



IT Department Technical Handbook

PREPARED BY:

GROUP 1

Table of Contents

- 1 Configurar y crear la Instancia
- 2 Preparación del servidor e instalación de servicios
- 3 Configuración de los diferentes servicios

1. Configurar y crear la Instancia:

Security Groups:

entrada

Reglas de entrada

ID de la regla del grupo de seguridad

Tipo

Protocolo

Intervalo de puertos

Origen

Descripción: opcional

-	SMB	TCP	445	Anywh...	Samba	Eliminar
-	TCP personalizado	TCP	9200	Anywh...	Elasticsearch REST API	Eliminar
-	TCP personalizado	TCP	5601	Anywh...	Kibana UI	Eliminar
-	SSH	TCP	22	Anywh...	Conexion remota SSH	Eliminar
-	RDP	TCP	3389	Anywh...	Conexion remota RDP	Eliminar

Agregar regla

salida:

Reglas de salida

ID de la regla del grupo de seguridad

Tipo

Protocolo

Intervalo de puertos

Destino

Descripción: opcional

sgr-0893f4c770b995345	Todo el tráfico	Todo	Todo	Person...	Actualizaciones, DNS, etc.	Eliminar
-----------------------	-----------------	------	------	-----------	----------------------------	----------

Agregar regla

Configuración de la instancia:

Ubuntu server:

Nombre y etiquetas Información

Nombre

[Agregar etiquetas adicionales](#)

▼ Imágenes de aplicaciones y sistemas operativos (Imagen de máquina de Amazon) Información

Una AMI es una plantilla que contiene la configuración de software (sistema operativo, servidor de aplicaciones y aplicaciones) necesaria para lanzar la instancia. Busque o examine las AMI si no ve lo que busca a continuación.

[AMI del catálogo](#) | [Recientes](#) | [Inicio rápido](#)

Nombre
 Ubuntu Server 24.04 LTS (HVM), SSD Volume Type

Descripción
 Ubuntu Server 24.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

ID de imagen
 ami-084568db4383264d4

Nombre de usuario ⓘ
 ubuntu

Catálogo	Publicado	Arquitectura	Virtualización	Tipo de dispositivo raíz	Habilitado para ENA
AMI de inicio rápido	2025-03-05T09:18:37.000Z	x86_64	hvm	ebs	Sí

Modo de arranque
 uefi-preferred

Proveedor verificado

Apto para la capa gratuita

Buscar más AMI

Inclusión de AMI de AWS, Marketplace y la comunidad

t2.large

▼ Tipo de instancia Información | [Obtener asesoramiento](#)

Tipo de instancia

t3.large

Familia: t3 2 vCPU 8 GiB Memoria Generación actual: true Bajo demanda Linux base precios: 0.0832 USD por hora
 Bajo demanda Windows base precios: 0.1108 USD por hora Bajo demanda RHEL base precios: 0.112 USD por hora
 Bajo demanda SUSE base precios: 0.1395 USD por hora Bajo demanda Ubuntu Pro base precios: 0.0867 USD por hora

☐ Todas las generaciones
[Comparar tipos de instancias](#)

[Se aplican costos adicionales a las AMI con software preinstalado](#)

Certificado de seguridad

Ponemos el grupo de seguridad antes creado y ponemos IP publica automática.

▼ Configuraciones de red

Información

VPC: obligatorio

Información

vpc-002b375fb26c7f2db

(predeterminado)

↻

Subred

Información

Sin preferencias

↻

Crear nueva subred

Asignar automáticamente la IP pública

Información

Habilitar

↻

Se aplican cargos adicionales cuando no se cumplen los límites del nivel gratuito

Firewall (grupos de seguridad)

Información

Un grupo de seguridad es un conjunto de reglas de firewall que controlan el tráfico de la instancia. Agregue reglas para permitir que un tráfico específico llegue a la instancia.

☐ Crear grupo de seguridad

☒ Seleccionar un grupo de seguridad existente

Grupos de seguridad comunes

Información

Seleccionar grupos de seguridad

↻

SMB&Monitoring sg-0e67de559146eb20c

VPC: vpc-002b375fb26c7f2db

✕

↻

Compare reglas de grupo de seguridad

Los grupos de seguridad que agrega o elimine aquí se agregarán a todas las interfaces de red o se eliminarán de ellas.

Configuramos el almacenamiento

▼ Configurar almacenamiento

Información

Avanzado

1x

8

GiB

gp3

↻

Volumen raíz, 3000 IOPS, No cifrado

Los clientes que cumplan los requisitos de la capa gratuita pueden obtener hasta 30 GB de almacenamiento magnético o de uso general (SSD) de EBS

✕

Agregar un nuevo volumen

The selected AMI contains instance store volumes, however the instance does not allow any instance store volumes. None of the instance store volumes from the AMI will be accessible from the instance

Haga clic en actualizar para ver la información de la copia de seguridad

↻

Las etiquetas que asigne determinan si alguna política de Data Lifecycle Manager realizará una copia de seguridad de la instancia.

0 x sistemas de archivos

Editar

Y lanzamos la instancia:

▼ Resumen

Número de instancias

Información

1

Imagen de software (AMI)

Ubuntu Server 24.04 LTS (HVM),...más información

ami-084568db4383264d4

Tipo de servidor virtual (tipo de instancia)

t2.micro

Firewall (grupo de seguridad)

SMB&Monitoring

Almacenamiento (volúmenes)

Volúmenes: 1 (8 GiB)


?

Nivel gratuito: Durante el primer año que abre una cuenta de AWS, obtiene 750 horas al mes de uso de instancias t2.micro (o t3.micro cuando t2.micro no esté disponible) si se utiliza con AMI de nivel gratuito, 750 horas al mes de uso de direcciones IPv4 públicas, 30 GiB de almacenamiento de EBS, 2 millones de E/S, 1 GB de instantáneas y 100 GB de ancho de banda para Internet.

