

# Trabajo elastich search

## índice

<b>Objetivo del proyecto.....</b>	<b>2</b>
<b>¿Qué es Elasticsearch?.....</b>	<b>2</b>
Información sobre elasticsearch.....	2
Para que se utiliza Elasticsearch.....	2
Ventajas de Elasticsearch.....	2
Desventajas de Elasticsearch.....	3
Donde se creó Elasticsearch.....	3
¿Quién va a usar Elasticsearch?.....	3
<b>¿Qué es Kibana?.....</b>	<b>3</b>
¿Qué puede hacer Kibana?.....	3
Precios.....	4
Estándar.....	4
SEGURIDAD.....	4
OBSERVABILIDAD.....	5
BÚSQUEDA.....	5
SOPORTE.....	5
Oro.....	5
SEGURIDAD.....	5
SOPORTE.....	5
Platino.....	6
SEGURIDAD.....	6
OBSERVABILIDAD.....	6
BÚSQUEDA.....	6
SOPORTE.....	6
Enterprise.....	7
SEGURIDAD.....	7
OBSERVABILIDAD.....	7
BÚSQUEDA.....	7
SOPORTE.....	7
<b>Bibliografía.....</b>	<b>8</b>
<b>Solucionar error memoria virtual para maquina docker.....</b>	<b>8</b>
<b>Instalación de elasticsearch con docker.....</b>	<b>9</b>
<b>Instalación de kibana.....</b>	<b>11</b>
<b>instalando en fleet.....</b>	<b>20</b>
<b>Ver con más detalle la información.....</b>	<b>22</b>
<b>Cómo añadir nuevas máquinas a la flota y asignarles un agente de elastic.....</b>	<b>28</b>
Windows.....	28
Ubuntu.....	30
<b>Como instalar agente standalone.....</b>	<b>34</b>

# **Objetivo del proyecto**

El objetivo del proyecto es monitorear el gasto de recursos de varias computadoras desde una sola terminal, para ello usaremos elasticsearch para manejar los datos y kibana para visualizarlos.

## **¿Qué es Elasticsearch?**

Elasticsearch es un motor de búsqueda y analítica de RESTful distribuido basado en Lucene capaz de abordar un gran número de usos, es el núcleo del Elastic Stack y como tal almacena los datos de forma central, para una búsqueda a gran velocidad, una gran relevancia y poderosas capacidades analíticas que escalan con facilidad.

## **Información sobre elasticsearch**

### **Para que se utiliza Elasticsearch**

Se utiliza para buscar información entre una gran cantidad de datos, por ejemplo queremos saber cuántas personas se llaman Paula, entre los datos del censo de una ciudad por ejemplo.

### **Ventajas de Elasticsearch**

- Al estar desarrollado en Java, es compatible en todas las plataformas donde Java lo sea.
- Tiene una gran velocidad de respuesta.
- Es distribuido, lo que lo hace fácilmente escalable y adaptable a las distintas situaciones.
- Simple realización de respaldos de los datos almacenados.

- Utiliza objetos JSON como respuesta, por lo que es fácil de invocar desde varios lenguajes de programación.

## Desventajas de Elasticsearch

- Sólo soporta como tipos de respuesta JSON, lo que lo limita al no soportar otros lenguajes, como CSV o XML.
- Algunas situaciones pueden generar casos de [split-brain](#).

## Donde se creó Elasticsearch

Elasticsearch fue creado por Shay Banon cuando intentaba mejorar la herramienta que creó anteriormente llamada Compass, entonces llegó a la conclusión que debería reescribir grandes cantidades del código para crear un motor de búsqueda escalable, entonces creó elasticsearch el cual era escalable desde el comienzo, con la interfaz JSON sobre HTTP, muy común y adecuada para lenguajes de programación que no sean Java Shay Banon liberó la primera versión en febrero de 2010

## ¿Quién va a usar Elasticsearch?

Los usuarios de Elasticsearch pueden ser tanto particulares, como empresas, las principales empresas que lo usan son: Wikimedia, StumbleUpon, Mozilla, Quora, Foursquare, Etsy, SoundCloud, GitHub, FDA, CERN, y Stack Exchange

## ¿Qué es Kibana?

Kibana es el framework visual de Elasticsearch, y desde el mismo vamos a poder consultar los datos que tengamos ingestados de una forma más visual.

## ¿Qué puede hacer Kibana?

Con Kibana podemos:

- Dar forma a nuestros datos
- Crear objetos los índices para poder trabajar sobre ellos y aplicarles todas las facilidades que ofrece Kibana, como son

operaciones de machine learning, analítica de logs, análisis semántico de los campos de texto, etcétera.

- Crear visualizaciones
- Elaborar dashboards y reportes a un nivel bastante profesional con las visualizaciones.

-Diagnóstico

Resumen de todo lo anterior, exponiendo tambien los intereses futuros para las empresas y para ti mismo

## II Definición del proyecto

-Instalación del programa

-Funcionamiento

-Usos

## III Producción del proyecto

### Precios

Los precios están sacados de la página oficial de Elasticsearch

#### Estándar

El precio de la versión estándar de elasticsearch es de **95 usd al mes o 89,06 €**  
la versión estándar incluye:

Características fundamentales del Elastic Stack, incluida la seguridad  
Discover, estadísticas de campo, Kibana Lens, Elastic Maps y Canvas  
Alertas y acción en el stack

Agrupación y alta disponibilidad

Potente búsqueda y análisis

Visualización y dashboards de datos

Seguridad del stack

#### SEGURIDAD

Alertas, incluidos motor de detección y reglas prediseñadas

Ingesta centralizada y gestión de agente

Prevención contra malware y recopilación de datos de host

Gestión de casos

Gestión de postura de seguridad en el cloud (CSPM) y gestión de vulnerabilidad en el cloud (CNVM)

## OBSERVABILIDAD

Apps para APM, logging y métricas  
Cientos de integraciones listas para usar  
Ingesta centralizada y gestión de agente  
Acceso al servicio de pruebas globales gestionadas para Synthetic Monitoring2  
Universal Profiling

## BÚSQUEDA

Base de datos de vectores y búsqueda  
Relevancia personalizable  
Dashboards de analíticas de comportamiento  
Monitoreo con un clic  
Control de Acceso basado en roles  
Conectores nativos  
Clientes de conectores de código abierto e integraciones de rastreadores web 3  
Marco de trabajo de conector de código abierto para clientes de conector personalizados

## SOPORTE

Soporte basado en la web  
2 contactos de soporte  
Tiempo de respuesta objetivo de 3 días hábiles (solo Elastic Cloud)

## Oro

El precio de la versión Oro es de **109 usd al mes o 102,19 €**  
la versión oro incluye:

Todo lo incluido en la suscripción Estándar, más:  
Reportes  
Acciones de alertas de terceros  
Watcher  
Monitoreo de múltiples stacks

## SEGURIDAD

Flujos de trabajo optimizados, incluidos flujos de trabajo de respuesta ante incidentes de terceros  
Notificaciones y acciones externas de alerta de detección  
Configuración avanzada de gestión de host

## **SOPORTE**

Soporte en horario comercial

Soporte telefónico y basado en la web

6 contactos de soporte

Tiempo de respuesta inicial objetivo:

Urgente: 4 horas hábiles

Alto: 1 día hábil

Normal: 2 días hábiles

## **Platino**

El precio de la versión Platino es de **125 usd al mes o 117,19€**

la versión platino incluye:

Todo lo incluido en la suscripción Oro, más:

Características de seguridad avanzadas del Elastic Stack

Machine learning: detección de anomalías, aprendizaje supervisado, gestión de modelo de terceros

Replicación entre clusters

## **SEGURIDAD**

Detección de anomalías con machine learning y trabajos de SIEM prediseñados

Protección contra ransomware basada en el comportamiento

## **OBSERVABILIDAD**

Categorización de logs

Mapas de servicios

Muestreo posterior

Objetivos de nivel de servicios

Correlaciones de APM

Reglas de machine learning específicas del dominio

Acceso al servicio de pruebas globales gestionadas para Synthetic Monitoring<sup>2</sup>

Universal Profiling

## **BÚSQUEDA**

Búsqueda semántica con el modelo de ML Learned Sparse Encoder de Elastic

Soporte para modelo de inferencia de ML de terceros

Clasificación híbrida con fusión de rango recíproco

Seguridad a nivel de documento

## **SOPORTE**

Soporte permanente

Soporte telefónico y basado en la web

8 contactos de soporte

Tiempo de respuesta inicial objetivo:

Urgente: 1 hora

Alto: 4 horas

Normal: 1 día hábil

## **Enterprise**

El precio de la versión enterprise es de **175 usd al mes o 164,06 €**

la versión enterprise incluye:

Todo lo incluido en la suscripción Platino, más:

Snapshots buscables

Soporte para niveles frío y congelado buscables

Servidor de Elastic Maps

## **SEGURIDAD**

Snapshots buscables para retención prolongada de archivos procesables

Acciones de respuesta del host

Protección de cargas de trabajo en el cloud para visibilidad profunda de las cargas de trabajo

Orientación de Elastic AI Assistant para AI generativa

## **OBSERVABILIDAD**

Snapshots buscables para más datos de logs, métricas y APM

Acceso al servicio de pruebas globales gestionadas para Synthetic Monitoring2

Universal Profiling

Orientación de Elastic AI Assistant para AI generativa

## **BÚSQUEDA**

Snapshots buscables para más datos de contenido de aplicación y registros históricos del lugar de trabajo

## **SOPORTE**

Soporte permanente

Soporte telefónico y basado en la web

8 contactos de soporte

Tiempo de respuesta inicial objetivo:

Urgente:

Autogestionado: 1 hora

Elastic Cloud: 30 minutos

Alto: 4 horas

Normal: 1 día hábil

## **-otros factores**

Problemas dentro de la investigación del programa

-Proceso de evaluación  
cómo te has visto a ti mismo del proyecto, si estás contento o no con los resultados, etc...

