📎 UDXXP01.- Configuració d'un bastion host a AWS

Objectiu

L'objectiu de la pràctica és configurar un host bastió a AWS, amb accés SSH des d'internet, per poder administrar la nostra infraestructura en el núvol.

Requisits:

En primer lloc, configurarem dos grups de seguretat:

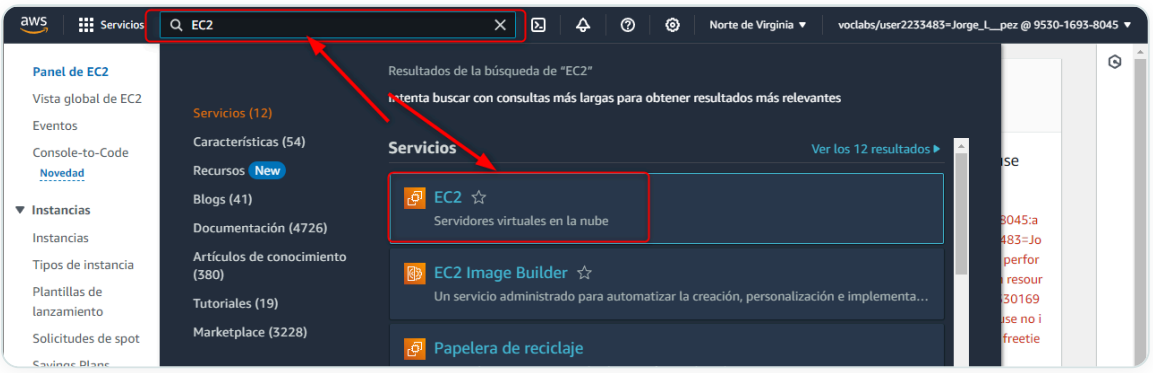
- ssh-internet: permetrà connectar des d'internet al port 22 de les instàncies EC2 que apliquen el grup de seguretat.
- Internet: permetrà l'accés a internet des de les instàncies EC2 que apliquen el grup de seguretat.

Posteriorment, desplegarem una instància EC2, configurada amb els grups de seguretat definits, i amb el sistema operatiu Ubuntu Server 24.04.

Una volta configurat el servei SSH a la nova instància, podrem connectar amb el nostre client SSH favorit:

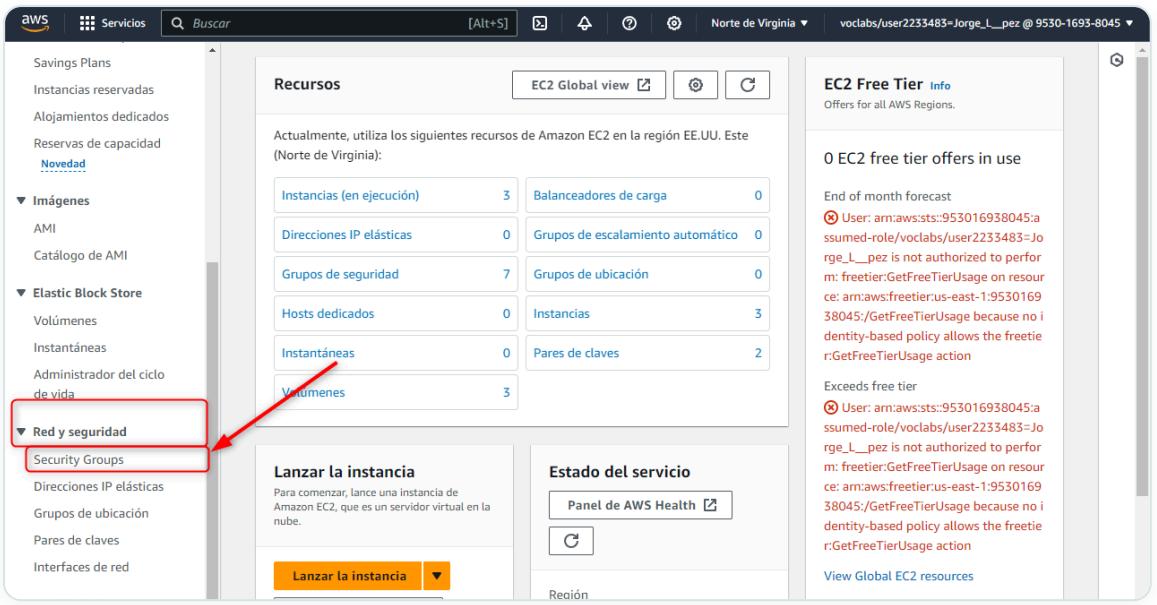
Creació dels grups de seguretat:

Accedim al panell d'EC2, al nostre compte d'AWS academy:



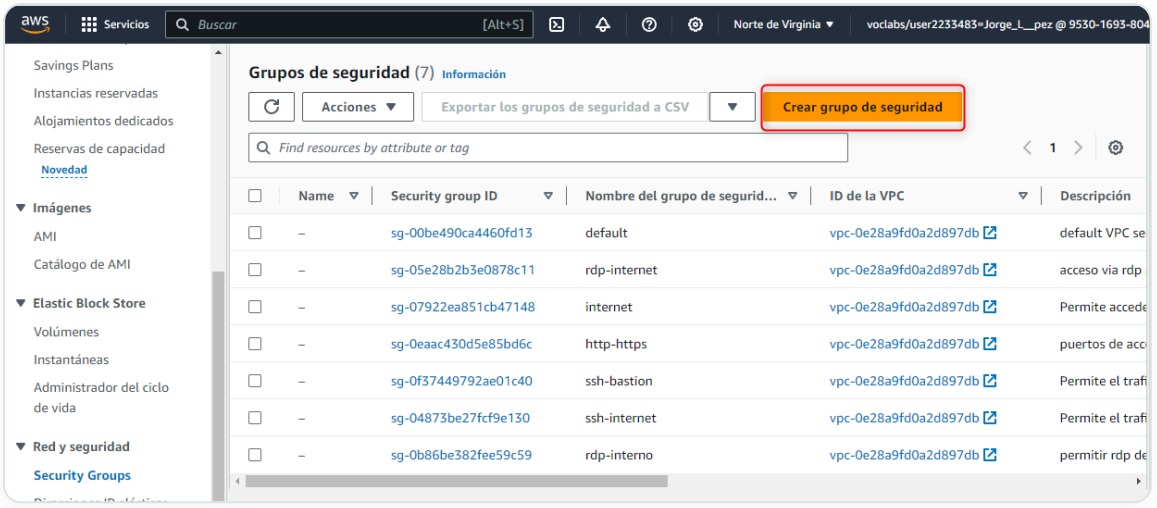
Cerca d'EC2 al cercador de serveis.

Dins del panell d'EC2, busquem l'opció "Security Groups", al menú de l'esquerra.



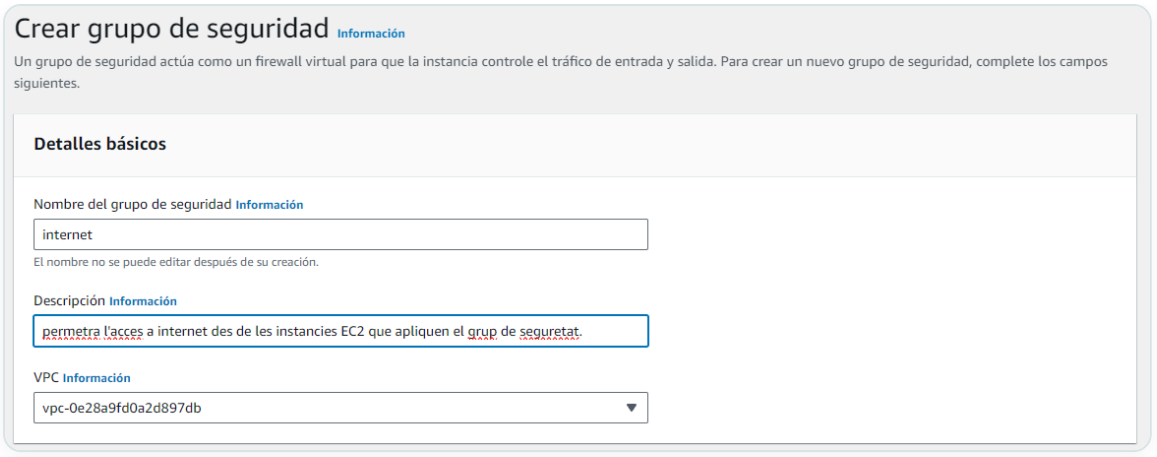
Accés a l'opció "Security Groups"

Dins de la pàgina de grups de seguretat, polsem el botó "Crear nou grup de seguretat".



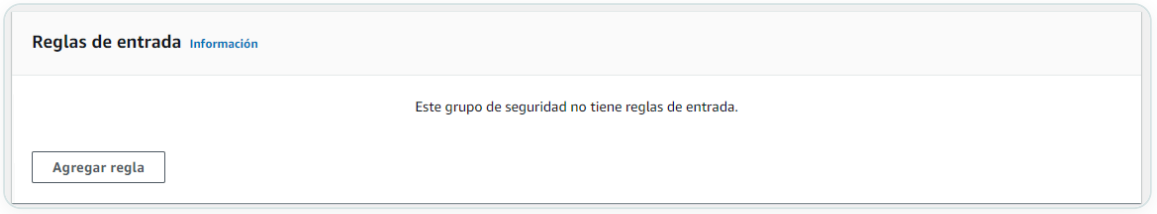
Creació d'un nou grup de seguretat.

Introduïm les dades bàsiques del grup de seguretat 'internet'.



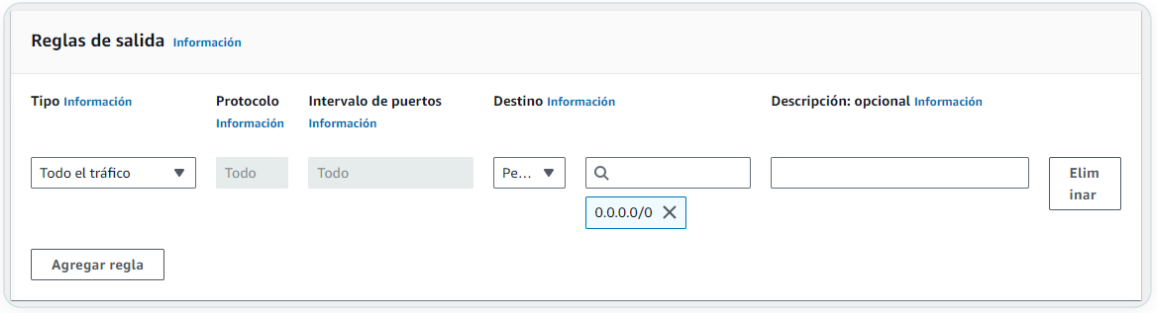
Dades bàsiques del grup de seguretat

Deixem les regles d'entrada buides.