×

Cancelar

Lanzar instancia

 Código de versión preliminar

Conexión con otras instancias (Vía IP Pública):

Primero creamos una asignación de IP elástica:

Asignar dirección IP elástica [Información](#)

Configuraciones de la dirección IP elástica [Información](#)

Grupo de direcciones IPv4 públicas

- ☒ El grupo de direcciones IPv4 de Amazon
 - ☐ Dirección IPv4 pública que trae a su cuenta de AWS con BYOIP. (opción deshabilitada porque no se encontraron grupos) [Más información](#)
 - ☐ Grupo de direcciones IPv4 propiedad del cliente creado desde su red local para su uso con un Outpost. (opción deshabilitada porque no se encontró ningún grupo propiedad del cliente) [Más información](#)
 - ☐ Asignar mediante un grupo de IPAM de IPv4 (opción deshabilitada porque no se encontró ningún grupo público de IPAM de IPv4 con un servicio de AWS como EC2)

Grupo fronterizo de red [Información](#)

Direcciones IP estáticas globales
 AWS Global Accelerator puede proporcionar direcciones IP estáticas globales que se anuncian en todo el mundo mediante anycast desde ubicaciones periféricas de AWS. Esto puede ayudar a mejorar la disponibilidad y la latencia del tráfico de usuarios mediante el uso de la red global de Amazon. [Más información](#)
[Crear un acelerador](#)

Etiquetas - opcional
 Una etiqueta es una marca que se asigna a un recurso de AWS. Cada etiqueta se compone de una clave y un valor opcional. Puede usar etiquetas para buscar y filtrar sus recursos o realizar un seguimiento de los costos de AWS. No hay etiquetas asociadas al recurso.
[Agregar una etiqueta nueva](#)
 Puede agregar hasta 50 etiquetas más

[Cancelar](#) [Asignar](#)

Una vez creada, la seleccionamos y le damos a “Dirección IP elástica asociada”

Acciones

Asignar dirección IP

Ver detalles

- Publicar direcciones IP elásticas
- Dirección IP elástica asociada**
- Desasociar dirección IP elástica
- Actualizar DNS inverso
- Habilitar transferencias
- Deshabilitar transferencias
- Aceptar transferencias

Y seleccionamos una Instancia y su IP privada para enlazarla a su IP pública

Dirección IP elástica asociada [Información](#)

Elija la instancia o la interfaz de red para asociarla a esta dirección IP elástica (3.226.157.142)

Dirección IP elástica: 3.226.157.142

Tipo de recurso
 Elija el tipo de recurso al que desea asociar la dirección IP elástica.

- ☒ Instancia
- ☐ Interfaz de red

⚠ Si asocia una dirección IP elástica a una instancia que ya tiene una dirección IP elástica asociada, la dirección IP elástica asociada anteriormente se desasociará, pero la dirección seguirá asignándose a su cuenta. [Más información](#)

Si no se especifica ninguna dirección IP privada, la dirección IP elástica se asociará a la dirección IP privada principal.

Instancia

Dirección IP privada
 La dirección IP privada a la que se asociará la dirección IP elástica.

Reasociación
 Especifica si la dirección IP elástica se puede volver a asociar a un recurso diferente si ya está asociada a un recurso.
 ☐ Permitir que se vuelva a asociar esta dirección IP elástica

[Cancelar](#) [Asociado](#)

Con esto logramos que su IP pública no cambie nunca y podamos acceder siempre desde esta misma IP sin necesidad de copiar la IP cada vez que cambia.

2. Preparación del servidor e instalación de servicios:

Preparación:

primero hacemos un “sudo apt update && sudo apt upgrade -y” para asegurar que todo está actualizado y listo para instalar y usar (esto puede tardar un poco)

```
ubuntu@ip-172-31-93-89:~$ sudo apt update && sudo apt upgrade -y
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu jammy-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
ubuntu@ip-172-31-93-89:~$
```

Creamos un usuario administrador para gestionar mejor nuestro servidor y cambiamos el hostname para organizar el servidor (en este caso pondremos “grup1SMB”)

```
ubuntu@ip-172-31-93-89:~$ sudo useradd -m -s /bin/bash smbmonitoreo
ubuntu@ip-172-31-93-89:~$ sudo usermod -aG sudo smbmonitoreo
ubuntu@ip-172-31-93-89:~$ sudo nano /etc/hostname
ubuntu@ip-172-31-93-89:~$
```

En nuestro caso, el usuario será “smb monitoreo” y su contraseña será “@ITB2024”

También le cambiamos la contraseña para poder acceder

```
ubuntu@grup1SMB:~$ sudo passwd smbmonitoreo
New password:
Retype new password:
passwd: password updated successfully
ubuntu@grup1SMB:~$ su smbmonitoreo
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

smbmonitoreo@grup1SMB:/home/ubuntu$ cd
smbmonitoreo@grup1SMB:~$
```


NFS:

Para el servicio de compartición de carpetas y datos entre servidores, usaremos NFS, un servicio de Linux bastante fácil de configurar y eficiente.

Para descargar el servicio usaremos la comando “**sudo apt install nfs-kernel-server -y**” en nuestros servidores y “**sudo apt install nfs-common -y**” en los clientes

```
smbmonitoreo@grup1SMB:/elastic$ sudo apt install nfs-kernel-server -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nfs-kernel-server is already the newest version (1:2.6.1-1ubuntu1.2).
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
smbmonitoreo@grup1SMB:/elastic$
```

```
Processing triggers for libc-bin (2.39-0ubuntu8.4) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@DNSserverip-172-31-92-232:~$ sudo apt install nfs-common -y
```

Monitoreo:

para el servicio de monitoreo, usaremos las herramientas de elasticsearch y kibana para el servidor nfs, y winlogbeat y auditbeat para el resto de servidores, unos servicios que si se ejecutan a la vez, nos proporcionan logs de lo que está pasando en las máquinas que se configuren.