## Bibliografía

Wikipedia  
<https://www.elastic.co/es/elasticsearch>

## Solucionar error memoria virtual para maquina docker

debemos hacer lo siguiente

```
sysctl -w vm.max_map_count=262144
```

pero eso es temporal y solo dura hasta que reiniciemos para que sea permanente  
debemos añadirlo al fichero vm.max\_map\_count a 262144 en /etc/sysctl.conf

añadiendo la siguiente línea

```
vm.max_map_count=262144
```

```

GNU nano 6.2                                         /etc/sysctl.conf *
#
# Do not send ICMP redirects (we are not a router)
#net.ipv4.conf.all.send_redirects = 0
#
# Do not accept IP source route packets (we are not a router)
#net.ipv4.conf.all.accept_source_route = 0
#net.ipv6.conf.all.accept_source_route = 0
#
# Log Martian Packets
#net.ipv4.conf.all.log_martians = 1
#
#####
# Magic system request Key
# 0=disable, 1=enable all, >1 bitmask of sysrq functions
# See https://www.kernel.org/doc/html/latest/admin-guide/sysrq.html
# for what other values do
#kernel.sysrq=438

vm.max_map_count=262144

^G Ayuda      ^O Guardar      ^W Buscar      ^K Cortar      ^T Ejecutar      ^C

```

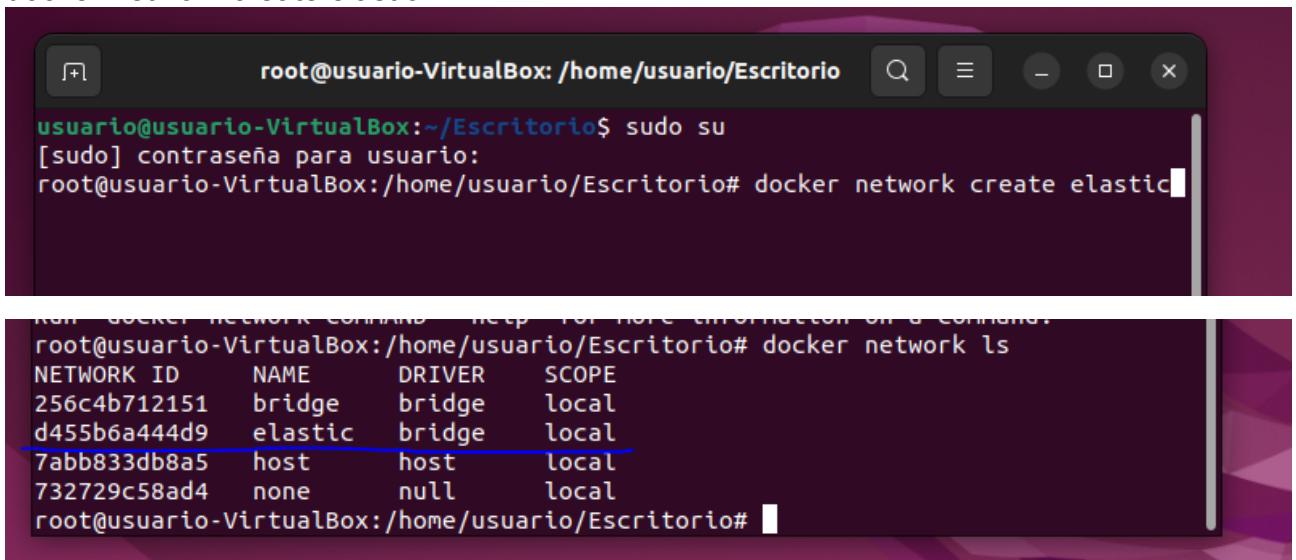
guardamos y una vez reiniciemos no tendremos que meter el comando cada vez

## Instalación de elasticsearch con docker

empezaremos con un cluster de un solo nodo

partiendo de que ya tenemos instalado docker en nuestra máquina, empezaremos creando una red para elastic search usando el siguiente comando en la consola

docker network create elastic



```

root@usuario-VirtualBox:~/Escritorio$ sudo su
[sudo] contraseña para usuario:
root@usuario-VirtualBox:/home/usuario/Escritorio# docker network create elastic

```

```

Run 'DOCKER_NETWORK_COMMAND --help' for more information on a command.
root@usuario-VirtualBox:/home/usuario/Escritorio# docker network ls
NETWORK ID      NAME      DRIVER      SCOPE
256c4b712151    bridge    bridge      local
d455b6a444d9    elastic   bridge      local
7abb833db8a5    host      host       local
732729c58ad4    none      null       local
root@usuario-VirtualBox:/home/usuario/Escritorio#

```

una vez la tenemos creada procedemos a hacer un pull de la imagen de docker en nuestro caso sera la version actual de docker la 8.12.2

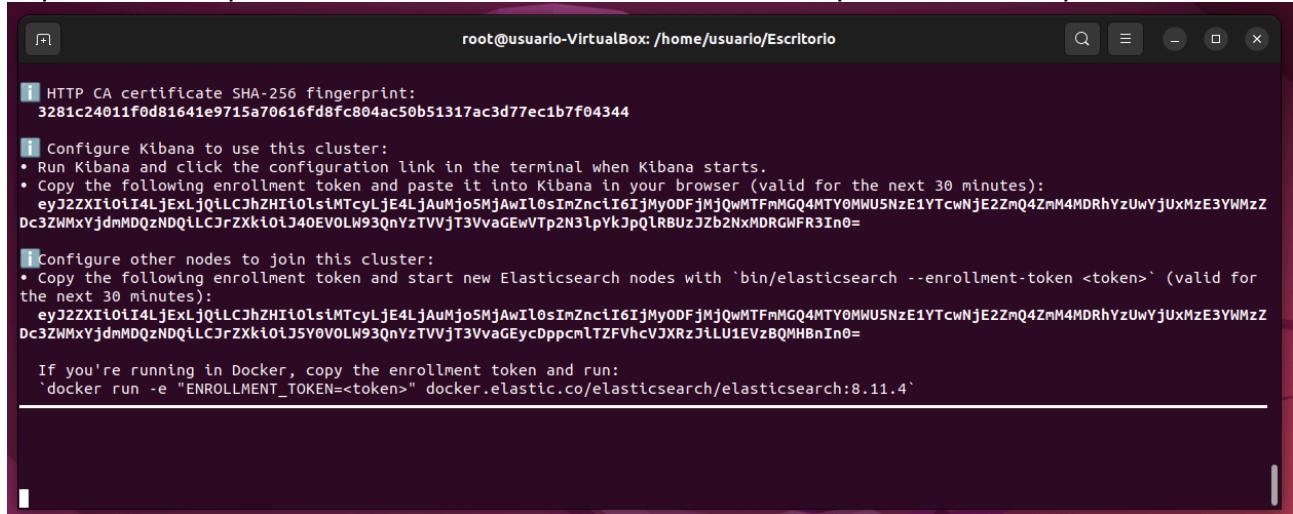
```
docker pull docker.elastic.co/elasticsearch/elasticsearch:8.12.2
```

```
root@usuario-VirtualBox:/home/usuario/Escritorio# docker pull docker.elastic.co/elasticsearch/elasticsearch:8.12.2
8.12.2: Pulling from elasticsearch/elasticsearch
43c43af79300: Pull complete
45d2cdef02ae: Pull complete
```

una vez tenemos la imagen usaremos el siguiente comando para crear la máquina

```
docker run --name es01 --net elastic -p 9200:9200 -it -m 1GB
docker.elastic.co/elasticsearch/elasticsearch:8.12.0
```

la primera vez que inicia nos enseñara unas contraseñas que debemos copiar



The screenshot shows a terminal window with the following text:

```
root@usuario-VirtualBox: /home/usuario/Escritorio
[i] HTTP CA certificate SHA-256 fingerprint:
3281c24011f0d81641e9715a70616fd8fc804ac50b51317ac3d77ec1b7f04344

[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):
eyJ2ZXIiOiI4LjExLjQlLCjhZHl0lsIMTcyLjE4LjAuMjo5MjAwIl0sImZnciI6IjMyODFjMjQwMTFmMGQ4MTY0MWU5NzE1YTwNjE2ZnQ4ZmM4MDRhYzUwYjUxMzE3YWMzZDc3ZWmxYjdmmMDQzNDQtlCJrZXkiOj40EVOLW93QnYzTVVjt3VvaGEwVtp2N3lpYkJpQLRBuZJzb2NxMDRGWFR3In0=

[i] Configure other nodes to join this cluster:
• Copy the following enrollment token and start new Elasticsearch nodes with `bin/elasticsearch --enrollment-token <token>` (valid for the next 30 minutes):
eyJ2ZXIiOiI4LjExLjQlLCjhZHl0lsIMTcyLjE4LjAuMjo5MjAwIl0sImZnciI6IjMyODFjMjQwMTFmMGQ4MTY0MWU5NzE1YTwNjE2ZnQ4ZmM4MDRhYzUwYjUxMzE3YWMzZDc3ZWmxYjdmmMDQzNDQtlCJrZXkiOj5Y0VOLW93QnYzTVVjt3VvaGEycDppcmLTZFVhcVjXRzJtLU1EVzBQMHBnIn0=

If you're running in Docker, copy the enrollment token and run:
'docker run -e "ENROLLMENT_TOKEN=<token>" docker.elastic.co/elasticsearch/elasticsearch:8.11.4'
```

si necesitamos regenerar alguna de estas contraseñas usaremos los siguientes comandos

```
docker exec -it es01 /usr/share/elasticsearch/bin/elasticsearch-reset-password -u elastic
```

```
docker exec -it es01 /usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana
```

una recomendación de la página de elastic search es exportar la contraseña como una variable de entorno

```
export ELASTIC_PASSWORD="your_password"
```

copiamos el certificado ssl del contenedor a nuestra máquina con el siguiente comando

```
docker cp es01:/usr/share/elasticsearch/config/certs/http_ca.crt .
```

```
[root@usuario-VirtualBox:~/home/usuario/Escritorio# docker cp es01:/usr/share/elasticsearch/config/certs/http_ca.crt .  
Successfully copied 3.58kB to /home/usuario/Escritorio/.  
root@usuario-VirtualBox:~/home/usuario/Escritorio# ]
```

Carpetas personales

Ahora con un curl nos aseguraremos que la máquina está funcionando

```
curl --cacert http_ca.crt -u elastic:$ELASTIC_PASSWORD https://localhost:9200
```

