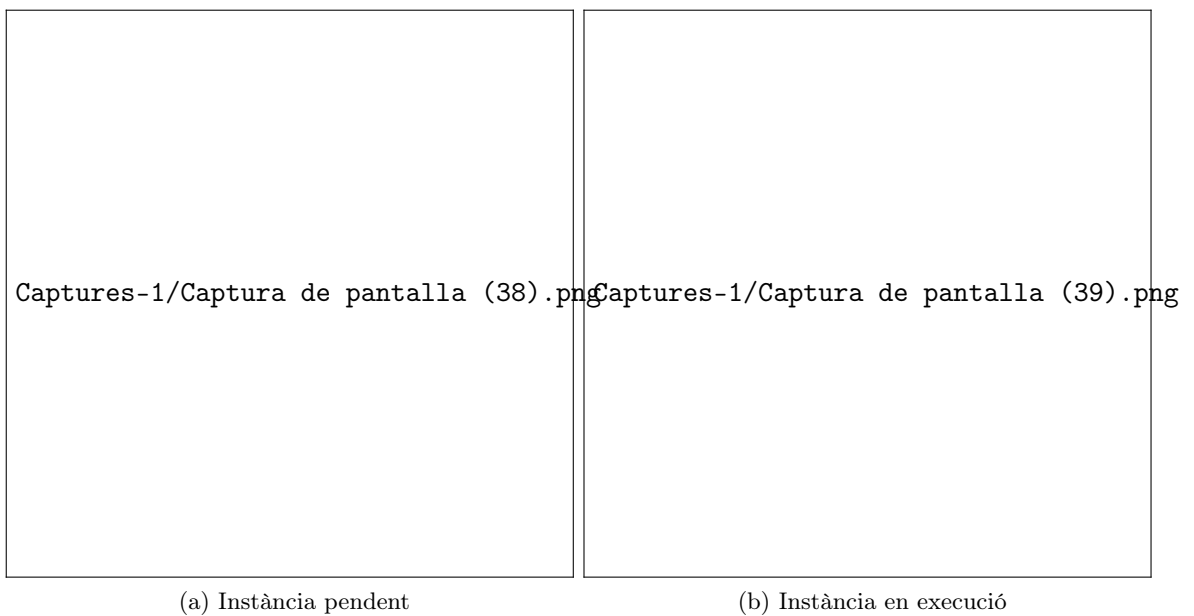
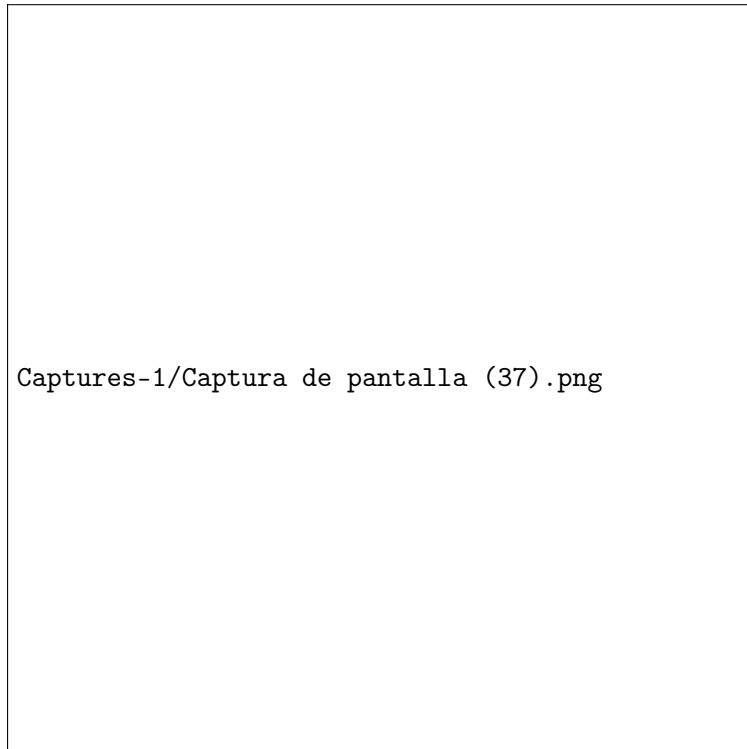
Captures-1/Captura de pantalla (34).png