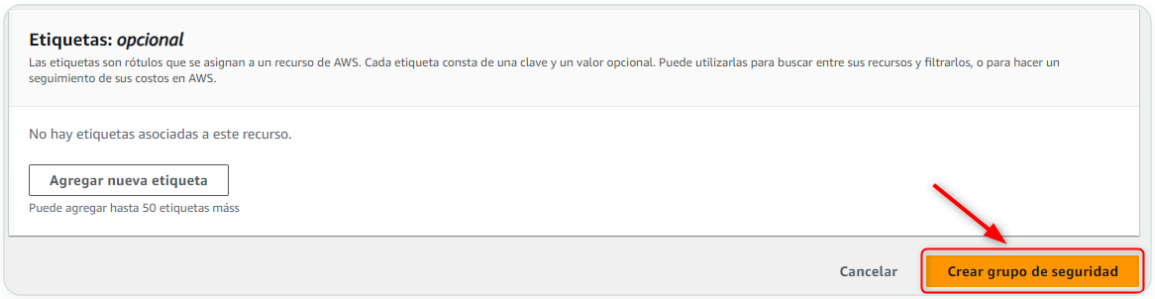
Sense regles d'entrada

Configurem la regla d'eixida, per a permetre la navegació a qualsevol IP/port.



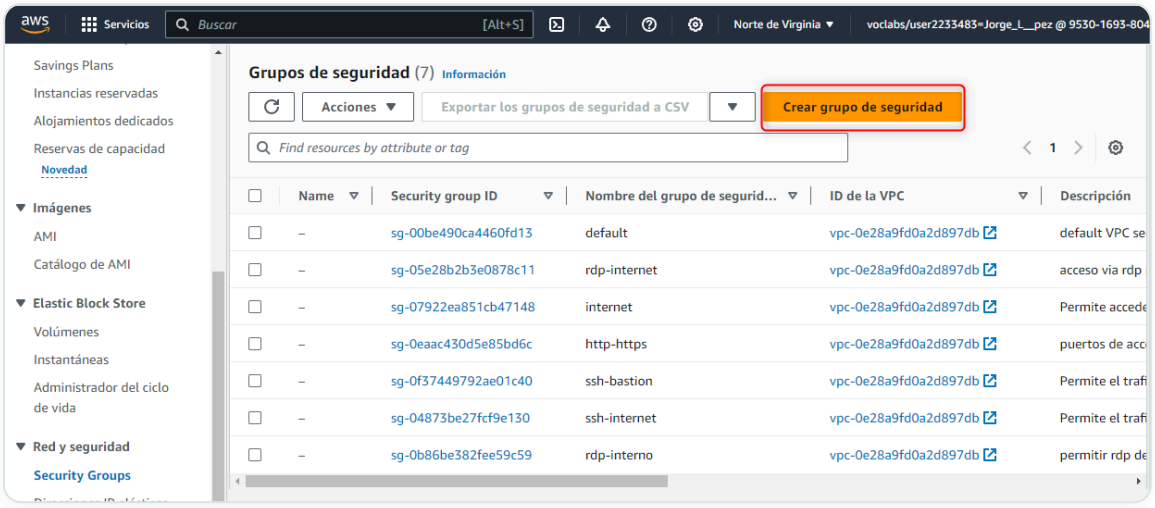
Regla d'eixida 0.0.0.0/0

I polsem sobre el botó 'Crear grup de seguretat'.



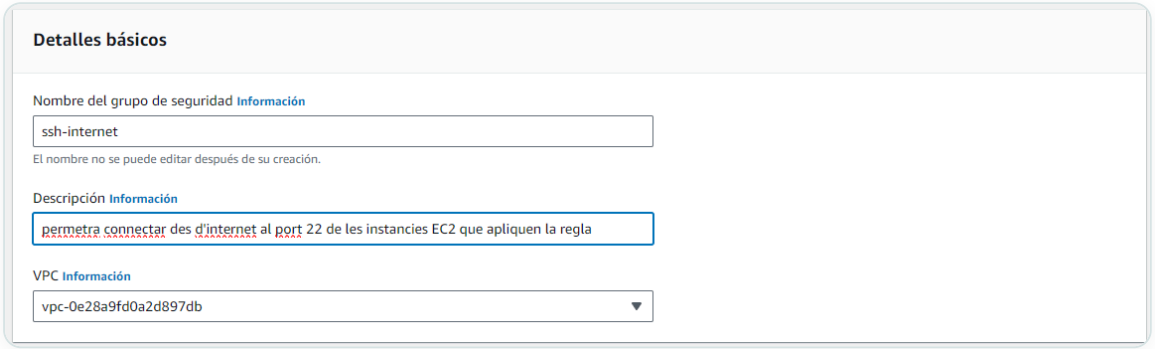
Confirmació de la creació del grup de seguretat.