## Instalación de kibana

para instalar kibana una vez tenemos instalado el contenedor de elasticsearch

primero hacemos un pull de la imagen de kibana

```
docker pull docker.elastic.co/kibana/kibana:8.12.2
```

```
[sudo] contraseña para usuario:  
root@usuario-VirtualBox:~/home/usuario/Escritorio# docker pull docker.elastic.co/kibana/kibana:8.12.2  
8.12.2: Pulling from kibana/kibana  
43c43af79300: Already exists  
13b7446e8ebf: Pull complete  
b02f86acc41a: Pull complete  
2150654e511b: Pull complete  
6592d1999328: Pull complete  
4ca545ee6d5d: Pull complete  
92f42e7229b6: Pull complete  
e4190a16b8e2: Pull complete  
191d75e49308: Pull complete  
fc65d2978b2b: Pull complete  
66e5f58966fd: Pull complete  
b032ccb80beba: Pull complete  
bb6c7962b88d: Pull complete  
d02c86cbbf71: Pull complete  
Digest: sha256:529459ea3b52ff1d74fea3a1c8ef0b12d92222621de73dff9760f0433b163b14  
Status: Downloaded newer image for docker.elastic.co/kibana/kibana:8.12.2  
docker.elastic.co/kibana/kibana:8.12.2  
root@usuario-VirtualBox:~/home/usuario/Escritorio# ]
```

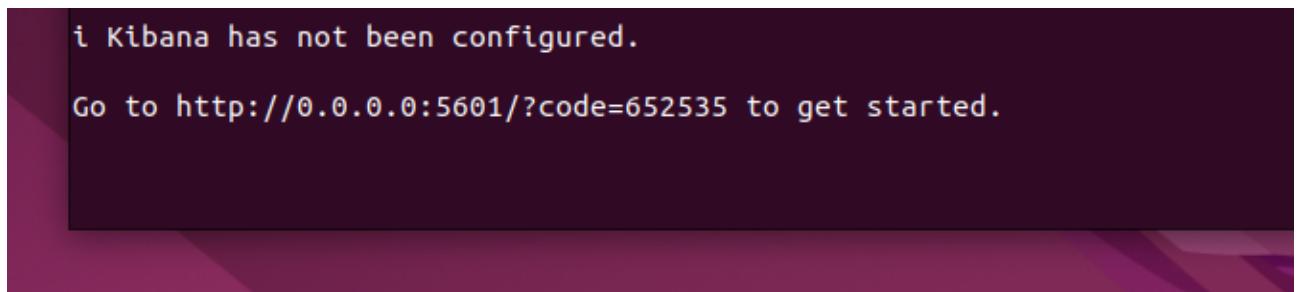
ahora usamos el siguiente comando para crear nuestro contenedor de kibana

```
docker run --name kib01 --net elastic -p 5601:5601 docker.elastic.co/kibana/kibana:8.12.2
```

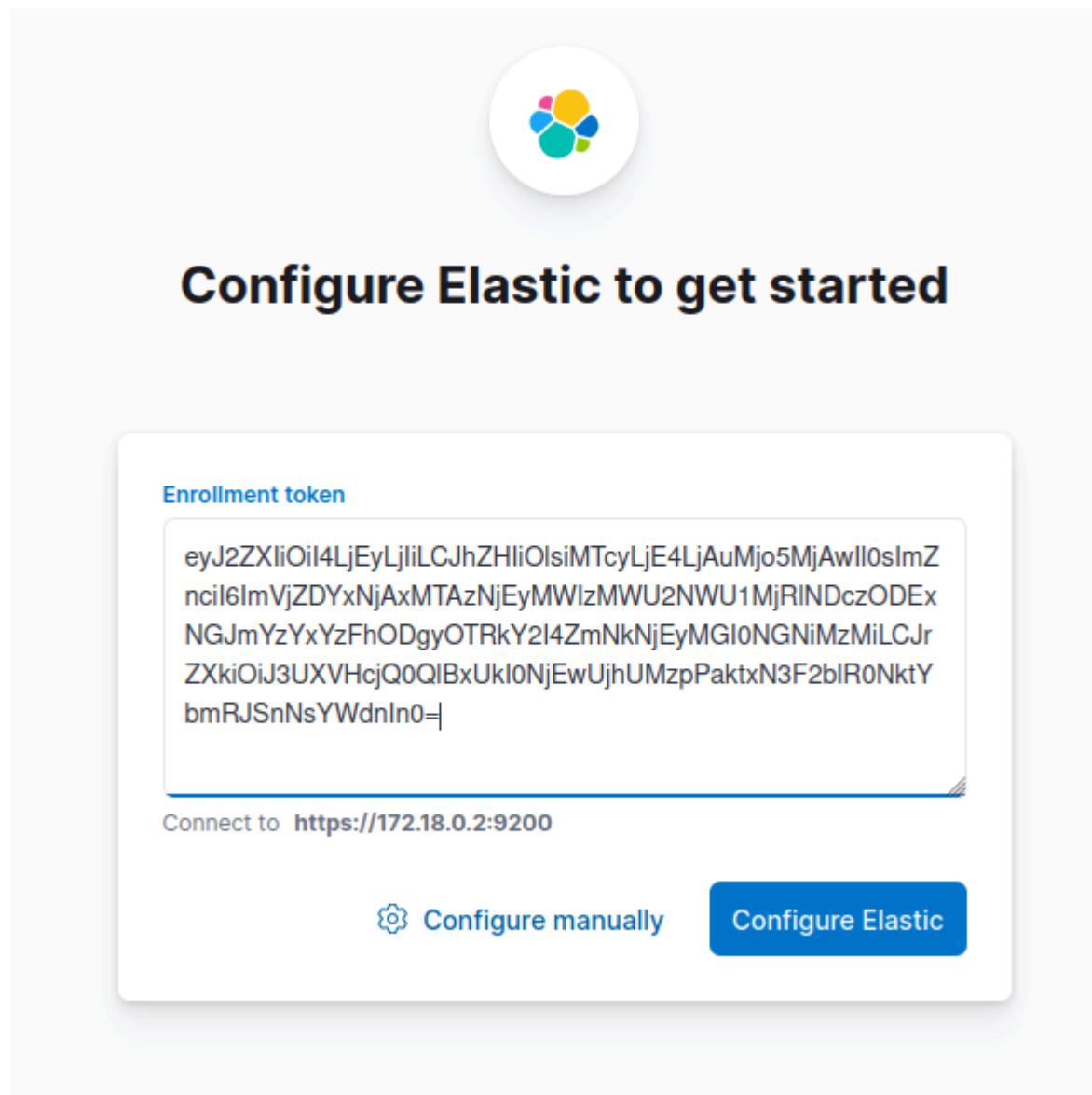
una vez iniciado nos iremos a la página que nos dice para la configuracion inicial de kibana

```
root@usuario-VirtualBox:/home/usuario/Escritorio# docker run --name kib01 --net elastic -p 5601:5601 docker.elastic.co/kibana/kibana:8.12.2
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/8.12.2/ssl.html
```

