

Examen 1a avaluació – Introducció al núvol

Instruccions:

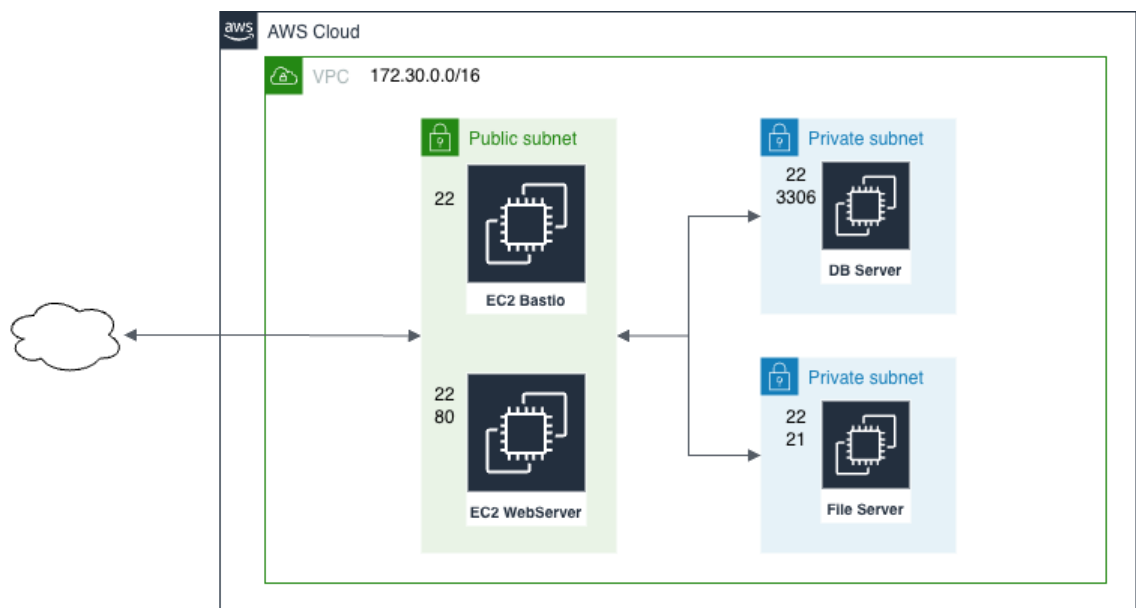
- Una vegada finalitzada, entrega l'activitat a la tasca d'Aules.
- L'entrega serà en pdf.
- Recorda que els enunciats han de formar part de l'entrega.
- Afig les captures a la secció adequada (revisar final de document)
- En aquest examen s'avaluen els RA1, RA2 i RA3, tots ells parcialment

1. Eres l'administrador d'una empresa que vol publicar una aplicació web senzilla a AWS. L'aplicació està formada per:

- Un bastió públic (punt d'entrada SSH)
- Una capa web (servidor públic)
- Una capa de base de dades (en xarxa privada).
- Una capa d'emmagatzematge intern (servidor de fitxers també privada).

Cada element s'ha de desplegar en una arquitectura pròpia i segura dins del núvol seguint la següent infraestructura:

NOTA: el dibuix està fet pel becari, segurament necessita serveis addicionals que no s'han tingut en compte a l'esquema



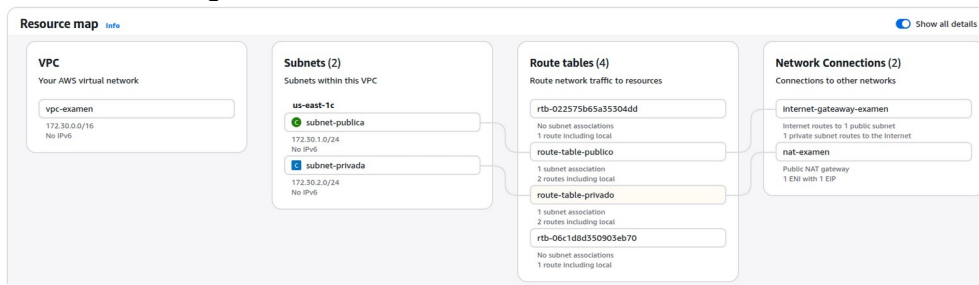
A més ens ha donat les següents indicacions:

- Totes les EC2 gastaran la AMI de Amazon Linux.
- Seguretat:
 - Sols el bastió serà accessible per SSH des de fora de la VPC.
 - La resta d'EC2 seran accessibles per SSH solament des del bastió.
 - Sols el Webserver serà accessible des de fora de la VPC pel port 80.
 - L'accés a la BD (3306) i al servidor de fitxers (21) seran accessibles solament des del servidor web.
 - Sols estaran oberts els ports estrictament necessaris.
 - És molt important la seguretat i és possible que en un futur s'afegisquen més EC2 a les subxarxes. Assegura't que encara que no es configuren SG, el tràfic siga restringit correctament.
- Les instàncies privades han de poder descarregar realitzar actualitzacions a través del núvol.
- La web estarà sempre disponible a la mateixa IP.
- Per a instal·lar el servidor web (BD i fitxers no cal instal·lar res):

```
sudo dnf update -y
sudo dnf install nginx -y
sudo systemctl start nginx
sudo systemctl enable nginx
sudo systemctl status nginx
```

Per avaluar, calen les següents captures (afig-les al seu apartat):

1. Creació de la xarxa (0,75 pt)
 - a. Vista general de la VPC



- b. Totes les subxarxes on es vega la IP associada

<input type="checkbox"/>	Name	Subnet ID	State	VPC	Bloc...	IPv4 CIDR	IPv6 ...	IPv6 ...	Available I...	Availability Zone
<input type="checkbox"/>	subnet-publica	subnet-067c2f5d76d9334e1	Available	vpc-06dfb6b40ad27469 vpc-examen	Off	172.30.1.0/24	-	-	249	us-east-1a (us-east-1c)
<input type="checkbox"/>	subnet-privada	subnet-03f29413bd3aee6c2	Available	vpc-06dfb6b40ad27469 vpc-examen	Off	172.30.2.0/24	-	-	249	us-east-1a (us-east-1c)

2. Configuració de gateways i encaminament (1,5 pt)
 - a. Taules de ruta creades i de les associacions amb subxarxes que tenen

Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	nat-12dbdb34547882ce2	Active	No	Create Route
172.30.0.0/16	local	Active	No	Create Route Table



CIF: Q9655627I – C/ Literat Azorín, 1, 46702 Gandia. Tel. 962829430 – 46004221@edu.gva.es

route-table-publico	rtb-0c0f7706975493d0c	subnet-067c2fd476d5934e1 / subnet-publica	-	No	vpc-06df6b640a0d27469 / vpc-...	471112527025
---------------------	-----------------------	---	---	----	---------------------------------	--------------

rtb-0c0f7706975493d0c / route-table-publico

Details Routes Subnet associations Edge associations Route propagation Tags

Routes (2)

Filter routes

Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	igw-06049c93f61821ea5	Active	No	Create Route
172.30.0.0/16	local	Active	No	Create Route Table

b. Components que ens permeten l'accés extern o l'eixida a internet

Internet gateways (1/2) Info

Find Internet gateways by attribute or tag

Name	Internet gateway ID	State	VPC ID	Owner
internet-gateway-examen	igw-06049c93f61821ea5	Attached	vpc-06df6b640a0d27469 / vpc-examen	471112527025
-	igw-0b692ade8992d1800	Attached	vpc-0a0d7dc6bd7c6a05	471112527025

igw-06049c93f61821ea5 / internet-gateway-examen

Details Tags

Details

Internet gateway ID
igw-06049c93f61821ea5

State
Attached

VPC ID
vpc-06df6b640a0d27469 / vpc-examen

Owner
471112527025

NAT gateways (1/1) Info

Find NAT gateways by attribute or tag

NAT gateway ID: nat-12dbdb54547882ce2

Clear filters

Name	NAT gateway ID	Connectivity...	State	State message	Availability ...	Route table ID	Primary public L...	Primary private L...	Prim
nat-examen	nat-12dbdb54547882ce2	Public	Available	-	Regional	rtb-022375b65...	18.235.105.201	-	Prim

nat-12dbdb54547882ce2 / nat-examen

Details IP addresses Monitoring Flow logs Tags

Details

NAT gateway ID
nat-12dbdb54547882ce2

NAT gateway ARN
arn:aws:ec2:us-east-1:471112527025:natgateway/nat-12dbdb54547882ce2

VPC
vpc-06df6b640a0d27469 / vpc-examen

Availability mode
Regional

Connectivity type
Public

Method of EIP allocation
Automatic

State
Available

Created
Tuesday, November 25, 2025 at 15:48:37 GMT+1

State message
-

Deleted
-

3. Assignació i configuració de les instàncies (1 pt)

a. Llistat d'instàncies on es vega la subxarxa en la que es troben així com les seues IP's (ambdós)

Instances (4) Info

Find Instance by attribute or tag (case-sensitive)

All states

Name	Private IP address	Instance ID	Subnet IDs	Instance state	Public IPv4 ...	Security group name
ec2-bastion	172.30.1.232	i-035fd32b2d09e3dd	subnet-067c2fd476d5934e1	Running	44.198.53.183	sec-grp-bastion
ec2-ddbb	172.30.2.136	i-04437159fd9a004b	subnet-05f29413bd3aee6c2	Running	-	sec-grp-ddbb
ec2-filer...	172.30.2.68	i-0ff547ecd9659cfa	subnet-05f29413bd3aee6c2	Running	-	sec-grp-filerserver
ec2-webserver	172.30.1.88	i-071bc5581653e5080	subnet-067c2fd476d5934e1	Running	3.221.163.72	sec-grp-webserver

4.

