



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**
- 3 Job Guidelines**
- 3 General Responsibilities**
- 4 Company Safety Program**
- 5 Company Health and Environment Programs**
- 6 Company Cleaning Programs**
- 7 Construction Worker Employee Orientation**
- 8 Incident Investigating and Reporting**
- 9 Auditing and Inspecting**

1. Configurar y crear la Instancia:

Security Groups:

entrada

Reglas de entrada Información

ID de la regla del grupo de seguridad	Tipo <small>Información</small>	Protocolo <small>Información</small>	Intervalo de puertos <small>Información</small>	Origen <small>Información</small>	Descripción: opcional <small>Información</small>		
-	SMB	TCP	445	Anywh...	0.0.0.0/0	Samba	Eliminar
-	TCP personalizado	TCP	9200	Anywh...	0.0.0.0/0	Elasticsearch REST API	Eliminar
-	TCP personalizado	TCP	5601	Anywh...	0.0.0.0/0	Kibana UI	Eliminar
-	SSH	TCP	22	Anywh...	0.0.0.0/0	Conexion remota SSH	Eliminar
-	RDP	TCP	3389	Anywh...	0.0.0.0/0	Conexion remota RDP	Eliminar

[Agregar regla](#)

salida:

Reglas de salida Información

ID de la regla del grupo de seguridad	Tipo <small>Información</small>	Protocolo <small>Información</small>	Intervalo de puertos <small>Información</small>	Destino <small>Información</small>	Descripción: opcional <small>Información</small>		
sgr-0893f4c770b995345	Todo el tráfico	Todo	Todo	Person...	0.0.0.0/0	Actualizaciones, DNS, etc.	Eliminar

[Agregar regla](#)

Configuración de la instancia:

Ubuntu server:

Nombre y etiquetas

Nombre

SMB & Monitoreo

Agregar etiquetas adicionales

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

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

Proveedor verificado

Apto para la capa gratuita

Descripción

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

Canonical, Ubuntu, 24.04, amd64 noble image

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

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 “smbmonitoreo” 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:~$
```


Samba:

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

Para descargar el servicio usaremos la comanda “sudo apt install samba -y”

```
ubuntu@ip-172-31-93-89:~$ sudo apt install samba -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
samba is already the newest version (2:4.15.13+dfsg-0ubuntu1.6).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
ubuntu@ip-172-31-93-89:~$
```

Monitoreo:

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

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 descomprimos.

```
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
```

3. Configuración de los diferentes servicios:

Samba:

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

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.backup
```

```
smbmonitoreo@grup1SMB:~$ sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.backup
[sudo] password for smbmonitoreo:
smbmonitoreo@grup1SMB:~$ ls /etc/samba/
gdbcommands  smb.conf  smb.conf.backup  tls
smbmonitoreo@grup1SMB:~$
```

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

```
# (you need to configure Samba to act as a domain controller too.)
;[netlogon]
;   comment = Network Logon Service
;   path = /home/samba/netlogon
;   guest ok = yes
;   read only = yes

# Un-comment the following and create the profiles directory to store
# users profiles (see the "logon path" option above)
# (you need to configure Samba to act as a domain controller too.)
# The path below should be writable by all users so that their
# profile directory may be created the first time they log on
;[profiles]
;   comment = Users profiles
;   path = /home/samba/profiles
;   guest ok = no
;   browseable = no
;   create mask = 0600
;   directory mask = 0700

[printers]
comment = All Printers
browseable = no
path = /var/spool/samba
printable = yes
guest ok = no
read only = yes
create mask = 0700

# Windows clients look for this share name as a source of downloadable
# printer drivers
[print$]
comment = Printer Drivers
path = /var/lib/samba/printers
browseable = yes
read only = yes
guest ok = no

# Uncomment to allow remote administration of Windows print drivers.
# You may need to replace 'lpadmin' with the name of the group your
# admin users are members of.
# Please note that you also need to set appropriate Unix permissions
# to the drivers directory for these users to have write rights in it
; write list = root, @lpadmin
```

^{^G} Help ^{^O} Write Out ^{^W} Where Is ^{^K} Cut ^{^T} Execute ^{^C} Location
^{^X} Exit ^{^R} Read File ^{^N} Replace ^{^U} Paste ^{^J} Justify ^{^_} Go To Line