<http://0.0.0.0:5601/>

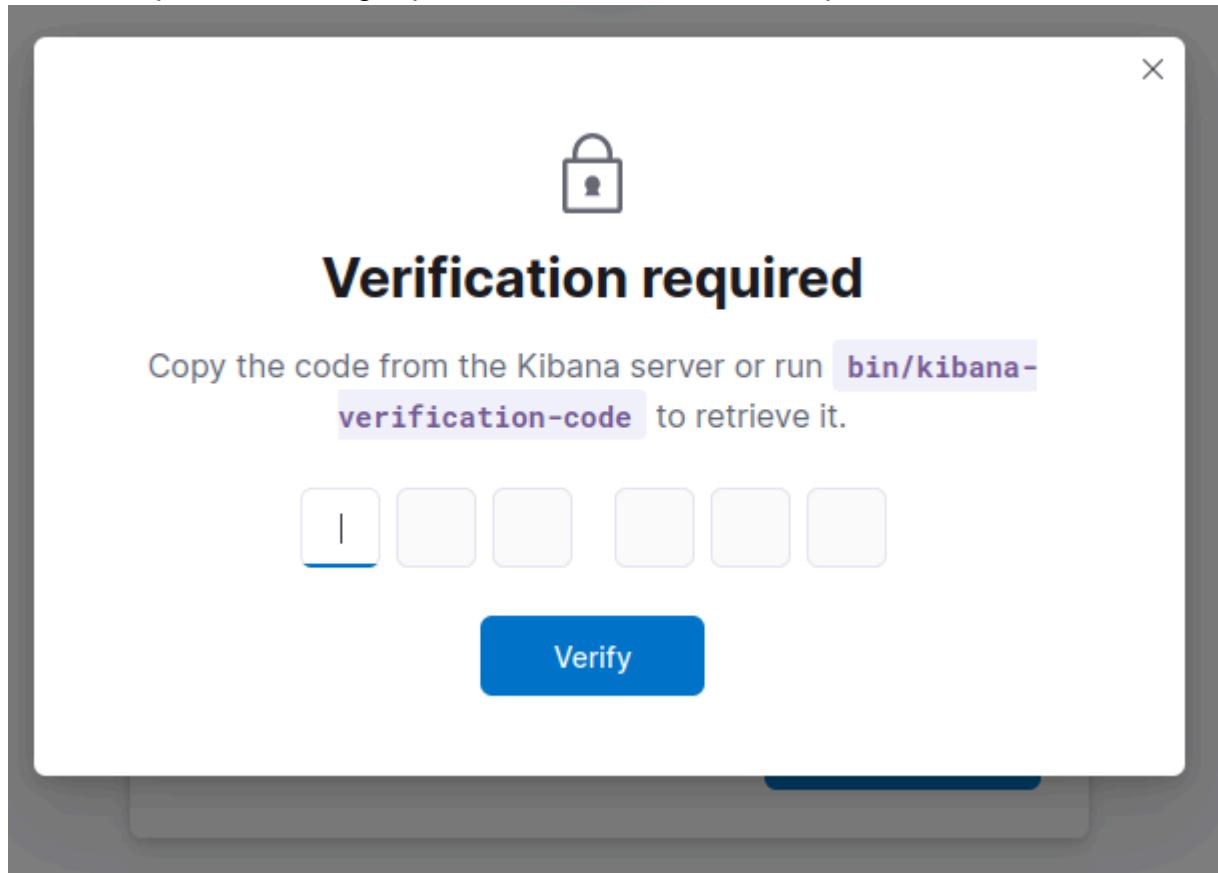


ahora tendremos que pegar el token que obtuvimos al instalar elasticsearch



ahora pulsamos configue elastic para continuar

ahora nos pedira un codigo que debemos sacar de la máquina del kibana



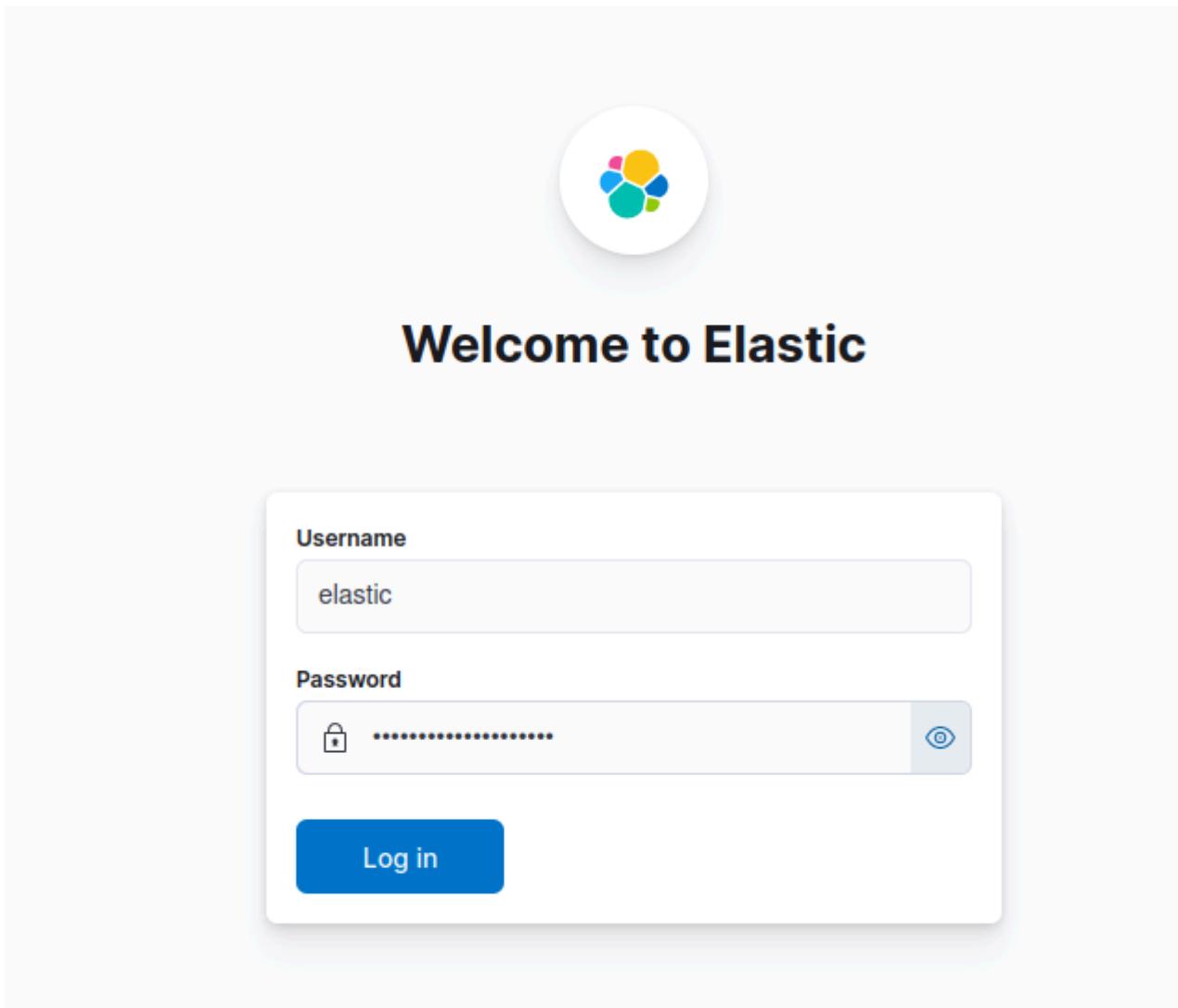
entramos a la máquina del kibana y usamos el comando  
`bin/kibana-verification-code`

```
root@usuario-VirtualBox:/home/usuario/Escritorio# docker exec -it kib01 bash
kibana@df6244a65c90:~$
```

```
kibana@df6244a65c90:~$ bin/kibana-verification-code
Kibana is currently running with legacy OpenSSL providers enabled! For
Your verification code is: 190 074
kibana@df6244a65c90:~$
```

ahora ponemos el código y se configurara automáticamente

una vez configurado para iniciar sesión usaremos el usuario elastic y la contraseña de elasticsearch



pulsamos log in

en nuestro caso guardaremos la contraseña en el navegador  
nos dará la bienvenida y que si queremos añadir integraciones o explorar por nuestra cuenta

# Welcome to Elastic



## Start by adding integrations

Add data to your cluster from any source, then analyze and visualize it in real time. Use our solutions to add search anywhere, observe your ecosystem, and defend against security threats.

[Add integrations](#)

[Explore on my own](#)

**Usage collection is enabled.** This allows us to learn what our users are most interested in, so we can improve our products and services. Refer to our [Privacy Statement](#). [Disable usage collection.](#)

en nuestro caso le daremos a explorar por nuestra cuenta y instalaremos los datos de prueba que tiene elasticsearch

### Get started by adding integrations

To start working with your data, use one of our many ingest options. Collect data from an app or service, or upload a file. If you're not ready to use your own data, play with a sample data set.

[+ Add integrations](#)

[Try sample data](#)

[Upload a file](#)

### Try managed Elastic

Deploy, scale, and upgrade your stack faster with Elastic Cloud. We'll help you quickly move your data.

[Move to Elastic Cloud](#)

en nuestro caso añadiremos los datos que aparecen abajo, pero también podemos mirar el entorno de prueba de la demo

**Explore our live demo environment**

Browse real-world data in a demo environment where you can explore search, observability, and security use cases like yours.

[Start exploring](#)

▼ Other sample data sets

**Sample eCommerce orders**

Sample data, visualizations, and dashboards for tracking eCommerce orders.

[Add data](#)

**Sample flight data**

Sample data, visualizations, and dashboards for monitoring flight routes.

[Add data](#)

**Sample web logs**

Sample data, visualizations, and dashboards for monitoring web logs.

[Add data](#)

[Activar \](#)
[Ve a Config](#)

simplemente le daremos a add data y cuando se descarguen ya podremos explorar los datos de prueba

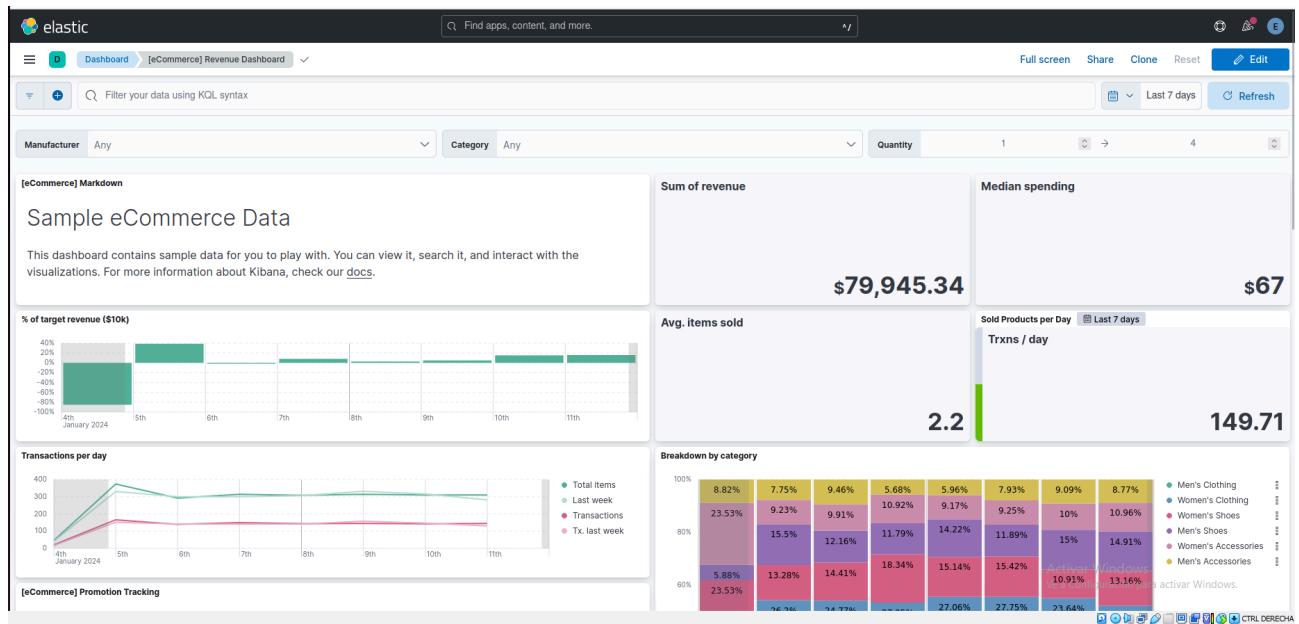
pulsaremos en view data y empezaremos a explorar los datos de prueba, nos aparecerán varias opciones nosotros le daremos a dashboard

▼ Other sample data sets

The screenshot shows the Kibana interface with a sidebar on the left containing a tree view of sample data sets. Three items are listed under the 'INSTALLED' section:

- Sample eCommerce orders**: Includes a summary card with metrics like Total revenue (\$80,027.35), Avg. items sold (2.2), and Median spending (\$67). Below it is a detailed description and two buttons: 'Remove' and 'View data'.
- Sample flight data**: Includes a summary card with metrics like Total flights (2.2k), Avg. passengers per flight (12.3%), and Total passengers (55.68k). Below it is a detailed description and two buttons: 'Remove' and 'View data'.
- Sample web logs**: Includes a summary card with metrics like Total logs (1.67k), Avg. log size (830), and Total bytes (3.71k). Below it is a detailed description and two buttons: 'Remove' and 'View data'.

nos aparecerá algo como esto



ahora probaremos a añadir alguna integración, en nuestro caso añadiremos una que mide el tráfico de red de Iptables

The screenshot shows the 'Get started by adding integrations' section of the Elastic Cloud interface. It includes a 'Try sample data' button, an 'Upload a file' button, and a search bar with the placeholder 'Search integrations...'. The background features a light gray gradient.