Accés

Name	Subnet ID
subnet-publica	subnet-067c2fd476d5934e1
subnet-privada	subnet-05f29413bd3aee6c2

segur (0,75 pt)

a. Connexió SSH des del teu PC al bastió

CIF: Q9655627I – C/ Literat Azorín, 1, 46702 Gandia. Tel. 962829430 – 46004221@edu.gva.es


```
ec2-user@ip-172-30-1-232:~ — Konsole
> ssh -A ec2-user@44.198.53.183
** WARNING: connection is not using a post-quantum key exchange algorithm
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html

      #_
    ~\_ #####_          Amazon Linux 2023
   ~~ \#####\
  ~~~ \###|
     ~ \#/ ---         https://aws.amazon.com/linux/amazon-linux-2023
    ~ ~V~' '->
        ~~~
           ~~-.- /-/-
              _/_/' /-/
                 _/m/'

Last login: Tue Nov 25 14:52:30 2025 from 213.0.87.4
[ec2-user@ip-172-30-1-232 ~]$
```

b. Connexió SSH des del bastió a un EC2 de la subxarxa privada.

```
[ec2-user@ip-172-30-1-232 ~]$ ssh -A 172.30.2.136
The authenticity of host '172.30.2.136 (172.30.2.136)' can't be established.
ED25519 key fingerprint is SHA256:FJD7H8AEdxlpwBHmu/3MGJ/yX9ZPVmwbjTalgL+9XbI.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.30.2.136' (ED25519) to the list of known hosts.
```



```
      #_
     _\#####_   Amazon Linux 2023
    NN \#####\
    NN  \###|
    NN   \#/___#
    NN    V^!'__>
        NNN
         NN_._.
          _/_/_/_/
           _/m/'
```