Elasticsearch & Kibana:

Primero de todo, creamos el usuario “elastic” para poder gestionar los ficheros (contraseña = @ITB2024)

```
smbmonitoreo@grup1SMB:~$ sudo adduser elastic
Adding user `elastic' ...
Adding new group `elastic' (1002) ...
Adding new user `elastic' (1002) with group `elastic' ...
Creating home directory `/home/elastic' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for elastic
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
smbmonitoreo@grup1SMB:~$ sudo usermod -aG sudo elastic
smbmonitoreo@grup1SMB:~$
```

también creamos la carpeta “/elastic” donde tendremos ahí toda la configuración del elastic

```
elastic@grup1SMB:/home/smbmonitoreo$ sudo mkdir /elastic
[sudo] password for elastic:
elastic@grup1SMB:/home/smbmonitoreo$ cd ..
elastic@grup1SMB:/home$ ls
elastic  smbmonitoreo  ubuntu
elastic@grup1SMB:/home$ cd /
elastic@grup1SMB:/ $ ls ..
bin  dev  etc  lib  lib64  lost+found  mnt  proc  run  snap  sys  usr
boot  elastic  home  lib32  libx32  media  opt  root  sbin  srv  tmp  var
elastic@grup1SMB:/ $ cd elastic/
elastic@grup1SMB:/elastic$
```

Una vez dentro, instalamos el kibana y el elasticsearch:

Elasticsearch:

```
elastic@grup1SMB:/elastic$ sudo wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-8.17.4-linux-x86_64.tar.gz
--2025-05-21 09:36:49-- https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-8.17.4-linux-x86_64.tar.gz
Resolving artifacts.elastic.co (artifacts.elastic.co)... 34.120.127.130, 2600:1901:0:1d7::
Connecting to artifacts.elastic.co (artifacts.elastic.co)|34.120.127.130|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 636389207 (607M) [application/x-gzip]
Saving to: 'elasticsearch-8.17.4-linux-x86_64.tar.gz'

elasticsearch-8.17.4-linu 100%[=====] 606.91M 15.0MB/s in 40s

2025-05-21 09:37:29 (15.2 MB/s) - 'elasticsearch-8.17.4-linux-x86_64.tar.gz' saved [636389207/636389207]

elastic@grup1SMB:/elastic$
```

Kibana:

```
elastic@grup1SMB:/elastic$ sudo wget https://artifacts.elastic.co/downloads/kibana/kibana-8.17.4-linux-x86_64.tar.gz
--2025-05-21 09:38:52-- https://artifacts.elastic.co/downloads/kibana/kibana-8.17.4-linux-x86_64.tar.gz
Resolving artifacts.elastic.co (artifacts.elastic.co)... 34.120.127.130, 2600:1901:0:1d7::
Connecting to artifacts.elastic.co (artifacts.elastic.co)|34.120.127.130|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 338458758 (323M) [application/x-gzip]
Saving to: 'kibana-8.17.4-linux-x86_64.tar.gz'

kibana-8.17.4-linux-x86_6 100%[=====] 322.78M 15.2MB/s in 22s

2025-05-21 09:39:14 (15.0 MB/s) - 'kibana-8.17.4-linux-x86_64.tar.gz' saved [338458758/338458758]

elastic@grup1SMB:/elastic$
```

y una vez descargados, los descomprimimos.

```
elastic@grup1SMB:/elastic$ sudo tar -xzf elasticsearch-8.17.4-linux-x86_64.tar.gz && sudo tar -xzf kibana-8.17.4-linux-x86_64.tar.gz
```

Winlogbeats & AuditBeat:

instalaremos el agente auditbeat (para ubuntu) y winlogbeats (para windows)

AuditBeat:

wget

https://artifacts.elastic.co/downloads/beats/auditbeat/auditbeat-8.17.4-linux-x86_64.tar.gz

```
elastic@grup1SMB: ~  
elastic@grup1SMB:~$ wget https://artifacts.elastic.co/downloads/beats/auditbeat/auditbeat-8.17.4-linux-x86_64.tar.gz  
--2025-05-23 10:11:39-- https://artifacts.elastic.co/downloads/beats/auditbeat/auditbeat-8.17.4-linux-x86_64.tar.gz  
Resolving artifacts.elastic.co (artifacts.elastic.co)... 34.120.127.130, 2600:1901:0:1d7::  
Connecting to artifacts.elastic.co (artifacts.elastic.co)|34.120.127.130|:443... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 41528351 (40M) [application/x-gzip]  
Saving to: 'auditbeat-8.17.4-linux-x86_64.tar.gz'  
  
auditbeat-8.17.4-li 100%[=====] 39.60M 50.6MB/s in 0.8s  
  
2025-05-23 10:11:41 (50.6 MB/s) - 'auditbeat-8.17.4-linux-x86_64.tar.gz' saved [41528351/41528351]  
  
elastic@grup1SMB:~$ sudo tar -xzf auditbeat-8.17.4-linux-x86_64.tar.gz
```

3. Configuración de los diferentes servicios:

NFS:

Para el servidor:

primero crearemos una copia del fichero de configuración en caso de que se corrompa o haya que hacer un backup:

```
sudo cp /etc/exports /etc/exports.backup
```

```
smbmonitoreo@grup1SMB:/elastic$ sudo cp /etc/exports /etc/exports.backup
smbmonitoreo@grup1SMB:/elastic$ ls /etc/ | grep exports
exports
exports.backup
smbmonitoreo@grup1SMB:/elastic$
```

una vez hecho el backup, editaremos el fichero con “sudo nano /etc/exports” y iremos al final del archivo, donde configuraremos nuestra carpeta que queremos compartir.

```
GNU nano 6.2 /etc/exports *
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4       gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes gss/krb5i(rw,sync,no_subtree_check)
#
```

en nuestro caso, como nos interesa una carpeta para cada uno, crearemos varias carpetas, una para cada servidor