## Management

pulsamos add integrations y una vez dentro buscamos iptables

The screenshot shows the 'Integrations' page with a search bar containing 'iptables'. The results list includes categories like APM, AWS, Azure, Cloud, Containers, and Custom, each with a count of available integrations (e.g., 348 APM, 1 AWS). A detailed view of the 'Iptables' integration is shown, featuring a Linux penguin icon, the title 'Iptables', and a brief description: 'Collect logs from Iptables with Elastic Agent.'

una vez dentro le daremos a añadir integración

The screenshot shows the 'Iptables' integration page. At the top, there's a penguin icon and a 'Back to integrations' link. The title 'Iptables' is displayed with a 'Elastic Agent' badge. Below the title are tabs for 'Overview' (which is selected), 'Settings', and 'API reference'. A 'Version 1.15.1' badge is on the right, along with a blue 'Add Iptables' button. The main content area is titled 'Iptables Integration' and contains a brief description of what it does. To the right, there are 'Screenshots' showing two interface snippets. On the left, there's a sidebar with 'Iptables Integration Logs'.

en nuestro caso dejaremos los ajustes por defecto

This screenshot shows the 'Add Iptables integration' configuration page. It's step 1 of 1, titled 'Configure integration'. It includes sections for 'Integration settings' (with fields for name and optional description) and 'Collect iptables application logs (input: udp)' (with options for collecting syslogs via UDP). The 'Syslog Host' is set to 'localhost' and the 'Syslog Port' is set to '9001'. A note at the bottom says 'The UDP port to listen for syslog traffic. Ports below 1024 require Ellebeat to run as root.' A black bar at the bottom right contains buttons for 'Activar Windows', 'Cancel', 'Preview API request', and 'Save and continue'.

ahora nos aparecera una ventana de establecer un agente elastic en nuestro caso le diremos que luego y procederemos a la instalacion del agente

This screenshot shows a confirmation dialog box titled '1 Configure integration'. It displays the message 'Iptables integration added'. Below the message, it says 'To complete this integration, add **Elastic Agent** to your hosts to collect data and send it to Elastic Stack.' At the bottom, there are two buttons: 'Add Elastic Agent later' (grayed out) and 'Add Elastic Agent to your hosts' (highlighted in blue).

# instalando en fleet

primero crearemos una fleet poniendo el nombre que queramos ponerle y la dirección ip de nuestra maquina en formato <https://192.168.0.0>

## Get started with Fleet Server

- ✓ Fleet Server policy created.

Fleet server policy and service token have been generated. Host configured at <https://192.168.100.108:443>. You can edit your Fleet Server hosts in [Fleet Settings](#).

Ahora seguiremos los siguientes comandos que nos dice la guia

2

## Install Fleet Server to a centralized host

Install Fleet Server agent on a centralized host so that other hosts you wish to monitor can connect to it. In production, we recommend using one or more dedicated hosts. For additional guidance, see our [installation docs](#).

[Linux Tar](#) [Mac](#) [Windows](#) [RPM](#) [DEB](#)

```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/e
tar xzvf elastic-agent-8.12.0-linux-x86_64.tar.gz
cd elastic-agent-8.12.0-linux-x86_64
sudo ./elastic-agent install \
--fleet-server-es=https://172.18.0.2:9200 \
--fleet-server-service-token=AAEAAWVsYXN0aWMvZmx1ZXQtc2VydmVyL3Rva2Vu
--fleet-server-policy=fleet-server-policy \
--fleet-server-es-ca-trusted-fingerprint=46895f502781ac0ec7e4af09499c
--fleet-server-port=8220
```

```

usuario@usuario-virtual:~/Escritorio/elastic-agent-8.12.0-linux-x86_64$ sudo su
[sudo] contraseña para usuario:
root@usuario-virtual:/home/usuario/Escritorio/elastic-agent-8.12.0-linux-x86_64# sudo ./elastic-agent install \
> --fleet-server-es=https://172.18.0.2:9200 \
> --fleet-server-service-token=AAEAAWsyXN0awMvZmxLZXQtc2VydnyL3Rva2VuLTE3MDY0NzY2Nz2NDQ6UldvzNCbfVTWG1QanlCVHVFVElqUQ \
> --fleet-server-policy=fleet-server-policy \
> --fleet-server-es-ca-trusted-fingerprint=46895f502781ac0ec7e4af09499cac52aa87491c77c9a0d7b9e839a366b412da \
> --fleet-server-ports=8220
Elastic Agent will be installed at /opt/Elastic/Agent and will run as a service. Do you want to continue? [Y/n]:y
[= ] Service Started [3m4s] Elastic Agent successfully installed, starting enrollment.
[= ] Waiting For Enroll... [3m7s] {"log.level":"info","@timestamp":"2024-01-28T22:18:22.780+0100","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":419},"message":"Generating self-signed certificate for Fleet Server","ecs.version":"1.6.0"}
[= ] Waiting For Enroll... [3m7s] {"log.level":"info","@timestamp":"2024-01-28T22:18:23.578+0100","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":461},"message":"Restarting agent daemon, attempt 0","ecs.version":"1.6.0"}
[==>] Waiting For Enroll... [3m9s] {"log.level":"info","@timestamp":"2024-01-28T22:18:25.582+0100","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":804},"message":"Waiting for Elastic Agent to start Fleet Server","ecs.version":"1.6.0"}
[==>] Waiting For Enroll... [3m21s] {"log.level":"info","@timestamp":"2024-01-28T22:18:37.591+0100","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":837},"message":"Fleet Server - Starting: spawned pid 9471","ecs.version":"1.6.0"}
[==>] Waiting For Enroll... [3m37s] {"log.level":"info","@timestamp":"2024-01-28T22:18:53.593+0100","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":837},"message":"Fleet Server - Starting","ecs.version":"1.6.0"}
[==>] Waiting For Enroll... [3m49s] {"log.level":"info","@timestamp":"2024-01-28T22:19:25.597+0100","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":818},"message":"Fleet Server - Running on policy with Fleet Server integration: fleet-server-policy; missing config fleet.agent.id (expected during bootstrap process)","ecs.version":"1.6.0"}
[==>] Waiting For Enroll... [3m49s] {"log.level":"info","@timestamp":"2024-01-28T22:19:26.281+0100","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":496},"message":"Starting enrollment to URL: https://usuario-virtual:8220/","ecs.version":"1.6.0"}
[==>] Waiting For Enroll... [3m49s] {"log.level":"info","@timestamp":"2024-01-28T22:20:55.932+0100","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":461},"message":"Restarting agent daemon, attempt 0","ecs.version":"1.6.0"}
("log.level":"info","@timestamp":"2024-01-28T22:20:55.934+0100","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":285}),"message":"Successfully triggered restart on running Elastic Agent.","ecs.version":"1.6.0"}
Successfully enrolled the Elastic Agent.
[ ==] Done [5m40s]
Elastic Agent has been successfully installed.
root@usuario-virtual:/home/usuario/Escritorio/elastic-agent-8.12.0-linux-x86_64#
```

Successfully enrolled the Elastic Agent.

[ ==] Done [5m40s]

Elastic Agent has been successfully installed.

una vez terminado nos saldra esto le pulsamos a continue

## Fleet Server connected

You can now continue enrolling agents with Fleet.

[Continue enrolling Elastic Agent](#)

una vez tengamos esto hecho ya deberíamos poder ver datos en elastic search en la sección fleet vemos que esta funcionando bien y recoge datos

## Fleet

Centralized management for Elastic Agents.

[Agents](#) [Agent policies](#) [Enrollment tokens](#) [Uninstall tokens](#) [Data streams](#) [Settings](#)

### ① Set up encryption key

An encryption key will make your environment more secure. Click [here](#) to learn how to set up an encryption key.

[Dismiss](#)

[② Agent activity](#) [Add Fleet Server](#) [Add agent](#)

Filter your data using KQL syntax Status Tags Agent policy Upgrade available

Showing 1 agent		Filter					
Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
<span>Healthy</span>	usuario-virtualbox	Fleet Server Policy rev. 1	0.85 %	240 MB	29 seconds ago	8.12.0	<a href="#">...</a>

Rows per page: 20 < 1 >

# Ver con más detalle la información

si entramos a los detalles podemos ver que integraciones tiene instaladas

The screenshot shows the Grafana Agent details page for the host 'usuario-virtualbox'. The top navigation bar includes 'View all agents' and 'Actions'. Below the title 'usuario-virtualbox', there are tabs for 'Agent details' (which is selected), 'Logs', and 'Diagnostics'. The 'Overview' section displays various metrics and status information:

Metric	Value
CPU	0.85 %
Memory	240 MB
Status	Healthy
Last activity	8 seconds ago
Last checkin message	Running
Agent ID	6129e71c-1955-4d84-84b1-51008aa2fd41
Agent policy	Fleet Server Policy rev. 1
Agent version	8.12.0
Host name	usuario-virtualbox
Logging level	info
Agent release	stable
Platform	ubuntu
Monitor logs	Enabled
Monitor metrics	Enabled
Tags	-

The 'Integrations' section lists two installed integrations:

- system-2 (represented by a heart rate monitor icon)
- fleet\_server-1 (represented by a cluster icon)

en nuestro caso tenemos la integracion para ver los datos del sistema

para verlo con más detalle iremos a la pestaña dashboards

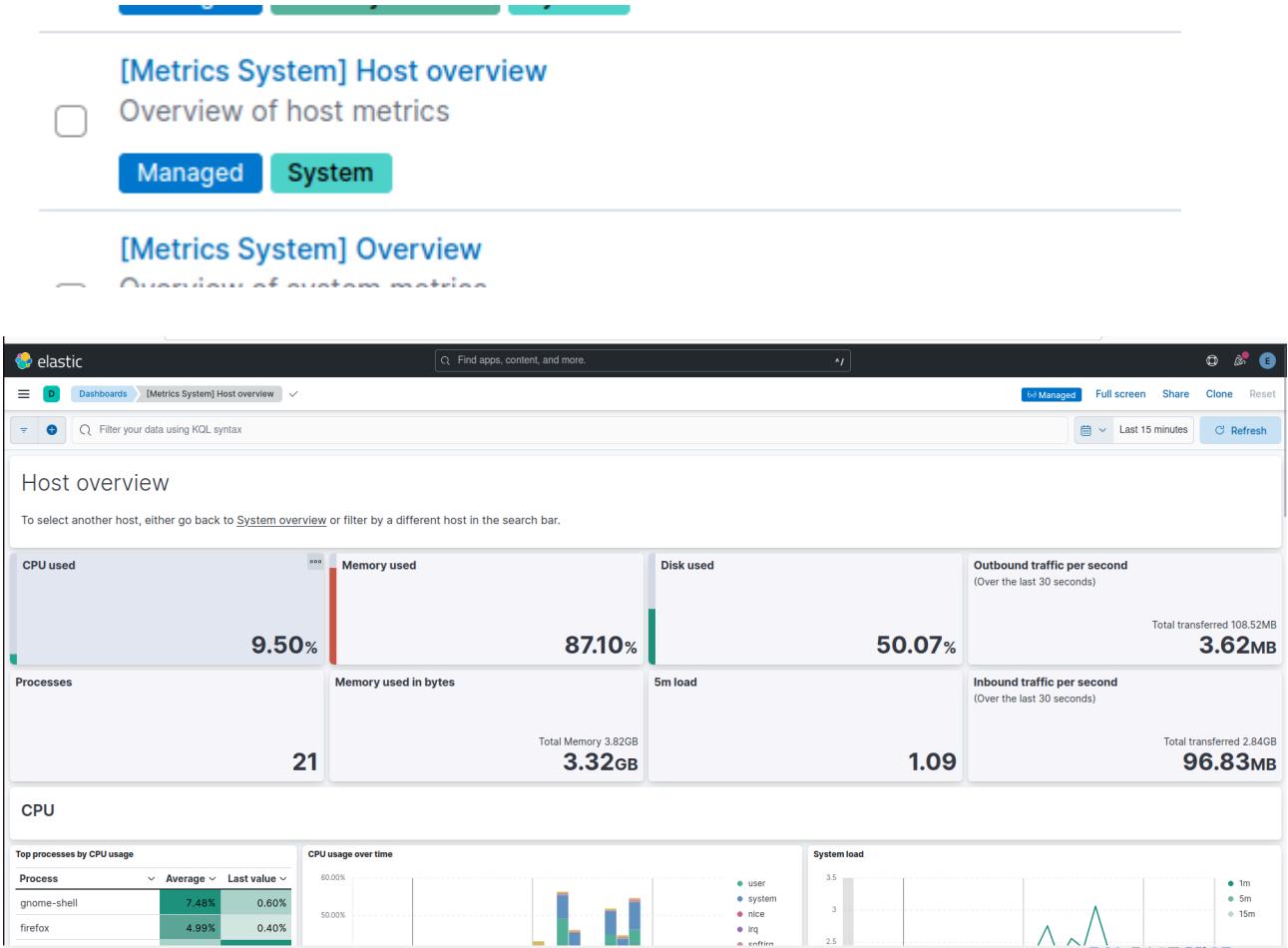
The screenshot shows the Elastic Stack interface. At the top, there's a dark header with the 'elastic' logo. Below it, a navigation bar has 'Dashboards' selected. On the left, a sidebar lists sections: 'Recently viewed', 'Analytics' (with 'Discover', 'Dashboards', 'Canvas', 'Maps', 'Machine Learning', 'Visualize Library'), and 'Search' (with 'Overview', 'Content', 'Elasticsearch'). The main area shows a search bar with 'syntax' and a large number '33.2'. A link 'go back to System' is visible.

## Dashboards

<input type="text"/> Search...	<input type="button"/> Recently updated	<input type="button"/> Tags	<input type="button"/> Create dashboard
<input type="checkbox"/> Name, description, tags	Last updated ↓		Actions
[System Windows Security] Failed and Blocked Accounts	29 minutes ago		
<input type="checkbox"/> Failed and blocked accounts. <small>Managed Security Solution System</small>	29 minutes ago		
[System Windows Security] Group Management Events	29 minutes ago		
<input type="checkbox"/> Group management activity. <small>Managed Security Solution System</small>	29 minutes ago		

aquí seleccionaremos el que nos interesa

en nuestro caso iremos a métricas del sistema



como vemos nos pode bastantes métricas como la carga de cpu, la memoria ram usada, como está de lleno el disco, el tráfico de red entrante y saliente, los procesos en ejecución y si bajamos veremos los distintos apartados con más detalle



ahora veremos un poco la pestaña de fleet

aquí podremos ver los agentes que tenemos instalados y conectados a nuestra máquina trayendo datos de la propia máquina o de otras

## Fleet

Centralized management for Elastic Agents.

Agents Agent policies Enrollment tokens Uninstall tokens Data streams Settings

### ① Set up encryption key

An encryption key will make your environment more secure. Click [here](#) to learn how to set up an encryption key.

Dismiss

⌚ Agent activity

Add Fleet Server

Add agent

Filter your data using KQL syntax							
		Status 4	Tags 0	Agent policy 2	Upgrade available		
Showing 1 agent Clear filters							
Status	Host	Agent policy	CPU ⓘ	Memory ⓘ	Last activity	Version	Actions
<input type="checkbox"/>	Healthy usuario-virtualbox	Fleet Server Policy rev. 1	0.92 %	240 MB	16 seconds ago	8.12.0	...

Rows per page: 20

< 1 >

en agent policies podemos ver cuales tenemos creadas y si tienen agentes y crear nuevas políticas

Centralized management for Elastic Agents.

Agents Agent policies Enrollment tokens Uninstall tokens Data streams Settings

Filter your data using KQL syntax				
Name	Description	Last update...	Agents	Integrations
Fleet Server Policy rev. 1	Fleet Server policy generated by Kibana	Jan 29, 2024	1	2
Agent policy 1 rev. 3		Jan 29, 2024	0	2

Rows per page: 20

< 1 >

en la siguiente pestaña podemos ver los tokens que deben usar los agentes para poder acceder

Agents Agent policies Enrollment tokens Uninstall tokens Data streams Settings

Create and revoke enrollment tokens. An enrollment token enables one or more agents to enroll in Fleet and send data.

Filter your data using KQL syntax				
Name	Secret	Agent policy	Created on	Active Actions
Default (00a0d92c-8c54-4d30-b9a2-16db... .....	.....	⌚ Fleet Server Policy	Jan 29, 2024	● ⚡
Default (645cf378-7fc8-4150-9c2b-771d78... .....	.....	⌚ Agent policy 1	Jan 29, 2024	● ⚡

Rows per page: 20

< 1 >

la siguiente pestaña sirve para borrar algún token que ya no nos haga falta

Agents	Agent policies	Enrollment tokens	Uninstall tokens	Data streams	Settings
Uninstall token allows you to get the uninstall command if you need to uninstall the Agent/Endpoint on the Host.					
<input type="text"/> Search by policy ID					
Policy ID			Created at	Token	Actions
fleet-server-policy			Jan 29, 2024	.....	
62f773d1-ed04-408a-9372-67d0dcfec04			Jan 29, 2024	.....	
Rows per page: 20			< 1 >		

la pestaña data streams nos dice de donde estamos recibiendo datos y de que integración

Agents	Agent policies	Enrollment tokens	Uninstall tokens	Data streams	Settings
<input type="text"/> Filter data streams				Dataset  Type  Namespace  Integration	
Dataset	Type	Namespace	Integration	Last activity	Size
elastic_agent.elastic_agent	metrics	default	elastic_agent	Jan 29, 2024 @ 4:05:06 PM	807.8kb
elastic_agent.filebeat	metrics	default	elastic_agent	Jan 29, 2024 @ 4:05:06 PM	628.3kb
elastic_agent.fleet_server	metrics	default	elastic_agent	Jan 29, 2024 @ 4:05:06 PM	550.9kb
elastic_agent.metricbeat	metrics	default	elastic_agent	Jan 29, 2024 @ 4:05:06 PM	635.4kb
system.cpu	metrics	default	system	Jan 29, 2024 @ 4:05:04 PM	396kb
system.diskio	metrics	default	system	Jan 29, 2024 @ 4:05:04 PM	847.4kb
system.filesystem	metrics	default	system	Jan 29, 2024 @ 4:05:04 PM	719.8kb
system.fsstat	metrics	default	system	Jan 29, 2024 @ 4:05:04 PM	458.6kb

en setting podemos decidir donde esta el servidor de la fleet

## Fleet

Centralized management for Elastic Agents.

Agents	Agent policies	Enrollment tokens	Uninstall tokens	Data streams	Settings								
<b>Fleet server hosts</b>													
Specify the URLs that your agents will use to connect to a Fleet Server. If multiple URLs exist, Fleet will show the first provided URL for enrollment purposes. For more information, see the <a href="#">Fleet and Elastic Agent Guide</a> .													
<table border="1"> <thead> <tr> <th>Name</th> <th>Host URLs</th> <th>Default</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>Servidor_Principal</td> <td>https://192.168.100.193:8220</td> <td></td> <td></td> </tr> </tbody> </table>						Name	Host URLs	Default	Actions	Servidor_Principal	https://192.168.100.193:8220		
Name	Host URLs	Default	Actions										
Servidor_Principal	https://192.168.100.193:8220												
<a href="#"> Add Fleet Server</a>													

## Outputs

Specify where agents will send data.

Name	Type	Hosts	Status	Default	Actions
default	Elasticsearch	https://192.168.100.193:92...		 	

[Add output](#)

además de decidir a qué dirección deben mandar los datos, que será la dirección de nuestro elasticsearch tenga dentro de docker

# Cómo añadir nuevas máquinas a la flota y asignarles un agente de elastic

## Windows

Vamos a instalar un agente en windows para que se comunique con nuestro elasticsearch  
Para empezar dejamos los pasos 1 y 2 por defecto y empezamos por el paso 3  
seleccionando windows.