```
[ec2-user@ip-172-30-2-136 ~]$
```

5. Seguretat a nivell d'instància (1,25 pt)

- a. Regles de seguretat de cada una de les instàncies. Assegura't que queda clar que la regla de seguretat correspon a la instància que intentes demostrar



<input checked="" type="checkbox"/>	ec2-bastion	172.30.1.232	i-035fdf32b2d09e3dd	subnet-067c2fd476d5934e1	<input checked="" type="checkbox"/> R
<input type="checkbox"/>	ec2-ddbb	172.30.2.136	i-04437159f0d9a004b	subnet-05f29413bd3aee6c2	<input checked="" type="checkbox"/> R
<input type="checkbox"/>	ec2-fileserver	172.30.2.68	i-0ffd547ecd9659cfa	subnet-05f29413bd3aee6c2	<input checked="" type="checkbox"/> R
<input type="checkbox"/>	ec2-webserver	172.30.1.88	i-071bc5581653e5080	subnet-067c2fd476d5934e1	<input checked="" type="checkbox"/> R

i-035fdf32b2d09e3dd (ec2-bastion)

Details | Status and alarms | Monitoring | **Security** | Networking | Storage | Tags

► Security details

▼ Inbound rules

Filter rules

< 1 >

Name	Security gr...	Port range	Protocol	Source	Security gr...	Description
-	sgr-037c9f...	22	TCP	0.0.0.0/0	sec-grp-ba...	-

▼ Outbound rules

Filter rules

< 1 >

Name	Security gr...	Port range	Protocol	Destination	Security gr...	Description
-	sgr-01bd9...	All	All	0.0.0.0/0	sec-grp-ba...	-

<input checked="" type="checkbox"/>	ec2-ddbb	172.30.2.136	i-04437159f0d9a004b	subnet-05f29413bd3aee6c2	<input checked="" type="checkbox"/> R
<input type="checkbox"/>	ec2-fileserver	172.30.2.68	i-0ffd547ecd9659cfa	subnet-05f29413bd3aee6c2	<input checked="" type="checkbox"/> R
<input type="checkbox"/>	ec2-webserver	172.30.1.88	i-071bc5581653e5080	subnet-067c2fd476d5934e1	<input checked="" type="checkbox"/> R

i-04437159f0d9a004b (ec2-ddbb)

Details | Status and alarms | Monitoring | **Security** | Networking | Storage | Tags

► Security details

▼ Inbound rules

Filter rules

< 1 >

Name	Security gr...	Port range	Protocol	Source	Security gr...	Description
-	sgr-0310a6...	22	TCP	172.30.1.232/32	sec-grp-dd...	bastion
-	sgr-0410f1...	3306	TCP	172.30.1.88/32	sec-grp-dd...	webserve

▼ Outbound rules

Filter rules

< 1 >

Name	Security gr...	Port range	Protocol	Destination	Security gr...	Description
-	sgr-064fa7...	All	All	0.0.0.0/0	sec-grp-dd...	-



CIF: Q9655627I – C/ Literat Azorín, 1, 46702 Gandia. Tel. 962829430 – 46004221@edu.gva.es

<input checked="" type="checkbox"/>	ec2-fileserver	172.30.2.68	I-Offd547ecd9659cfa	subnet-05f29413bd3aee6c2	
<input type="checkbox"/>	ec2-webserver	172.30.1.88	I-071bc5581653e5080	subnet-067c2fd476d5934e1	

i-Offd547ecd9659cfa (ec2-fileserver)

Details | Status and alarms | Monitoring | **Security** | Networking | Storage | Tags

► Security details

▼ Inbound rules

Filter rules

< 1 >

Name	Security gr...	Port range	Protocol	Source	Security gr...	Descripti...
-	sgr-01b61...	21 - 22	TCP	172.30.1.88/32	sec-grp-file...	FTP para
-	sgr-01543e...	22	TCP	172.30.1.232/32	sec-grp-file...	bastion

▼ Outbound rules

Q

Filter rules

< 1 >

Name	Security gr...	Port range	Protocol	Destination	Security gr...	Description
-	sgr-03d1c7...	All	All	0.0.0.0/0	sec-grp-file...	-

<input checked="" type="checkbox"/>	ec2-webserver	172.30.1.88	I-071bc5581653e5080	subnet-067c2fd476d5934e1	
-------------------------------------	---------------	-------------	---------------------	--------------------------	--

i-071bc5581653e5080 (ec2-webserver)

Details | Status and alarms | Monitoring | **Security** | Networking | Storage | Tags

► Security details

▼ Inbound rules

Filter rules

< 1 >

Name	Security gr...	Port range	Protocol	Source	Security gr...	Descripti
-	sgr-097ee0...	22	TCP	172.30.1.232/32	sec-grp-we...	Ssh pal bi
-	sgr-0b1e11...	80	TCP	0.0.0.0/0	sec-grp-we...	-

▼ Outbound rules

Filter rules

< 1 >

Name	Security gr...	Port range	Protocol	Destination	Security gr...	Description
-	sgr-06343f...	All	All	0.0.0.0/0	sec-grp-we...	-

6. Seguretat a nivell de subxarxa (1 pt)
 - a. Vista general o resum de les regles de filtratge a nivell de subxarxa.
7. Funcionament general (1,25 pts)
 - a. IP fixa assignada a la ec2 del servidor



54.225.128.100



View IP address usage and recommendations to release unused IPs with [Public IP Insights](#)



Summary

Tags

Summary

Allocated IPv4 address

54.225.128.100

Type

Public IP

Allocation ID

elpalloc-0915e8a0102f25a43

Reverse DNS record

–

Association ID

elpassoc-05eacfb8864610859

Scope

VPC

Associated instance ID

i-071bc5581653e5080

Private IP address

172.30.1.88

Network interface ID

eni-08d1d9abdfa858181

Network interface owner account ID

471112527025

Public DNS

–

NAT Gateway ID

–

Address pool

Amazon

Network border group

us-east-1

Service managed

–

b. Accès des del navegador a la web

No es seguro http://54.225.128.100

Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to [nginx.org](#).
Commercial support is available at [nginx.com](#).

Thank you for using nginx.

c. Accès a internet des de instàncies privades (pots fer un update)

```
[ec2-user@ip-172-30-2-68 ~]$ sudo dnf update
Amazon Linux 2023 repository                69 MB/s | 49 MB    00:00
Amazon Linux 2023 Kernel Livepatch repository 278 kB/s | 29 kB   00:00
Dependencies resolved.
Nothing to do.
Complete!
[ec2-user@ip-172-30-2-68 ~]$
```

nat-1ef0df281a73022ee / nat-2-examen

Actions

Details

NAT gateway ID

nat-1ef0df281a73022ee

Availability mode

Regional

State

Available

State message

–

NAT gateway ARN

arn:aws:ec2:us-east-1:471112527025:natgateway/nat-1ef0df281a73022ee

Connectivity type

Public

Created

Tuesday, November 25, 2025 at 16:34:11 GMT+1

Deleted

–

VPC

vpc-06dfb6b40a0d27469 / vpc-examen

Method of EIP allocation

Automatic