En este caso para el de Audio y video, DNS, WEB y el servidor de base de datos.

```
smbmonitoreo@grup1SMB:~$ sudo mkdir /srv/audiovideo
[sudo] password for smbmonitoreo:
smbmonitoreo@grup1SMB:~$ sudo mkdir /srv/DNS
smbmonitoreo@grup1SMB:~$ sudo mkdir /srv/web
smbmonitoreo@grup1SMB:~$ sudo mkdir /srv/bbdd
smbmonitoreo@grup1SMB:~$
```

y los configuramos para que cada servidor vea su carpeta

```
GNU nano 6.2 /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
# to NFS clients. See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4 gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes gss/krb5i(rw,sync,no_subtree_check)
#
/srv/DNS 172.31.83.194(rw,sync,no_subtree_check)
/srv/audiovideo 172.31.89.60(rw,sync,no_subtree_check)
# FALTA IP
# /srv/bbdd IP_CLIENTE_BBDD(rw,sync,no_subtree_check)
# FALTA IP
# /srv/web IP_CLIENTE_WEB(rw,sync,no_subtree_check)

/srv/DNS 127.0.0.1(rw,sync,no_subtree_check) 172.31.93.89(rw,sync,no_subtree_check)
/srv/audiovideo 127.0.0.1(rw,sync,no_subtree_check) 172.31.93.89(rw,sync,no_subtree_check)
```

ahora hacemos un “sudo exportfs -ra” para que el fichero “/etc/exports” exporte todos los directorios y sincronizando el fstab con el /etc/exports

```
smbmonitoreo@grup1SMB:/elastic$ sudo nano /etc/exports
smbmonitoreo@grup1SMB:/elastic$ sudo exportfs -ra
smbmonitoreo@grup1SMB:/elastic$
```

Y les asignaremos permisos para que puedan acceder

```
smbmonitoreo@grup1SMB:/home/ubuntu$ sudo chown -R audiovideo_user:audiovideo_user /srv/audiovideo
smbmonitoreo@grup1SMB:/home/ubuntu$ sudo chmod -R 0770 /srv/audiovideo
smbmonitoreo@grup1SMB:/home/ubuntu$ sudo chown -R bbdd_user:bbdd_user /srv/bbdd
smbmonitoreo@grup1SMB:/home/ubuntu$ sudo chmod -R 0770 /srv/bbdd
smbmonitoreo@grup1SMB:/home/ubuntu$ sudo chown -R dns_user:dns_user /srv/DNS
smbmonitoreo@grup1SMB:/home/ubuntu$ sudo chmod -R 0770 /srv/DNS
smbmonitoreo@grup1SMB:/home/ubuntu$ sudo chown -R web_user:web_user /srv/web
smbmonitoreo@grup1SMB:/home/ubuntu$ sudo chmod -R 0770 /srv/web
smbmonitoreo@grup1SMB:/home/ubuntu$ ls -la /srv
total 24
drwxr-xr-x 6 root root 4096 May 21 06:59 .
drwxr-xr-x 20 root root 4096 May 22 06:03 ..
drwxrwx--- 2 dns_user dns_user 4096 May 21 06:59 DNS
drwxrwx--- 2 audiovideo_user audiovideo_user 4096 May 21 06:59 audiovideo
drwxrwx--- 2 bbdd_user bbdd_user 4096 May 21 06:59 bbdd
drwxrwx--- 2 web_user web_user 4096 May 21 06:59 web
smbmonitoreo@grup1SMB:/home/ubuntu$
```

Para los clientes:

primero creamos el directorio donde queramos poner la carpeta compartida:

“**sudo mkdir -p /mnt/nfs/dns_server_share**”

```
ubuntu@DNSserverip-172-31-92-232:~$ sudo mkdir -p /mnt/nfs/dns_server_share
ubuntu@DNSserverip-172-31-92-232:~$
```

y luego lo montamos con “**sudo mount -t nfs 3.226.157.142:/srv/DNS /mnt/nfs/dns_server_share**”

```
ubuntu@DNSserverip-172-31-92-232:~$ sudo mount -t nfs 3.226.157.142:/srv/DNS /mnt/nfs/dns_server_share/
ubuntu@DNSserverip-172-31-92-232:~$ df -h | grep nfs
3.226.157.142:/srv/DNS 78G 6.7G 71G 9% /mnt/nfs/dns_server_share
ubuntu@DNSserverip-172-31-92-232:~$ ls -la /mnt/nfs/dns_server_share/
total 8
drwxrwxr-x 2 nobody nogroup 4096 May 26 08:21 .
drwxr-xr-x 3 root root 4096 May 27 08:33 ..
-rw-r--r-- 1 root root 0 May 26 08:21 ola
```

en caso de querer hacer esto automáticamente cada vez que se inicie la máquina, configuramos el fichero “/etc/fstab” de cada máquina,

y agregamos la siguiente línea editando la IP y el directorio dependiendo del servidor:

`"3.226.157.142:/srv/DNS /mnt/nfs/dns_server_share nfs defaults,_netdev,rw 0 0`

```
GNU nano 7.2 /etc/fstab
LABEL=cloudimg-rootfs / ext4 discard,commit=30,errors=remount-ro 0 1
LABEL=BOOT /boot ext4 defaults 0 2
LABEL=UEFI /boot/efi vfat umask=0077 0 1

3.226.157.142:/srv/DNS /mnt/nfs/dns_server_share nfs defaults,_netdev,rw 0 0
```