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

```
[BBDD]

comment = Servidor de Base de Datos
path = /srv/bbdd
browseable = yes
writable = yes
guest ok = no
valid users = bbdd_user
create mask = 0660
directory mask = 0770

[WEB]

comment = Servidor Web
path = /srv/web
browseable = yes
writable = yes
guest ok = no
valid users = web_user
create mask = 0660
directory mask = 0770

[DNS]

comment = Servidor DNS
path = /srv/DNS
browseable = yes
writable = yes
valid users = dns_user
create mask = 0660
directory mask = 0770

[Audio y Video]

comment = Servidor de Audio y video
path = /srv/audiovideo
browseable = yes
writable = yes
guest ok = no
valid users = audiovideo_user
create mask = 0660
directory mask = 0770
```

Y es asignaremos permisos para que puedan acceder

```
smbmonitoreo@grup1SMB:~$ sudo chown -R audiovideo_user:audiovideo_user /srv/audiovideo
[sudo] password for smbmonitoreo:
Sorry, try again.
[sudo] password for smbmonitoreo:
chown: invalid user: 'audiovideo_user:audiovideo_user'
smbmonitoreo@grup1SMB:~$ sudo chmod -R 0770 /srv/audiovideo
smbmonitoreo@grup1SMB:~$
```

(los usuarios serán sustituidos por otros usuarios)

Para que los otros puedan acceder con su usuario, hay que meter los usuarios y su contraseña a la base de datos de samba, eso lo hacemos con la comanda “sudo smbpasswd -a USER”, que en este caso, sería “audiovideo_user”.

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):
eyJ2ZXliOiI4LjE0LjAiLCJhZHliOlsMTcyLjMxLjkzLjg5OjkyMDAiXSwiZmdyIjoIMjk3MGJmODc2ZTZiZDk5NjBkYTMyMGIsY2U3NjB1OTgzZTNmZW1NzYxNjc3YTJhZjU4YTc3NDQzNTI1YzQ5YyIsImtleSI6Im5lTTk4cFICOWdMVWh5WFVyMzJpOmVpRHBXUC1yVGN1SkdnVHZZbDJMRkEifQ==

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.
```

en este caso tenemos la siguiente información:

Password: mL4sGLjaaC=TwrMnI6GY

CA: 2970bf876e6bd9960da320b9ce760e983e3fec5761677a8cf58a77443525c49c

Token:

eyJ2ZXliOiI4LjE0LjAiLCJhZHliOlsMTcyLjMxLjkzLjg5OjkyMDAiXSwiZmdyIjoIMjk3MGJmODc2ZTZiZDk5NjBkYTMyMGIsY2U3NjB1OTgzZTNmZW1NzYxNjc3YTJhZjU4YTc3NDQzNTI1YzQ5YyIsImtleSI6Im5lTTk4cFICOWdMVWh5WFVyMzJpOmVpRHBXUC1yVGN1SkdnVHZZbDJMRkEifQ==

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: eyJ2ZXIiOiI4LjE0LjAilCJhZHI0LsiMTcyLjMxLjkzLjg5OjkyMDAiXSwiZmduIjoimjk3MGJmODc2ZTZiZDk5NjBkYTMyMG15Y2U3NjBlOTgzZTNmZW11ZmZyYXNjc3YThjZjU4YTc3NDQzNTI1YzQ5YyIsImtleSI6Im5lTTk4cFliOmdMVWWh5WFVzMzJpOmVpRHBXUC1yVGN1SkdnVHZZbDZMRKEifQ==

✓ 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"

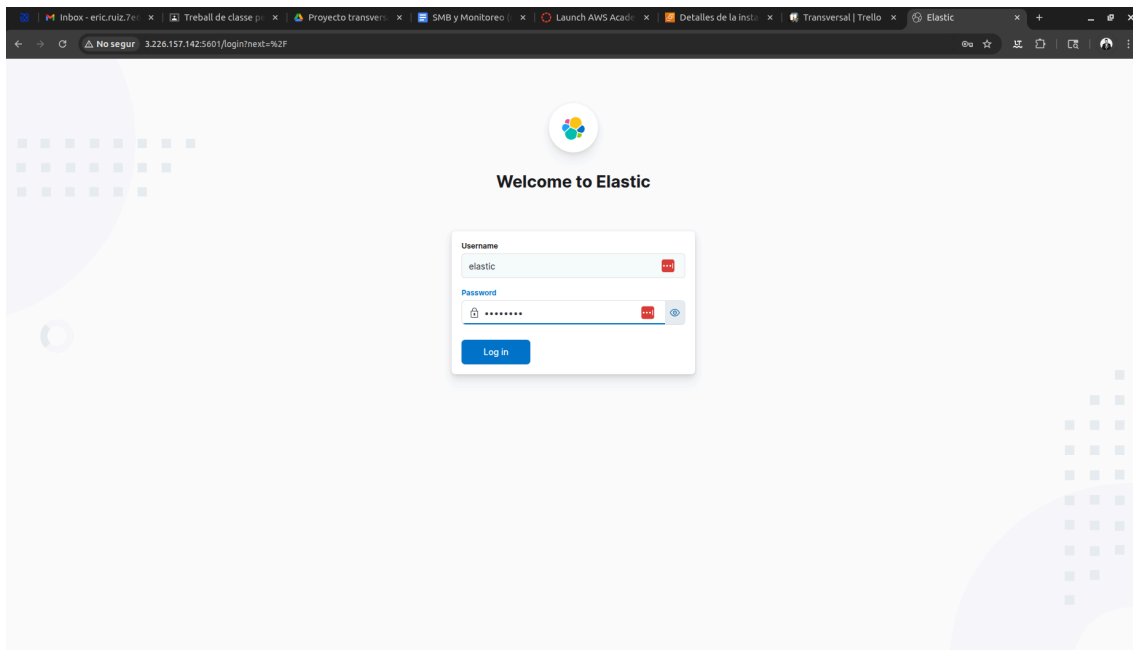
# Enables you to specify a path to mount Kibana at if you are running behind a
# Use the `server.rewriteBasePath` setting to tell Kibana if it should
# from requests it receives, and to prevent a deprecation warning at
# This setting cannot end in a slash.
#server.basePath: ""
```