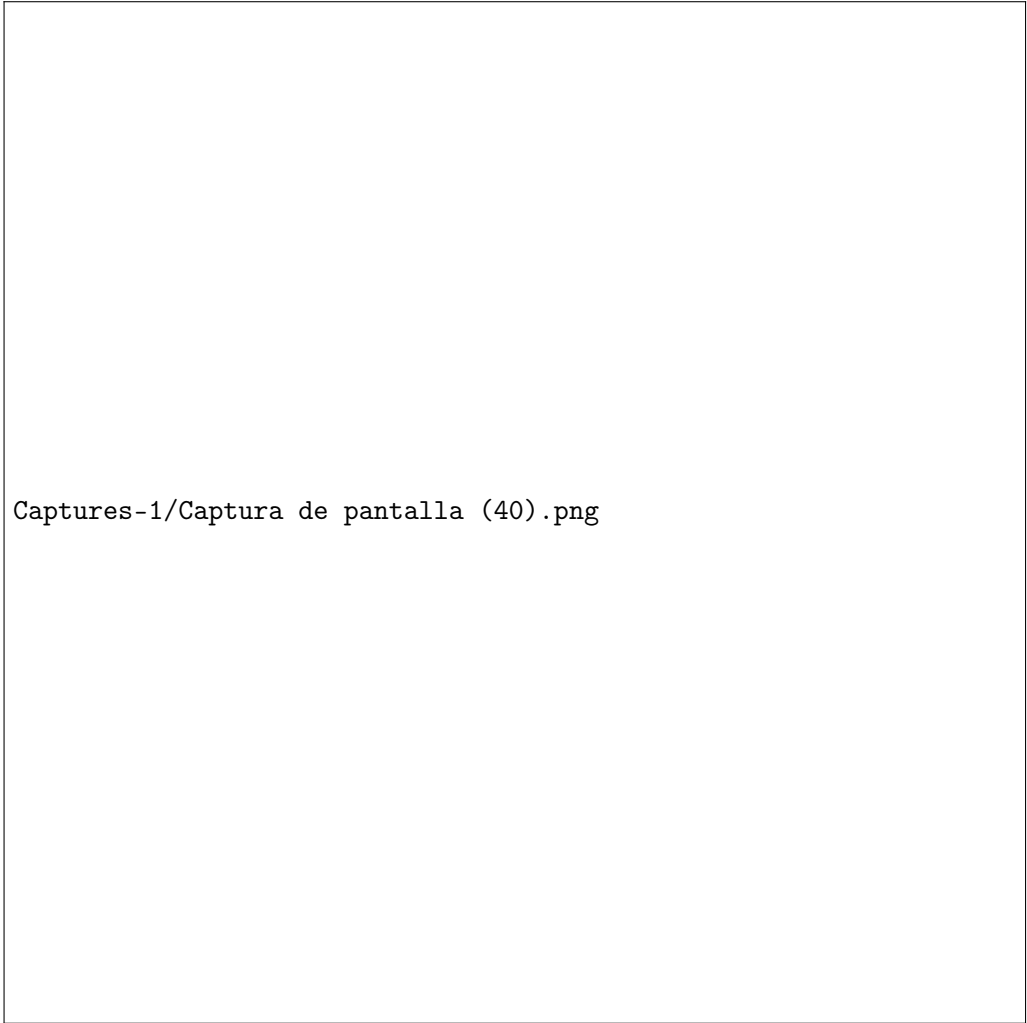


Captures-1/Captura de pantalla (35).png



Captures-1/Captura de pantalla (36).png





Captures-1/Captura de pantalla (40).png