Monitoreo:

ahora para configurar el elastic, tendremos que cambiar los permisos de la carpeta elastic.

```
elastic@grup1SMB:/elastic$ sudo chown -R elastic:elastic /elastic
elastic@grup1SMB:/elastic$ sudo chmod -R 755 /elastic
elastic@grup1SMB:/elastic$
```

y con el usuario de elastic, ejecutamos el fichero que genera toda la información: "elastic@grup1SMB:/elastic/elasticsearch-8.17.4\$./bin/elasticsearch" (le podemos poner un & para que se ejecute en segundo plano, y poder ejecutar kibana sin necesidad de abrir otro terminal)

y como resultado nos dará algo como esto:

```
✓ Elasticsearch security features have been automatically configured!
✓ Authentication is enabled and cluster connections are encrypted.

i Password for the elastic user (reset with `bin/elasticsearch-reset-password -u elastic`):
mL4sGLjaaC=TwrMnI6GY

i HTTP CA certificate SHA-256 fingerprint:
2970bf876e6bd9960da320b9ce760e983e3fec5761677a8cf58a77443525c49c

i Configure Kibana to use this cluster:
• Run Kibana and click the configuration link in the terminal when Kibana starts.
• Copy the following enrollment token and paste it into Kibana in your browser (valid for the next 30 minutes):
eyJ2ZXIiOiI4LjE0LjAiLCJhZHliOlsMTcyLjMxLjkzLjg5OjkyMDAiXSwiZmdyIjoImjk3MGJmODc2ZTZiZDk5NjBkYTMyMGIMGI5Y2U3NjBjOTgzZTNmZWMM1NzYXNjc3YThjZjU4YTc3NDQzNTI1YzQ5YyIsImtleSI6Im5iTTk4cFlCOWdMVWh5WFVyMzJpOmVpRHBXUC1yVGN1SkdnVHZZbDJMRkEifQ==

i Configure other nodes to join this cluster:
• On this node:
  - Create an enrollment token with `bin/elasticsearch-create-enrollment-token -s node`.
  - Uncomment the transport.host setting at the end of config/elasticsearch.yml.
  - Restart Elasticsearch.
• On other nodes:
  - Start Elasticsearch with `bin/elasticsearch --enrollment-token <token>`, using the enrollment token that you generated.
```

(he tenido que reiniciar la contraseña, así lo he hecho)

```
elastic@grup1SMB:/elastic$ sudo ./bin/elasticsearch-reset-password -u elastic
This tool will reset the password of the [elastic] user to an autogenerated value.
The password will be printed in the console.
Please confirm that you would like to continue [y/N]

Password for the [elastic] user successfully reset.
New value: 18hvWDa2xli-x1-WjAHS
elastic@grup1SMB:/elastic$
```

en este caso tenemos la siguiente información:

Password: 18hvWDa2xli-x1-WjAHS

CA: 2970bf876e6bd9960da320b9ce760e983e3fec5761677a8cf58a77443525c49c

Token:

eyJ2ZXIiOiI4LjE0LjAiLCJhZHliOlsMTcyLjMxLjkzLjg5OjkyMDAiXSwiZmdyIjoImjk3MGJmODc2ZTZiZDk5NjBkYTMyMGIMGI5Y2U3NjBjOTgzZTNmZWMM1NzYXNjc3YThjZjU4YTc3NDQzNTI1YzQ5YyIsImtleSI6Im5iTTk4cFlCOWdMVWh5WFVyMzJpOmVpRHBXUC1yVGN1SkdnVHZZbDJMRkEifQ==

Ahora, configuraremos el kibana. Nos iremos a su carpeta y ejecutaremos lo siguiente:
“elastic@grup1SMB:/elastic/kibana-8.17.4\$./bin/kibana-setup”

nos pedirá el token que nos ha generado antes, así que lo copiaremos directamente

```
elastic@grup1SMB:/elastic/kibana-8.17.4$ ./bin/kibana-setup
Kibana is currently running with legacy OpenSSL providers enabled! For details and instructions on how to disable see https://www.elastic.co/guide/en/kibana/8.17/production.html#openssl-legacy-provider
Native global console methods have been overridden in production environment.
? Enter enrollment token: eyJ2ZXIiOiI4LjE0LjAiLCJhZHI0I0siMTcyLjMxLjkzLjg5OjkyMDAiXSwiZmdyIjoimjk3MGJmODc2ZTZiZDk5NjBkYTMyMGI5Y2U3NjBlOTgzZTNmZWMM1NzYxNjc3YTJhZjU4YTc3NDQzNTIiYzQ5YyIsImtleSI6Im5iTTk4cFlCOwDMVWh5WFVyMzJpOmVpRHBXUC1yVGN1SkdnVHZzbDZMRKEifQ==

✓ Kibana configured successfully.

To start Kibana run:
  bin/kibana
elastic@grup1SMB:/elastic/kibana-8.17.4$
```

una vez lo tengamos configurado nos iremos a la carpeta de elastic de nuevo.

```
elastic@grup1SMB:/elastic$ sudo nano ./elasticsearch-8.17.4/config/elasticsearch.yml
```

y editaremos el fichero de configuración, donde tenemos que descomentar las opciones “network.host” y “http.port” del apartado “Network”.

```
GNU nano 6.2 ./.elasticsearch-8.17.4/config/elasticsearch.yml
#
# Path to directory where to store the data (separate multiple locations by comma):
#
#path.data: /path/to/data
#
# Path to log files:
#
#path.logs: /path/to/logs
#
# ----- Memory -----
#
# Lock the memory on startup:
#
#bootstrap.memory_lock: true
#
# Make sure that the heap size is set to about half the memory available
# on the system and that the owner of the process is allowed to use this
# limit.
#
# Elasticsearch performs poorly when the system is swapping the memory.
#
# ----- Network -----
#
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
#
network.host: 0.0.0.0
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
#
http.port: 9200
#
# For more information, consult the network module documentation.
#
# ----- Discovery -----
```