### 3 Install Elastic Agent on your host

Select the appropriate platform and run commands to install, enroll, and start Elastic Agent. Reuse commands to set up agents on more than one host. For aarch64, see our [downloads page](#). This guidance is for AMD but you can adapt it to your device architecture. For additional guidance, see our [installation docs](#).

Linux Tar Mac Windows RPM DEB Kubernetes

```
$ProgressPreference = 'SilentlyContinue'  
Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-  
Expand-Archive .\elastic-agent-8.12.2-windows-x86_64.zip -DestinationPath .  
cd elastic-agent-8.12.2-windows-x86_64  
.\\elastic-agent.exe install --url=https://192.168.100.193:8220 --enrollment-token=VGZ2UFFv  
NEIxYmVrR28tYVIOV0c6NkMzOVpzSW9SUIM3MXBZanNDZGpQdw==
```

entramos en powershell como administrador y pegamos el comando para instalar el agente

```
Selezionare Administrador: Windows PowerShell  
Windows PowerShell  
Copyright (C) Microsoft Corporation. Todos los derechos reservados.  
Prueba la nueva tecnologia PowerShell multiplataforma https://aka.ms/powershell  
PS C:\Windows\system32> $ProgressPreference = 'SilentlyContinue'  
PS C:\Windows\system32> Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.12.2-windows-x86_64.zip  
PS C:\Windows\system32> Expand-Archive .\\elastic-agent-8.12.2-windows-x86_64.zip -DestinationPath .  
PS C:\Windows\system32> cd elastic-agent-8.12.2-windows-x86_64  
PS C:\Windows\system32> .\\elastic-agent.exe install --url=https://192.168.100.193:8220 --enrollment-token=VGZ2UFFvNEIxYmVrR28tYVIOV0c6NkMzOVpzSW9SUIM3MXBZanNDZGpQdw==  
Elastic Agent will be installed at C:\Program Files\Elastic\Agent and will run as a service. Do you want to continue? [Y/n]:y
```

```
$ProgressPreference = 'SilentlyContinue'  
Invoke-WebRequest -Uri  
https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.12.2-windows-x86  
_64.zip -OutFile elastic-agent-8.12.2-windows-x86_64.zip  
Expand-Archive .\\elastic-agent-8.12.2-windows-x86_64.zip -DestinationPath .  
cd elastic-agent-8.12.2-windows-x86_64  
.\\elastic-agent.exe install --url=https://192.168.100.193:8220  
--enrollment-token=VGZ2UFFvNEIxYmVrR28tYVIOV0c6NkMzOVpzSW9SUIM3MXBZanN  
DZGpQdw== --insecure
```

en este caso nos denegara el acceso por que estamos usando un certificado autofirmado

para que funcione debemos añadir al final del comando --insecure

```
[ =] Waiting for enroll... [32s] {"log.level": "info", "@timestamp": "2023-09-27T10:45:12.345Z", "log.type": "agent.enroll", "agent.id": "Windows-1", "agent.name": "Windows-1", "agent.version": "8.12.2", "beat.name": "elastic-agent", "beat.type": "agent", "beat.version": "8.12.2", "filebeat.inputs": [{"path": "C:\Windows\system32\elastic-agent-8.12.2-windows-x86_64"}], "filebeat.marshal": "true", "filebeat.parser": "windows", "filebeat.tags": ["filebeat"], "filebeat.type": "log"}, {"=] Successfully enrolled the Elastic Agent. [ =] Done [32s] Elastic Agent has been successfully installed. PS C:\Windows\system32\elastic-agent-8.12.2-windows-x86_64>
```

veremos en el kibana si se instaló bien, por que recibirá datos del agente.

## Add agent

Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.

Linux Tar Mac Windows RPM DEB Kubernetes

```
$ProgressPreference = 'SilentlyContinue'  
Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-  
Agent-8.12.2-windows-x86_64.zip -DestinationPath .  
cd elastic-agent-8.12.2-windows-x86_64  
.\\elastic-agent.exe install --url=https://192.168.100.193:8220 --enrollment-token=VGZ2UFFv
```

### Agent enrollment confirmed

✓ 1 agent has been enrolled.

[View enrolled agents](#)

### Incoming data confirmed

✓ Incoming data received from 1 of 1 recently enrolled agent.

[Close](#)

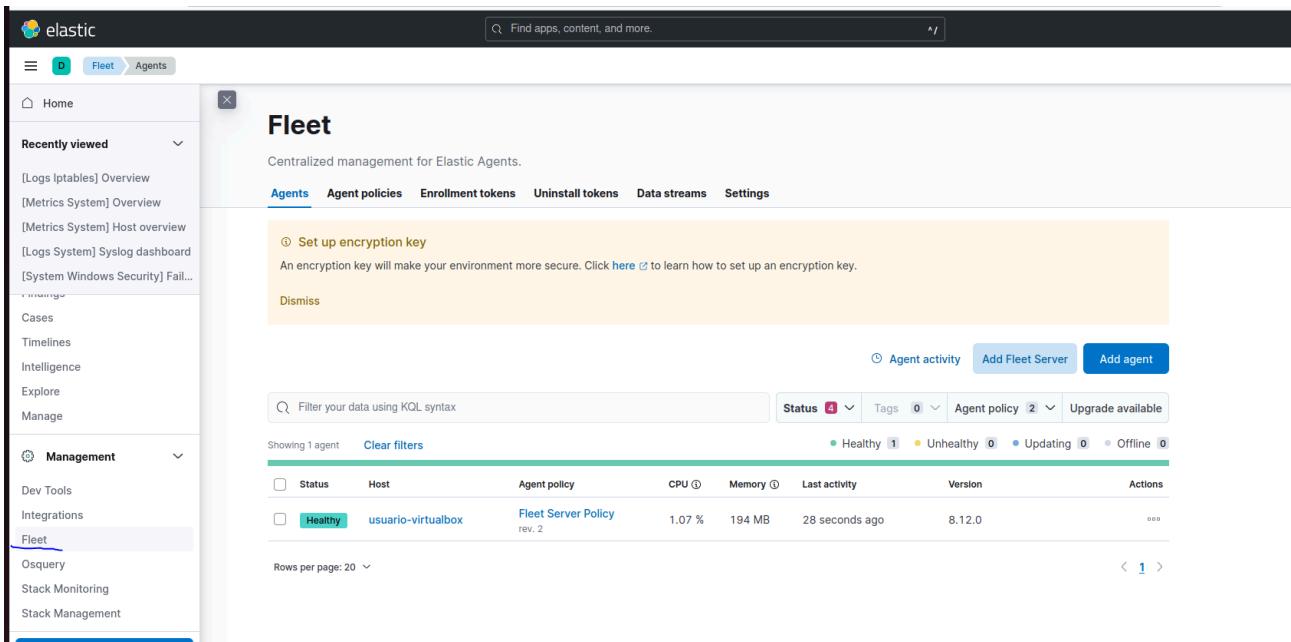
CTRL DERECHA

ahora en kibana deberíamos poder ver nuestro windows instalado en la pestaña fleet

Ingest Overview Metrics			Agent Info Metrics			Agent activity		Add Fleet Server	Add agent
<input type="text"/> Filter your data using KQL syntax						Status	Tags	Agent policy	Upgrade available
Showing 3 agents		<a href="#">Clear filters</a>							
Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions		
<input type="checkbox"/>	Healthy desktop-gnn59ps	Windows-1 rev. 1	N/A	131 MB	32 seconds ago	8.12.2			

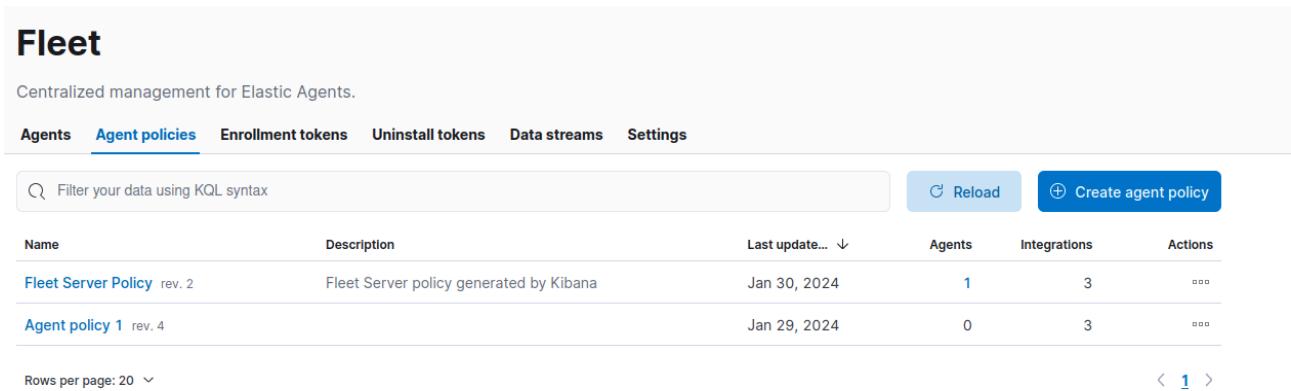
# Ubuntu

para ello tenemos que entrar a la pestaña fleet de elasticsearch



The screenshot shows the Elasticsearch Fleet interface. On the left, there's a sidebar with navigation links like Home, Recently viewed, Cases, Timelines, Intelligence, Explore, Manage, Dev Tools, Integrations, and Fleet (which is selected). The main area is titled 'Fleet' and contains a message about setting up an encryption key. Below that is a table showing one agent: 'usuario-virtualbox' (Healthy, rev. 2), running 'Fleet Server Policy' (rev. 2) with 1.07% CPU usage, 194 MB memory, and last activity 28 seconds ago. The version is 8.12.0. There are buttons for Agent activity, Add Fleet Server, and Add agent.

una vez dentro nos vamos a agent policies  
y seleccionamos el agente que queremos o también podemos crear uno nuevo



The screenshot shows the 'Agent policies' tab in the Fleet interface. It lists two policies: 'Fleet Server Policy' (rev. 2) and 'Agent policy 1' (rev. 4). Both policies were last updated on Jan 30, 2024. The table includes columns for Name, Description, Last update..., Agents, Integrations, and Actions. Buttons for Reload and Create agent policy are visible at the top right.