Figure 11: *Public IPv4 DNS* de la instància *Web Server 1*

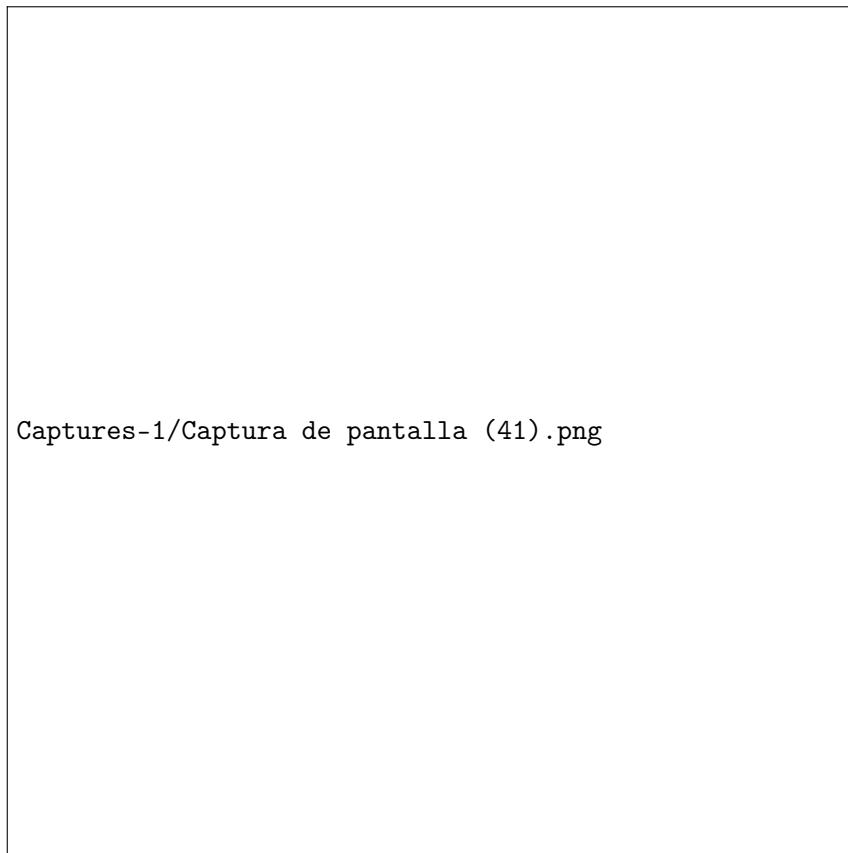
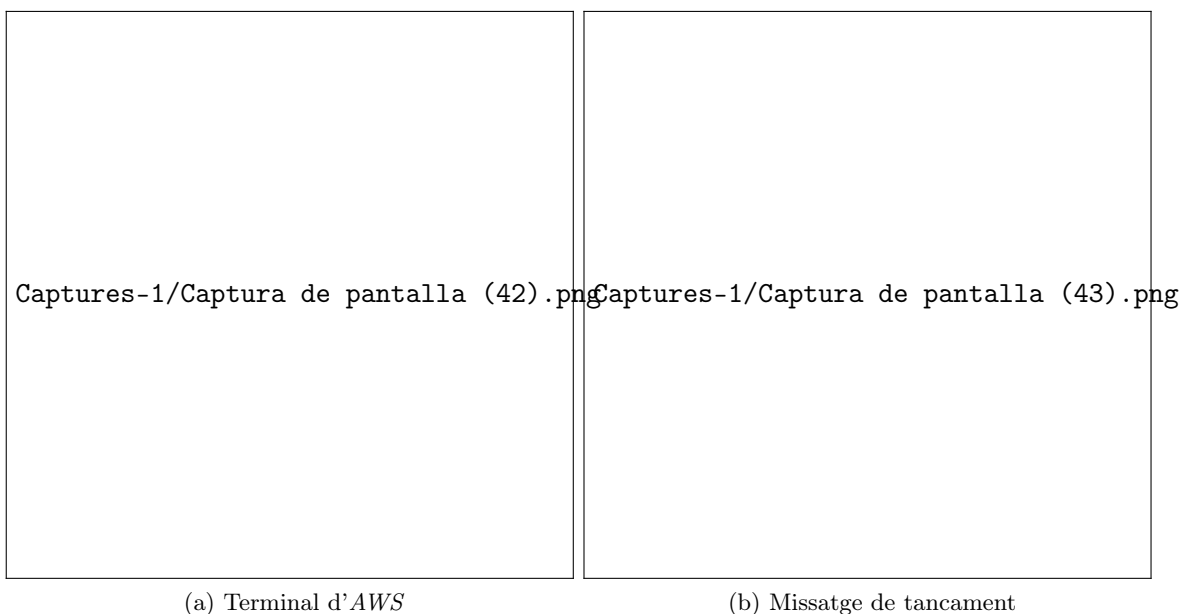