Tornarem al llistat de grups de seguretat, i tornem a crear sobre el botó 'Crear grup de seguretat'.



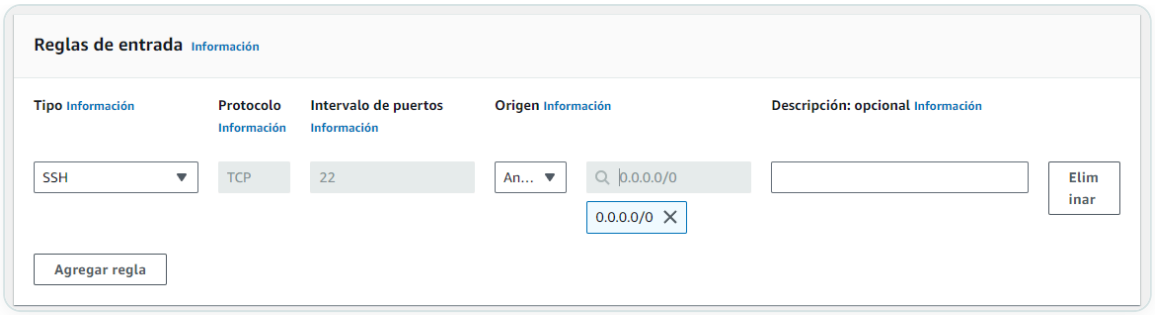
Creació d'un nou grup de seguretat.

Introduïm les dades bàsiques del grup de seguretat 'ssh-internet'.



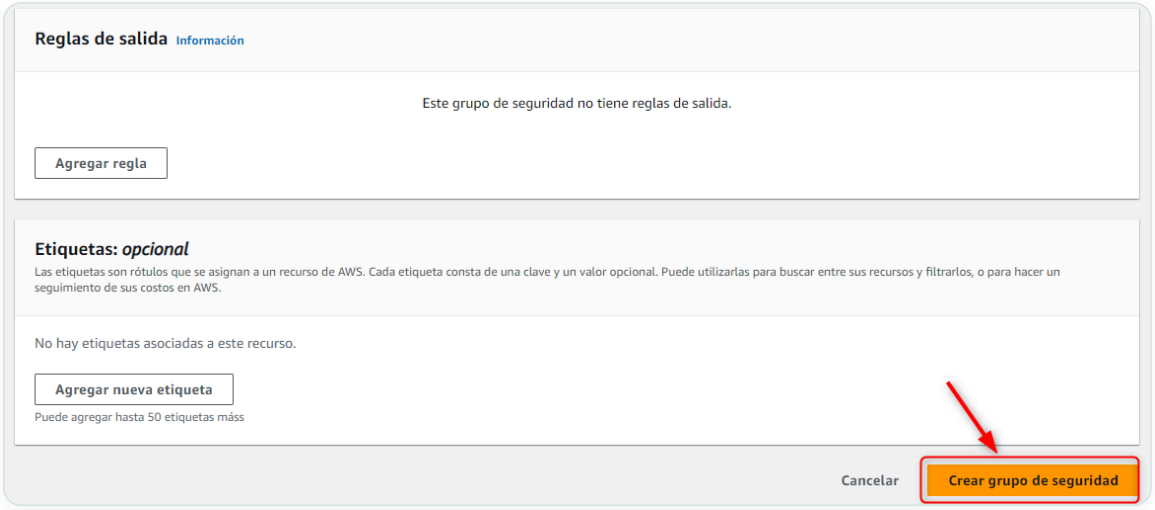
Dades bàsiques del grup de seguretat

Configurem la regla d'entrada, per a permetre l'accés al port 22 des de qualsevol IP.



Regla d'entrada SSH (TCP/22) des de 0.0.0.0/0

Deixem les regles d'eixida buides, i polsem sobre el botó 'Crear grup de seguretat'.