Y por último, ejecutamos el kibana

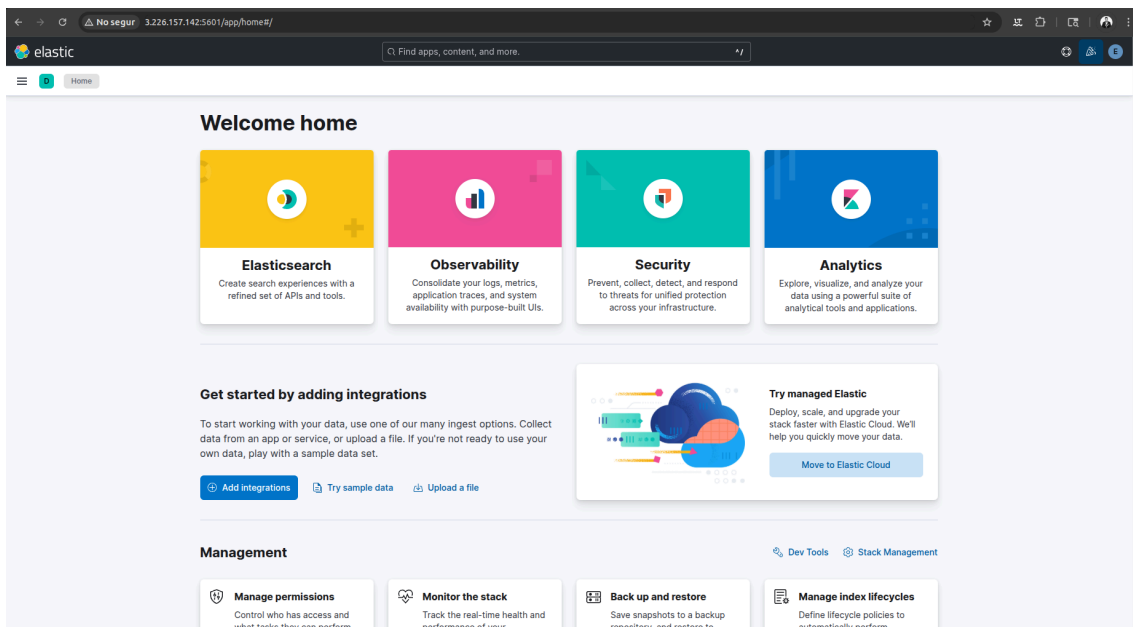
```
elastic@grup1SMB:/elastic$ cd kibana-8.17.4/
elastic@grup1SMB:/elastic/kibana-8.17.4$ ./bin/kibana
Kibana is currently running with legacy OpenSSL providers enabled! For details and instructions on how
to disable see https://www.elastic.co/guide/en/kibana/8.17/production.html#openssl-legacy-provider
{"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