Figure 12: *Accés pel navegador a Web Server 1*



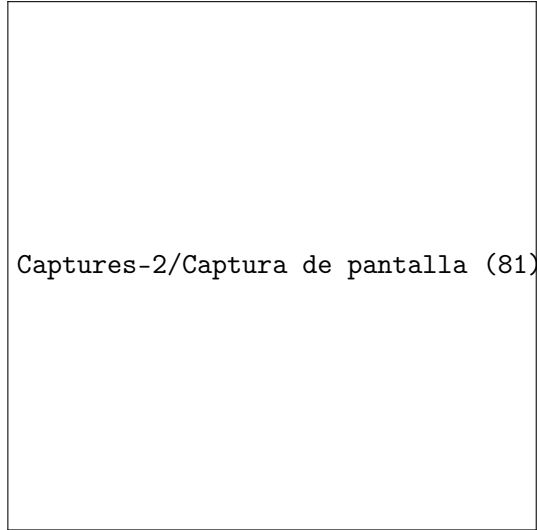
(a) Terminal d'AWS

(b) Missatge de tancament

Figure 13: Tancament del laboratori

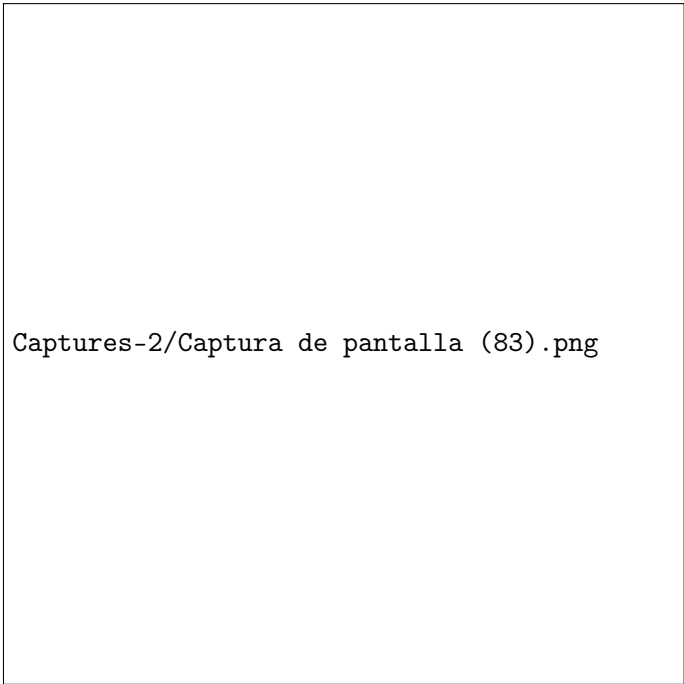
En el nostre cas, per aquesta sessió, introduïm com a nom de la VPC on situarem les subxarxes com *GO* i, d'aquesta manera, definirem tots els requeriments de la VPC mitjançant aquesta etiqueta, tal i com es pot veure a la imatge mostrada a la dreta.

S'indica també que es crearan altres recursos addicionals, i s'observa a la dreta com es va creant la taula de rutes de la xarxa.