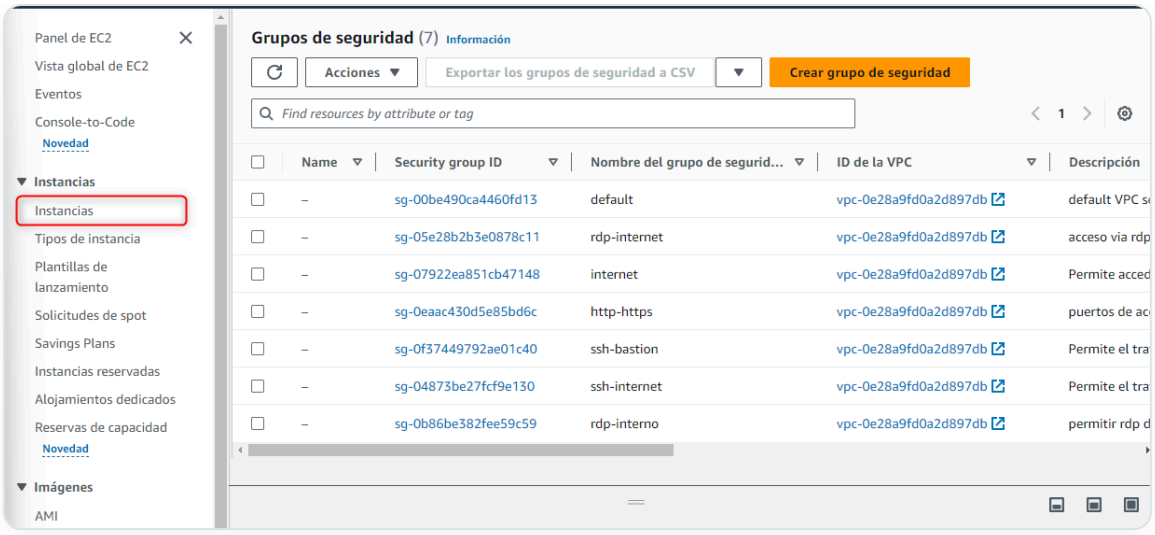


Confirmació de la creació del grup de seguretat.

Tornarem al llistat de grups de seguretat, on podrem comprovar que tenim les noves regles definides.

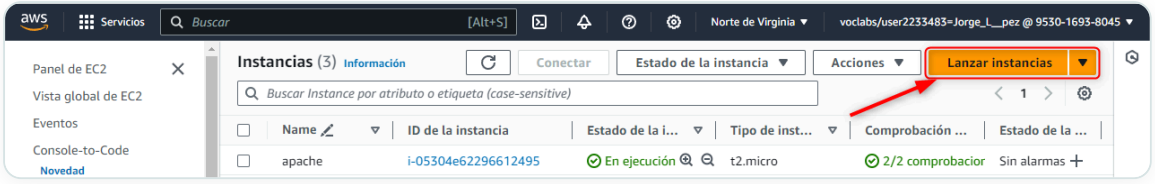
Creació del host bastió:

A continuació, polsem sobre l'opció 'instàncies' al menú lateral esquerre.



Llistat de grups de seguretat, i opció 'instàncies'

Accedirem a la pàgina d'instàncies EC2 desplegades al nostre compte d'AWS Academy, i podrem polsar sobre el botó 'Llançar instància', per configurar el nostre host bastió.



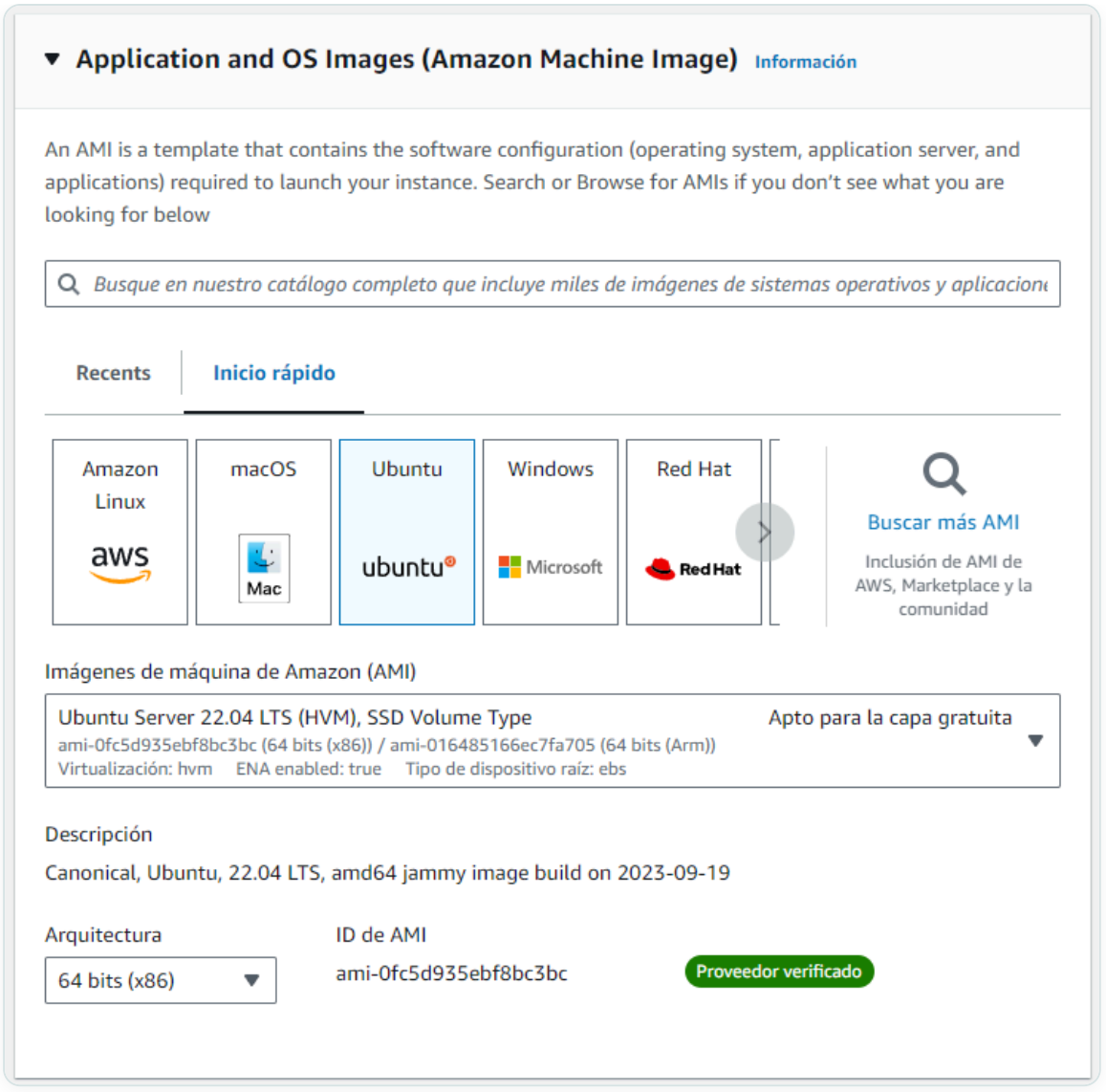
Opció 'llançar una nova instància'.