También tendremos que cambiar el fichero de configuración de kibana ubicado en **/elastic/kibana-8.17.4/config/kibana.yml**

```
GNU nano 6.2 config/kibana.yml *
# For more configuration options see the configuration guide for Kibana
# https://www.elastic.co/guide/index.html

# ===== System: Kibana Server =====
# Kibana is served by a back end server. This setting specifies the
#server.port: 5601

# Specifies the address to which the Kibana server will bind. IP address
# The default is 'localhost', which usually means remote machines will
# To allow connections from remote users, set this parameter to a non-loopback
server.host: "0.0.0.0"

# Enables you to specify a path to mount Kibana at if you are running behind a
# Use the `server.rewriteBasePath` setting to tell Kibana if it should
# from requests it receives, and to prevent a deprecation warning of
# This setting cannot end in a slash.
#server.basePath: ""
```

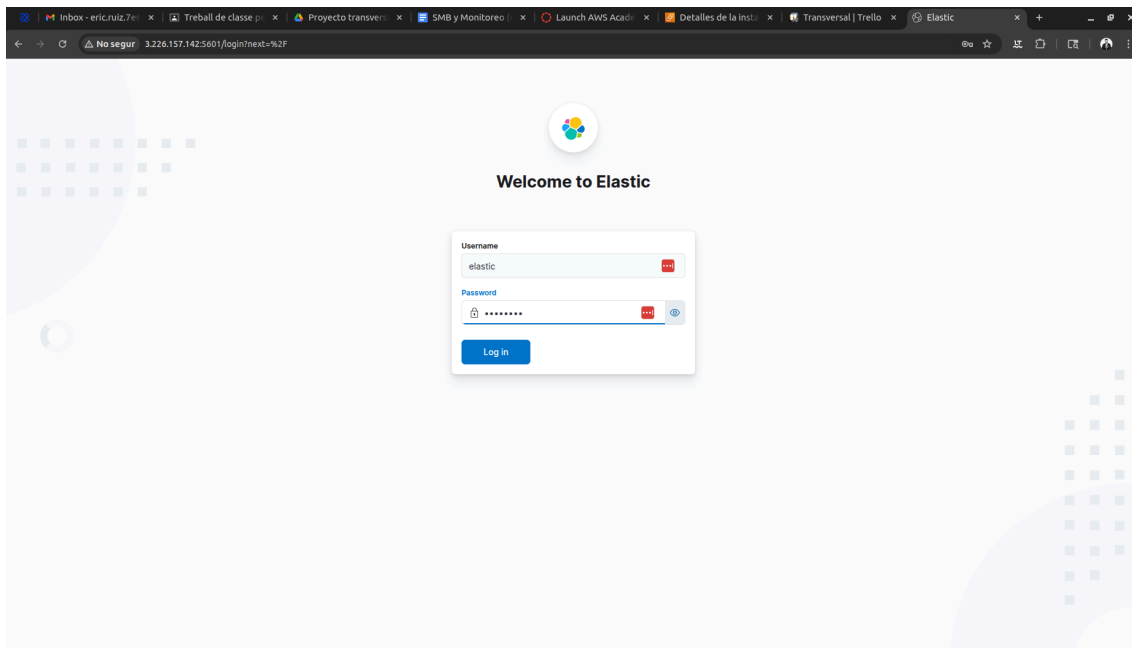
ES IMPORTANTE PONER LOS APARTADOS DE CERTIFICADOS Y XPACK EN FALSE O COMENTARLOS POR EL TEMA DEL HTTPS

Y por último, ejecutamos el kibana

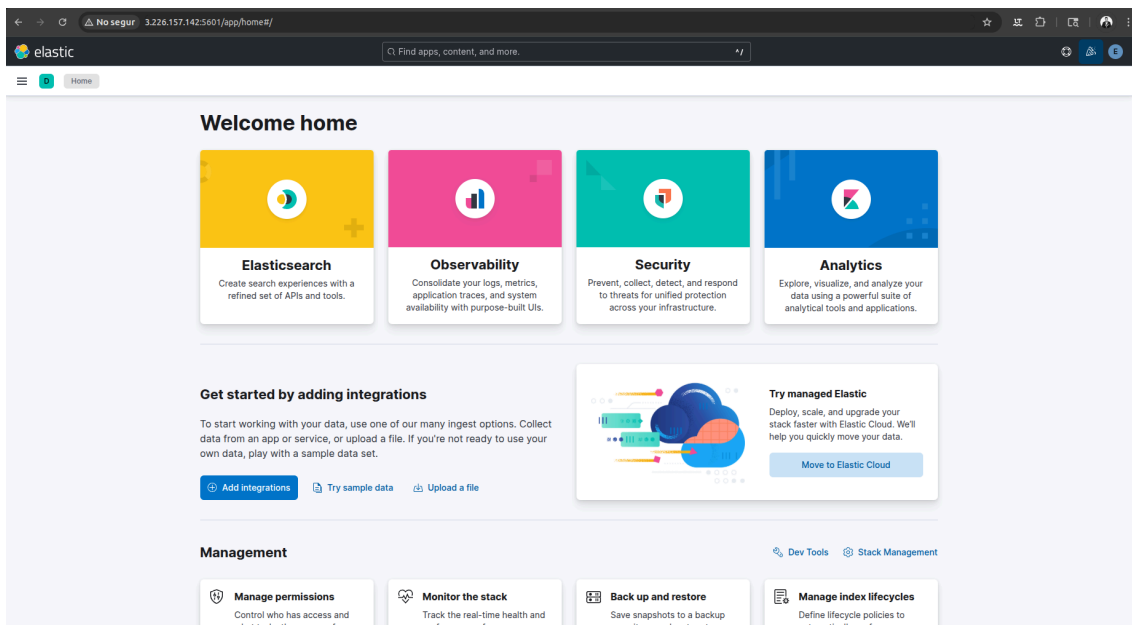
```
elastic@grup1SMB:/elastic$ cd kibana-8.17.4/
elastic@grup1SMB:/elastic/kibana-8.17.4$ ./bin/kibana
Kibana is currently running with legacy OpenSSL providers enabled! For details and instructions on how
to disable see https://www.elastic.co/guide/en/kibana/8.17/production.html#openssl-legacy-provider
{"log.level":"info","@timestamp":"2025-05-21T10:00:57.291Z","log.logger":"elastic-apm-node","ecs.version":"8.10.0",
"agentVersion":"4.10.0","env":{"pid":6206,"proctitle":"./bin/./node/glibc-217/bin/node","os":"linux 6.8.0-1029-aws",
"arch":"x64","host":"grup1SMB","timezone":"UTC+00","runtime":"Node.js v20.18.2"},"config":{"active":{"source":"start",
"value":true},"breakdownMetrics":{"source":"start","value":false},"captureBody":{"source":"start","value":"off",
"commonName":"capture_body"},"captureHeaders":{"source":"start","value":false},"centralConfig":{"source":"start",
"value":false},"contextPropagationOnly":{"source":"start","value":true},"environment":{"source":"start","value":"production"},
"globalLabels":{"source":"start","value":["git_rev","57a32881bd4c7055491b10f3c957e7dcef2f1bf0"]},"sourceValue":{"git_rev":"57a32881bd4c7055491b10f3c957e7dcef2f1bf0"},
"logLevel":{"source":"default","value":"info"},"commonName":"log_level"},"metricsInterval":{"source":"start","value":120,
"sourceValue":"120s"},"serverUrl":{"source":"start","value":"https://kibana-cloud-apm.apm.us-east-1.aws.found.io/",
"commonName":"server_url"},"transactionSampleRate":{"source":"start","value":0.1,"commonName":"transaction_sample_rate"},
"captureSpanStackTraces":{"source":"start","sourceValue":false},"secretToken":{"source":"start","value":"[REDACTED]",
"commonName":"secret_token"},"serviceName":{"source":"start","value":"kibana","commonName":"service_name"},"serviceVersion":{"source":"start",
"value":"8.17.4","commonName":"service_version"},"activationMethod":"require","message":"Elastic APM Node.js Agent v4.10.0"}
Native global console methods have been overridden in production environment.
```