Captures-2/Captura de pantalla (81).png

Figure 14: Creació de la *VPC*



Captures-2/Captura de pantalla (83).png

Figure 15: Visualització de la *VPC*

Comentar finalment que el procés d'incialització de les instàncies s'ha fet una a una però que hauria estat més eficaç haber fet una imatge de la primera instància creada i, per tant, anar fent còpies de la imatge modificant la subxarxa que li correspondria.

Per cada llançament d'imatge, s'ha obtingut una confirmació d'èxit com la de la imatge que es mostra a la dreta.

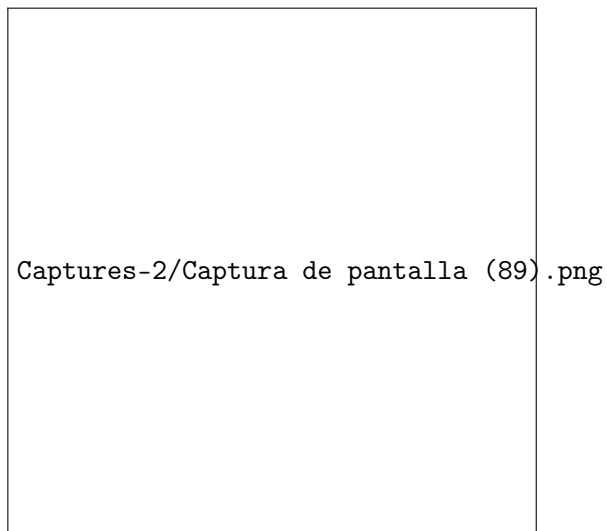
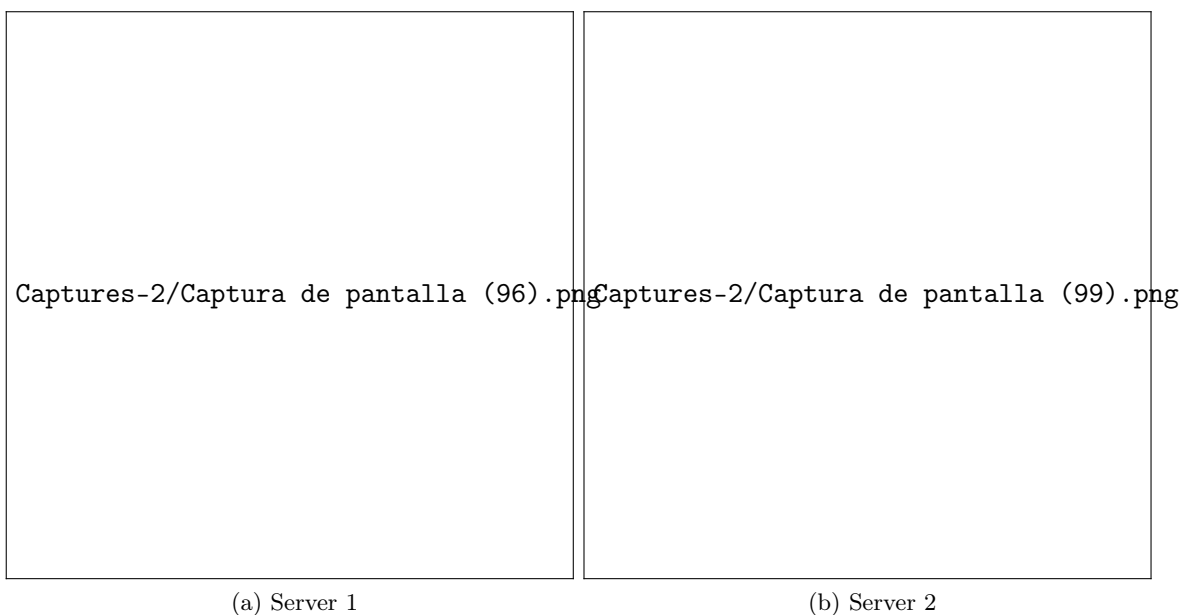