En el formulari de creació d'instàncies, configurem el nom de la instància.



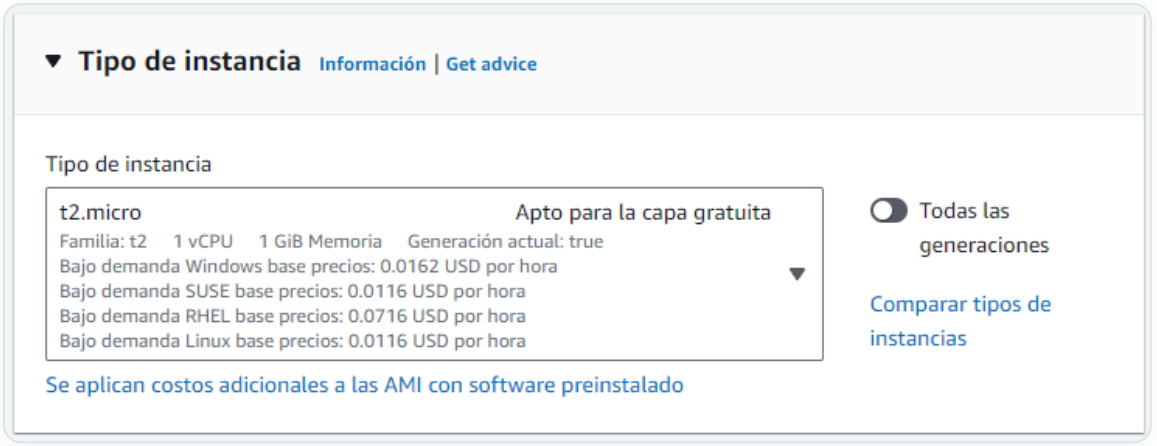
Configuració de la instància.

A continuació devem seleccionar l'AMI (Amazon Machine Image), amb la que s'inicialitzarà la instància EC2, configurada amb un sistema operatiu i programari base. En aquest cas, configurada amb Ubuntu 24.04 LTS, amb el servei OpenSSH.



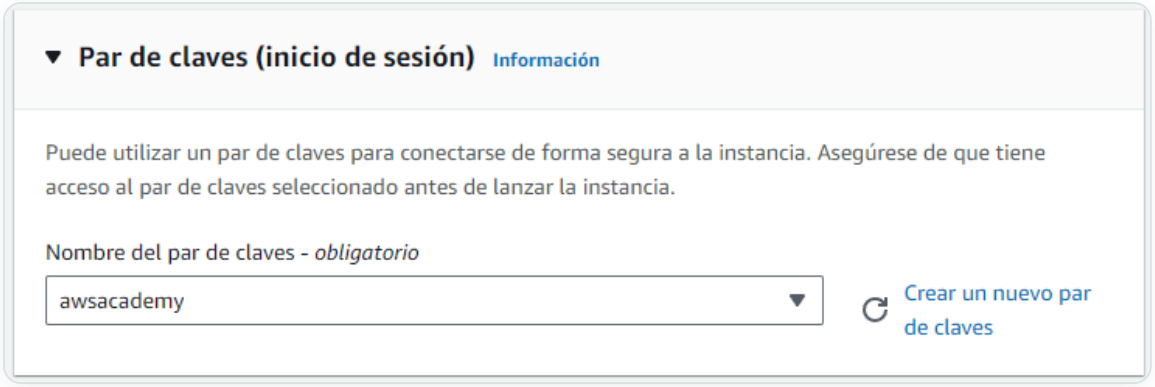
Selecció d'AMI

Seleccionem el tipus d'instància, que determinarà la capacitat de procés i memòria. Al nostre cas farem servir una instància t2.micro, amb 1 CPU virtual i 1 GB de memòria.



Selecció del tipus d'instància.

I seleccionarem el parell de claus amb el que connectarem a la instància.