(cabe recalcar, que tanto elasticsearch, como kibana deben estar ejecutándose en el terminal para que funcione todo)

Ahora, con todo ejecutado, solo tenemos que irnos a la máquina principal y conectarnos a la web (en nuestro caso, sería 3.226.157.142:5601)



(el usuario es elastic, y la contraseña la que nos ha dado antes)



y con esto ya tendríamos acceso a elastic y al monitoreo

Ahora para tener los logs y diferente información, configuraremos el auditbeat:

una vez tengamos extraído el fichero tar y tengamos su carpeta, editaremos el fichero "auditbeat.yml"

en el apartado kibana pondremos el host al que queremos mandar la información

```
elastic@grup1SMB: /elastic/auditbeat/auditbeat-8.17.4-linux-x86_64
GNU nano 6.2 auditbeat.yml
# versions, this URL points to the dashboard archive on the artifacts.elastic.co
# website.
#setup.dashboards.url:

# ===== Kibana =====

# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.
# This requires a Kibana endpoint configuration.
setup.kibana:

  host: "http://localhost:5601"
  username: "elastic"
  password: "18hvWda2xli-x1-WjAHS"
  # Kibana Host
  # Scheme and port can be left out and will be set to the default (http and 5601)
  # In case you specify an additional path, the scheme is required: http://localhost:5601/path
  # IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
  #host: "localhost:5601"

# Kibana Space ID
# ID of the Kibana Space into which the dashboards should be loaded. By default,
# the Default Space will be used.
#space.id:
```

y hacemos lo mismo con el apartado de elasticsearch

```
elastic@grup1SMB: /elastic/auditbeat/auditbeat-8.17.4-linux-x86_64
GNU nano 6.2 auditbeat.yml *
# Configure what output to use when sending the data collected by the beat.
# ----- Elasticsearch Output -----
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["http://localhost:9200"]
  username: "elastic"
  password: "18hvWda2xli-x1-WjAHS"

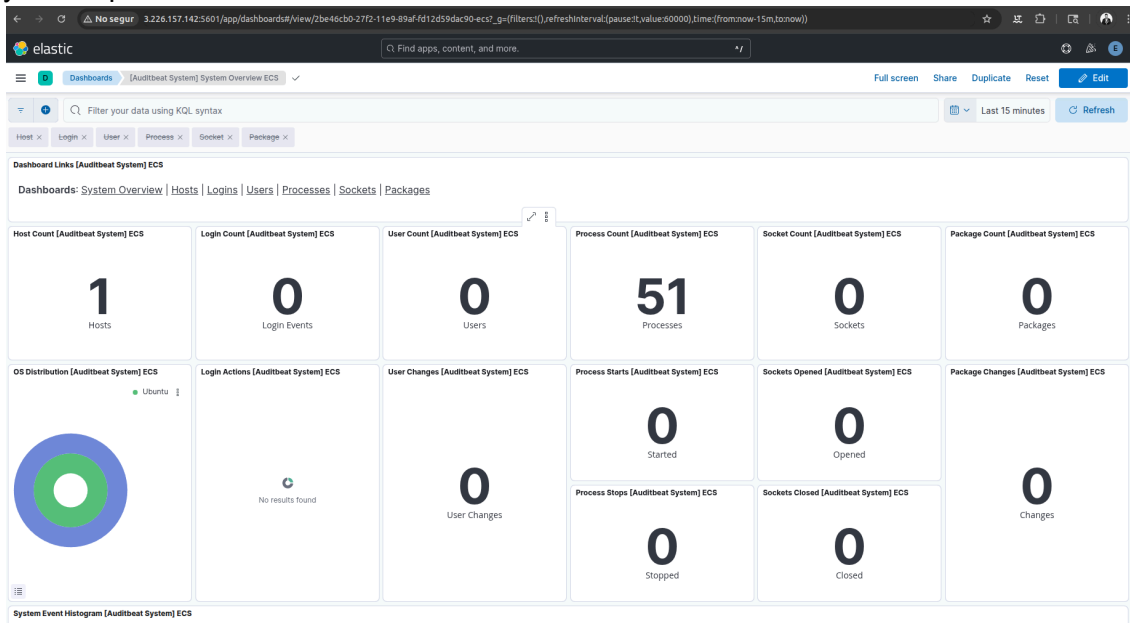
  # Performance preset - one of "balanced", "throughput", "scale",
  # "latency", or "custom".
  preset: balanced
  ssl.verification_mode: "none"
  # Protocol - either 'http' (default) or 'https'.
  #protocol: "https"

# Authentication credentials - either API key or username/password.
#api_key: "id:api_key"
#username: "elastic"
#password: "changeme"
```