Figure 16: Missatge d'èxit del llançament



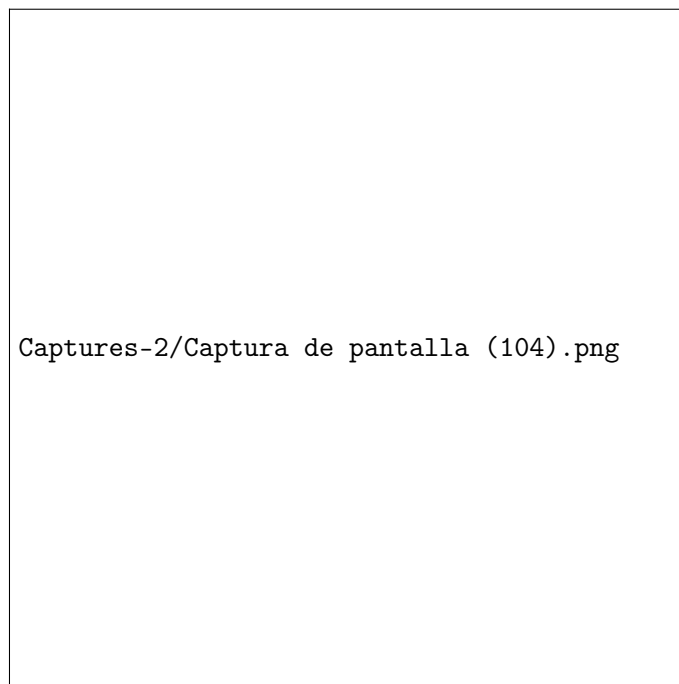
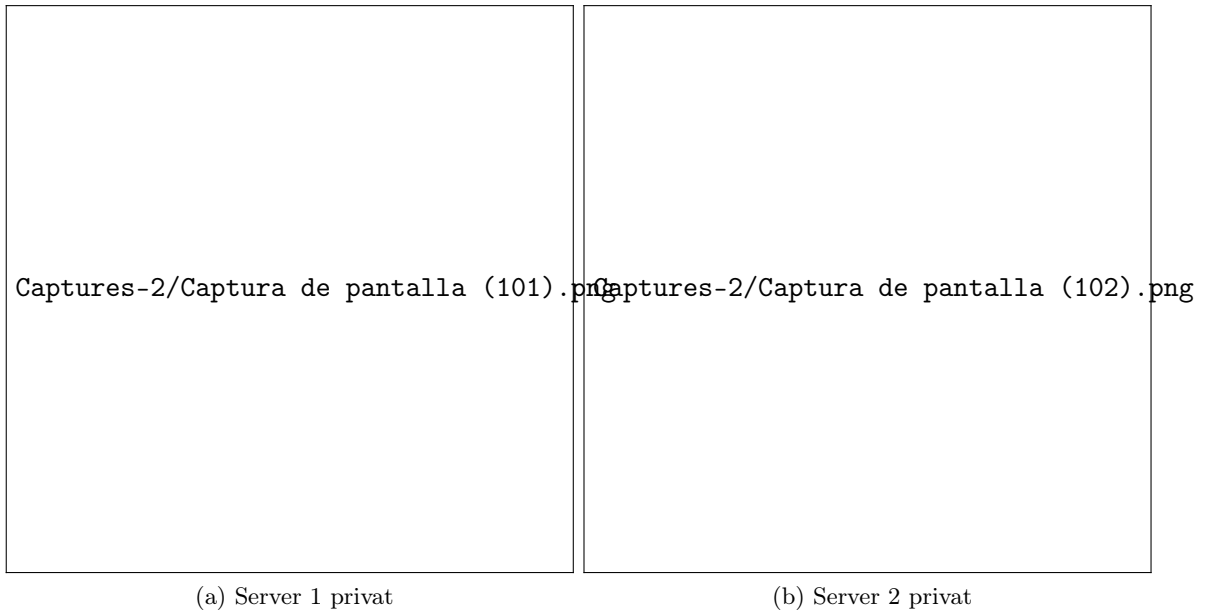


Figure 17: Habilitació de clau pública