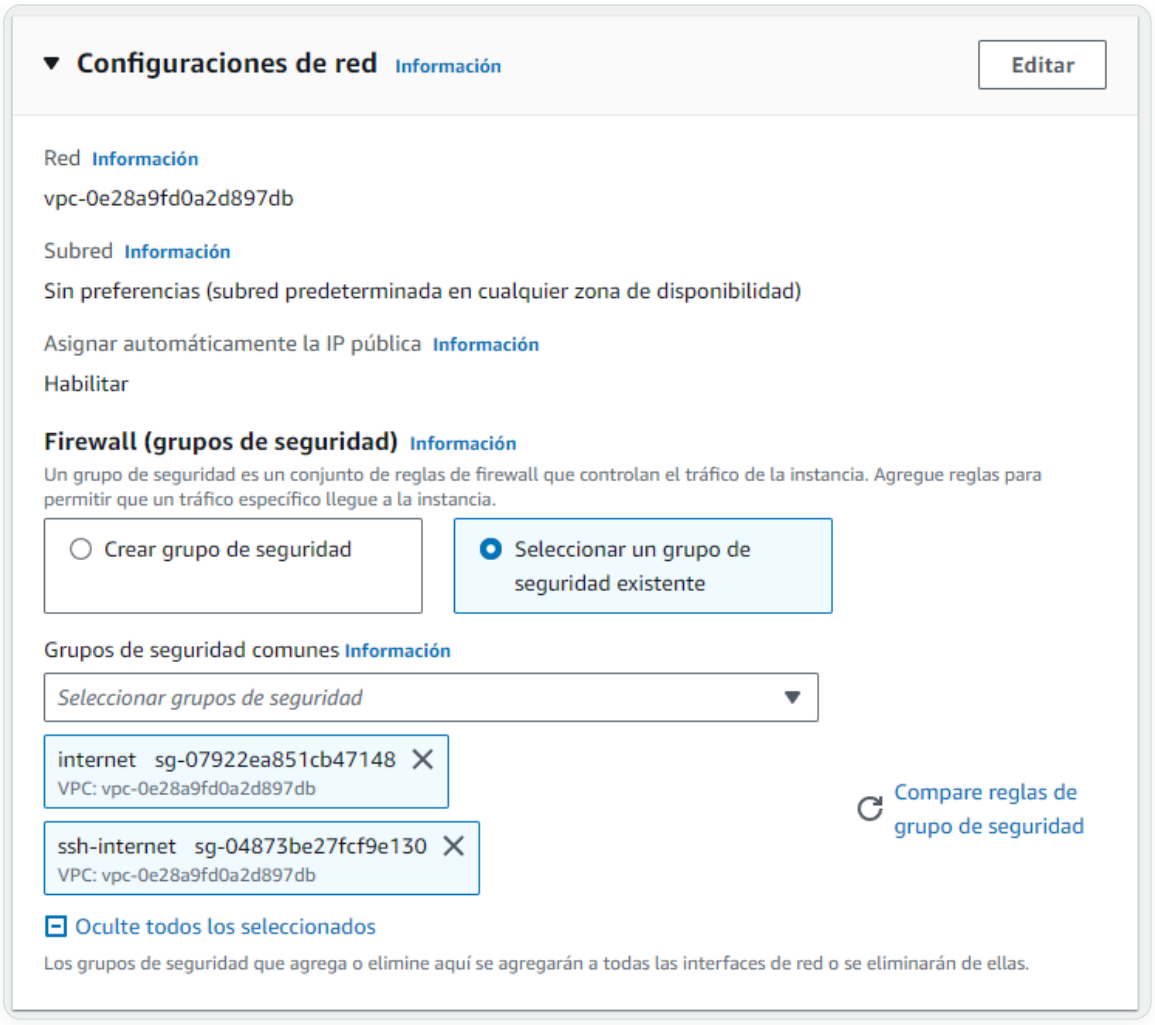


Selecció del parell de claus per autenticar l'administrador

> **Informació**
>
> Si encara no hem creat i descarregat un parell de claus, haurem de fer-ho abans de seleccionar-les.

> **Perill**
>
> Una volta generades les claus, i descarregades, haurem de tindre cura amb la custòdia d'aquestes, perquè seran necessàries per a connectar amb la instància configurada.

Seleccionem els grups de seguretat a aplicar a la nova instància, que hem creat anteriorment (internet i ssh-internet).