Una vez configurado, cargamos los logs

y iniciamos el servicio

y ahora podríamos ver la información



ahora para que esto se inicie cada vez que el sistema arranque, crearemos un servicio de todo

```
ubuntu@grup1SMB: ~  
GNU nano 6.2 /etc/systemd/system/elasticsearch.service  
[Unit]  
Description=Elasticsearch  
After=network-online.target  
  
[Service]  
ExecStart=/elastic/elasticsearch-8.17.4/bin/elasticsearch  
User=elastic  
Group=elastic  
WorkingDirectory=/elastic/elasticsearch-8.17.4  
  
[Install]  
WantedBy=multi-user.target  
[ Wrote 12 lines ]  
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  ^C Location  
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify  ^_ Go To Line
```

```
ubuntu@grup1SMB: ~  
GNU nano 6.2 /etc/systemd/system/kibana.service  
[Unit]  
Description=Kibana  
After=network-online.target  
  
[Service]  
ExecStart=/elastic/kibana-8.17.4/bin/kibana  
User=elastic  
Group=elastic  
WorkingDirectory=/elastic/kibana-8.17.4  
  
[Install]  
WantedBy=multi-user.target  
[ Wrote 12 lines ]  
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  ^C Location  
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify  ^_ Go To Line
```

```

ubuntu@grup1SMB: ~
GNU nano 6.2 /etc/systemd/system/auditbeat.service
[Unit]
Description=Auditbeat
After=network-online.target

[Service]
ExecStart=/elastic/auditbeat/auditbeat-8.17.4-linux-x86_64/auditbeat -e
User=root
Group=root
WorkingDirectory=/elastic/auditbeat/auditbeat-8.17.4-linux-x86_64

[Install]
WantedBy=multi-user.target

[Wrote 12 lines]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line

ubuntu@grup1SMB:~$ sudo nano /etc/systemd/system/elasticsearch.service
ubuntu@grup1SMB:~$ sudo nano /etc/systemd/system/kibana.service
ubuntu@grup1SMB:~$ sudo nano /etc/systemd/system/auditbeat.service
ubuntu@grup1SMB:~$ sudo systemctl daemon-reload
ubuntu@grup1SMB:~$ sudo systemctl enable elasticsearch
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /etc/systemd/system/elasticsearch.service.
ubuntu@grup1SMB:~$ sudo systemctl start elasticsearch
ubuntu@grup1SMB:~$ sudo systemctl enable kibana
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service → /etc/systemd/system/kibana.service.
ubuntu@grup1SMB:~$ sudo systemctl enable auditbeat
Created symlink /etc/systemd/system/multi-user.target.wants/auditbeat.service → /etc/systemd/system/auditbeat.service.
ubuntu@grup1SMB:~$ sudo systemctl start kibana
ubuntu@grup1SMB:~$ sudo systemctl start auditbeat
ubuntu@grup1SMB:~$ sudo systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/etc/systemd/system/elasticsearch.service; enabled; vendor
   Active: active (running) since Fri 2025-05-23 10:58:12 UTC; 25s ago

```


ahora para los clientes descargamos lo mismo, el auditbeat, creamos el usuario elastic y ponemos la configuración en el auditbeat.yml

```
GNU nano 6.2 /elastic/auditbeat-8.17.4-linux-x86_64/auditbeat.yml
# This is an example configuration file highlighting only the most common
options. The auditbeat.reference.yml file from the same directory contains all
the supported options with more comments. You can use it as a reference.

# You can find the full configuration reference here:
https://www.elastic.co/guide/en/beats/auditbeat/index.html

#==== Modules configuration =====
auditbeat.modules:

- module: auditd
  # audit_rule_files: [ '${path.config}/audit.rules.d/*.conf' ]
  # audit_rules: [ ]

- module: file_integrity
  paths:
    - /bin
    - /usr/bin
    - /sbin
    - /usr/sbin
    - /etc

#==== Elasticsearch KIBANA setup =====
# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.
# This requires a Kibana endpoint configuration.
setup.kibana:
  host: "http://3.226.157.142:5601"
  username: "elastic"
  password: "18hvWDa2xli-x1-WjAHS"
  # space.id:

#==== Outputs =====
# Configure what output to use when sending the data collected by the beat.

#-----ELASTICSEARCH OUTPUT -----
# Array of hosts to connect to.
output.elasticsearch:
  hosts: ["http://3.226.157.142:9200"]
  username: "elastic"
  password: "18hvWDa2xli-x1-WjAHS"
  # Performance preset - one of "balanced", "throughput", "scale",
  # "latency", or "custom"
  # preset: balanced
  ssl_verification_mode: "none"
  # Protocol - either `http` (default) or `https`.
  # protocol: "https"
```