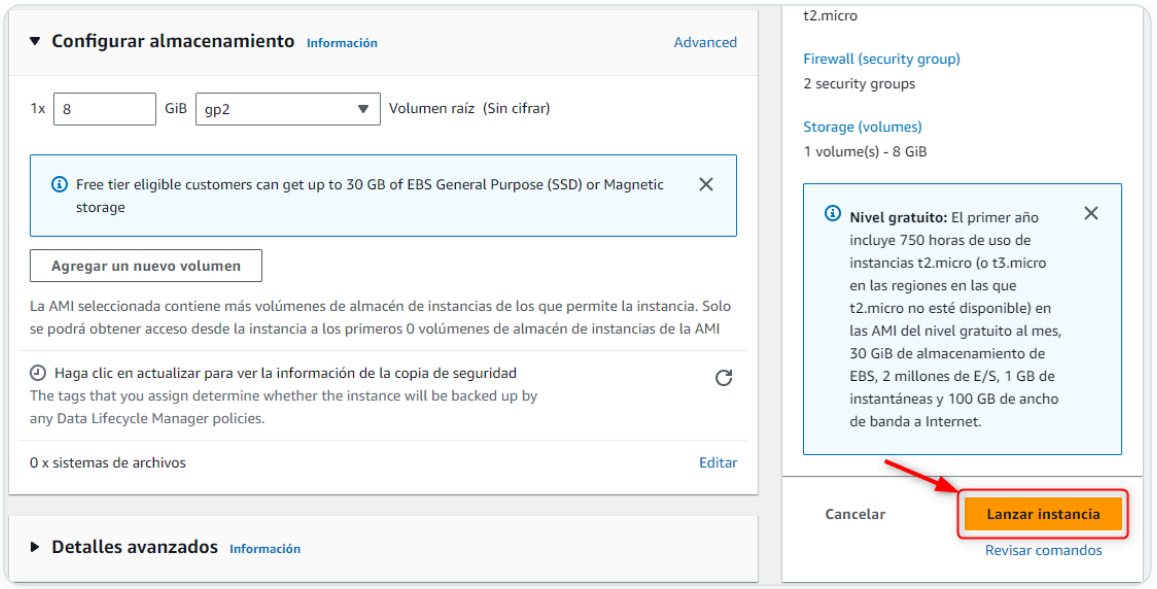


Selecció dels grups de seguretat

Informació

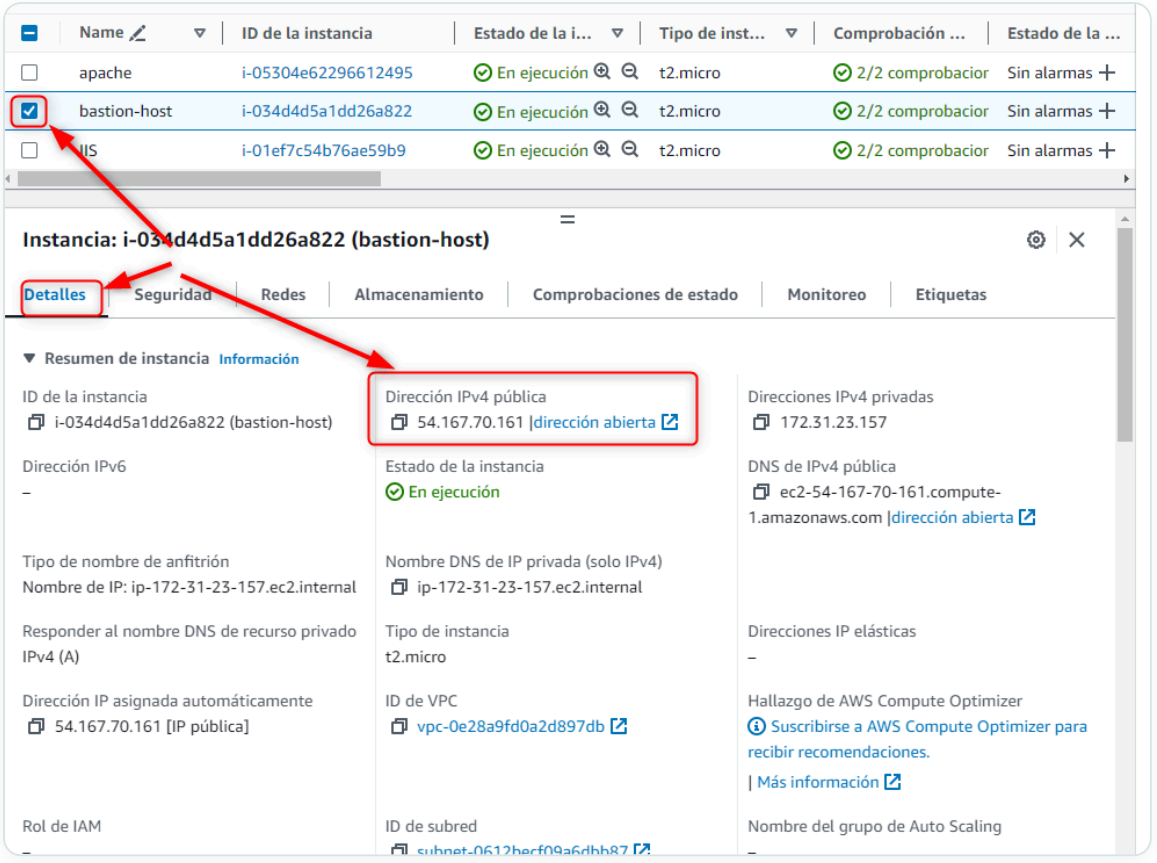
Recordem que els grups de seguretat actuen com a regles de filtrat de tràfic de xarxa, a la nostra infraestructura virtual.

I llancem la instància, polsant el botó corresponent.



Llançament de la instància

En llançar la instància, tornarem al llistat d'instàncies en execució del panell EC2, a on podrem seleccionar l'estat de la instància, i podrem seleccionar-la, per obtindre les dades de connexió.



Detall de la instància desplegada.

> **Atenció**
>
> Recordatori: per a connectar amb clau privada a les instancies Ubuntu Server a AWS, hem de fer servir l'usuari ubuntu, com al següent exemple:
>
> ssh -i /path/to/private-key ubuntu@ip-publica

> **Perill**
>
> Per a poder connectar, la clau privada ha de tindre aplicat permisos de soles lectura, i soles per a l'usuari:
>
> chmod 400 /path/to/private-key

Format de l'entrega

- L'activitat es corregirà presencialment a classe, mostrant la configuració aplicada als grups de seguretat i al host bastió.