Name	Description	Last update...	Agents	Integrations	Actions
Fleet Server Policy rev. 2	Fleet Server policy generated by Kibana	Jan 30, 2024	1	3	...
Agent policy 1 rev. 4		Jan 29, 2024	0	3	...

para ver cómo instalarla en una computadora linux entramos en la que queremos instalar y pulsamos acciones y añadir agente

Agent policy 1

Integrations 4 | Agents 3 | Last updated on Jan 29, 2024 | Actions

Name ↑	Integration	Namespace
iptables-1	Iptables v1.15.2	default
sysmon_linux-1	Sysmon for Linux v1.6.2	default
system-1	System v1.53.0	default

seleccionamos con que token usará y si la queremos en flota o standalone

## Add agent

Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.

### 1 Select enrollment token

Agent policy 1 has been selected. Select which enrollment token to use when enrolling agents.

#### Authentication settings

Enrollment token Default (645cf378-7fc8-4150-9c2b-771d78ba3c77)

### 2 Enroll in Fleet?

- Enroll in Fleet (recommended)** – Enroll in Elastic Agent in Fleet to automatically deploy updates and centrally manage the agent.
- Run standalone** – Run an Elastic Agent standalone to configure and update the agent manually on the host where the agent is installed.

ahora aquí nos pondrá los comandos necesarios según la plataforma en nuestro caso ubuntu

3

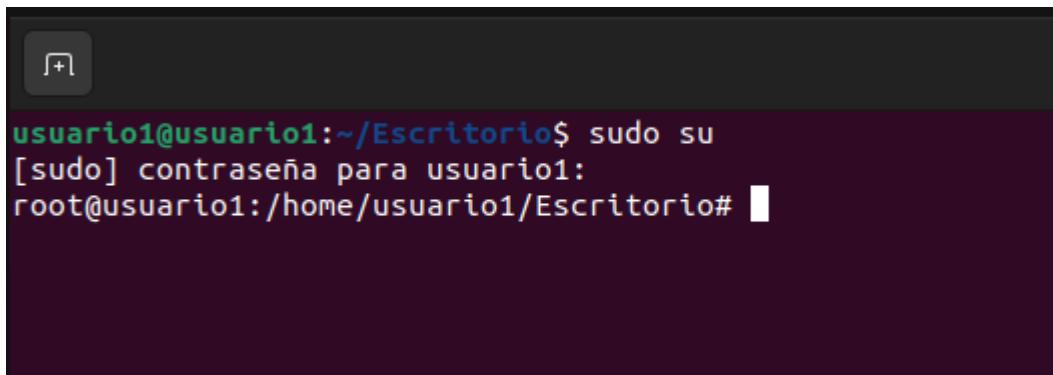
### Install Elastic Agent on your host

Select the appropriate platform and run commands to install, enroll, and start Elastic Agent. Reuse commands to set up agents on more than one host. For aarch64, see our [downloads page](#). This guidance is for AMD but you can adapt it to your device architecture. For additional guidance, see our [Installation docs](#).

[Linux Tar](#) [Mac](#) [Windows](#) [RPM](#) [DEB](#) [Kubernetes](#)

```
curl -L -0 https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.12.0-linux-x86_64.tar.gz
tar xzvf elastic-agent-8.12.0-linux-x86_64.tar.gz
cd elastic-agent-8.12.0-linux-x86_64
sudo ./elastic-agent install --url=https://192.168.100.193:443 --enrollment-token=aURlZVZZMEJjY6cGw0cVNlVmpSY0t4cVZUS2o0U1RRUQ==
```

ponemos el comando en nuestra máquina estando como sudo

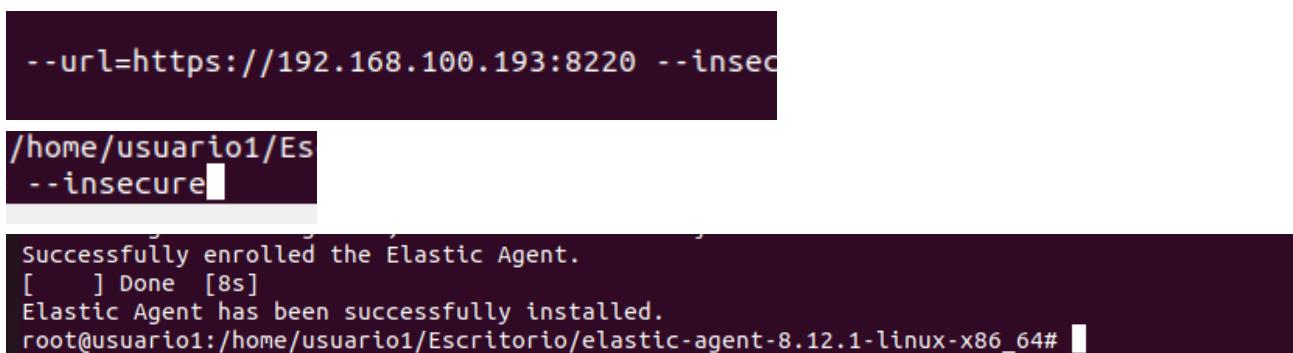


```
usuario1@usuario1:~/Escritorio$ sudo su
[sudo] contraseña para usuario1:
root@usuario1:/home/usuario1/Escritorio#
```

ahora pegamos el comando y lo ejecutamos (Hay que recordar que debemos añadir la bandera --insecure al comando para enrolar el agente al tener en nuestro caso un certificado autofirmado)

```
root@usuario1:/home/usuario1/Escritorio# curl -L -0 https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.12.0-linux-x86_64.tar.gz
tar xzvf elastic-agent-8.12.0-linux-x86_64.tar.gz
cd elastic-agent-8.12.0-linux-x86_64
sudo ./elastic-agent install --url=https://192.168.100.193:443 --enrollment-token=aURlZVZZMEJjY6cGw0cVNlVmpSY0t4cVZUS2o0U1RRUQ==
% Total    % Received % Xferd  Average Speed   Time   Time  Current
          Dload  Upload   Total   Spent    Left  Speed
 4  552M    4 24.5M     0      0  5791k      0  0:01:37  0:00:04  0:01:33  5791k
```

cuando pongamos el ultimo comando debemos acordarnos de ponerle en vez del puerto 443 el 5601 y la flag --insecure



```
--url=https://192.168.100.193:8220 --insec
```

```
/home/usuario1/Esc
--insecure
```

```
Successfully enrolled the Elastic Agent.
[ ] Done [8s]
Elastic Agent has been successfully installed.
root@usuario1:/home/usuario1/Escritorio/elastic-agent-8.12.1-linux-x86_64#
```

Al hacer esto nos debería aparecer de esta manera en kibana

**Add agent**

Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.

Linux Tar Mac Windows RPM DEB Kubernetes

```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.12.2.tgz
tar xzvf elastic-agent-8.12.2-linux-x86_64.tgz
cd elastic-agent-8.12.2-linux-x86_64
sudo ./elastic-agent install --url=https://192.168.100.193:8220 --enrollment-token=b2Z1N1F
```

**Agent enrollment confirmed**

✓ 1 agent has been enrolled.

[View enrolled agents](#)

**Incoming data confirmed**

✓ Incoming data received from 1 of 1 recently enrolled agent.

[Close](#)

CTRL DERECHA

y en la pestaña de flota se verá de la siguiente manera

Ingest Overview Metrics		Agent Info Metrics		Agent activity		Add Fleet Server		Add agent			
<input type="text"/> Filter your data using KQL syntax		<input type="button"/> Status 4 Tags 0 Agent policy 2 Upgrade available		<span>Healthy 2</span>		<span>Unhealthy 0</span>		<span>Updating 0</span>			
Showing 2 agents Clear filters											
Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions				
<input type="checkbox"/>	Healthy usuario1	Linux-1 rev. 2	0.49 %	195 MB	34 seconds ago	8.12.2	<input type="button"/>	<input type="button"/>	<input type="button"/>		
<input type="checkbox"/>	Healthy usuario-virtualbox	Fleet Server Policy rev. 1	0.88 %	223 MB	11 seconds ago	8.12.2	<input type="button"/>	<input type="button"/>	<input type="button"/>		

# Como instalar agente standalone

esta parte es de cuando no conseguía poner bien la flota y probe con la versión standalone

Es sencillo instalar standalone un agente, la desventaja es que cuando actualicemos una integración deberemos volver a hacer estos pasos, excepto el de instalación del agente.

primero vamos a la política que queremos usar y pulsamos añadir agente

The screenshot shows a table of agents under the 'Prueba2' policy. There are two agents listed:

Name	Integration	Namespace
sysmon_linux-3	Sysmon for Linux v1.6.2	default
system-3	System v1.54.0	default

seleccionamos la opción standalone

**1 Select enrollment token**

Prueba2 has been selected. Select which enrollment token to use when enrolling agents.

Enrollment token Default (e78492f1-61a7-4902-b88d-b7b99428d703)

**2 Enroll in Fleet?**

**Enroll in Fleet (recommended)** – Enroll in Elastic Agent in Fleet to automatically deploy updates and centrally manage the agent.

**Run standalone** – Run an Elastic Agent standalone to configure and update the agent manually on the host where the agent is installed.

**3 Install Elastic Agent on your host**

instalamos el agente usando el comando que nos proporciona

nos preguntará durante la instalación si queremos añadirlo a alguna fleet le decimos que no

### 3 Install Elastic Agent on your host

Select the appropriate platform and run commands to install, enroll, and start Elastic Agent. Reuse commands to set up agents on more than one host. For aarch64, see our [downloads page](#). This guidance is for AMD but you can adapt it to your device architecture. For additional guidance, see our [installation docs](#).

Linux Tar Mac Windows RPM DEB

```
curl -L -0 https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.12.2.tgz  
tar xzvf elastic-agent-8.12.2-linux-x86_64.tar.gz  
cd elastic-agent-8.12.2-linux-x86_64  
sudo ./elastic-agent install
```

y una vez instalado debemos copiar la politica al archivo elastic-agent.yml en la ruta /opt/Elastic/Agent

### 2 Configure the agent

Copy this policy to the `elastic-agent.yml` on the host where the Elastic Agent is installed. Modify `ES_USERNAME` and `ES_PASSWORD` in the `outputs` section of `elastic-agent.yml` to use your Elasticsearch credentials.

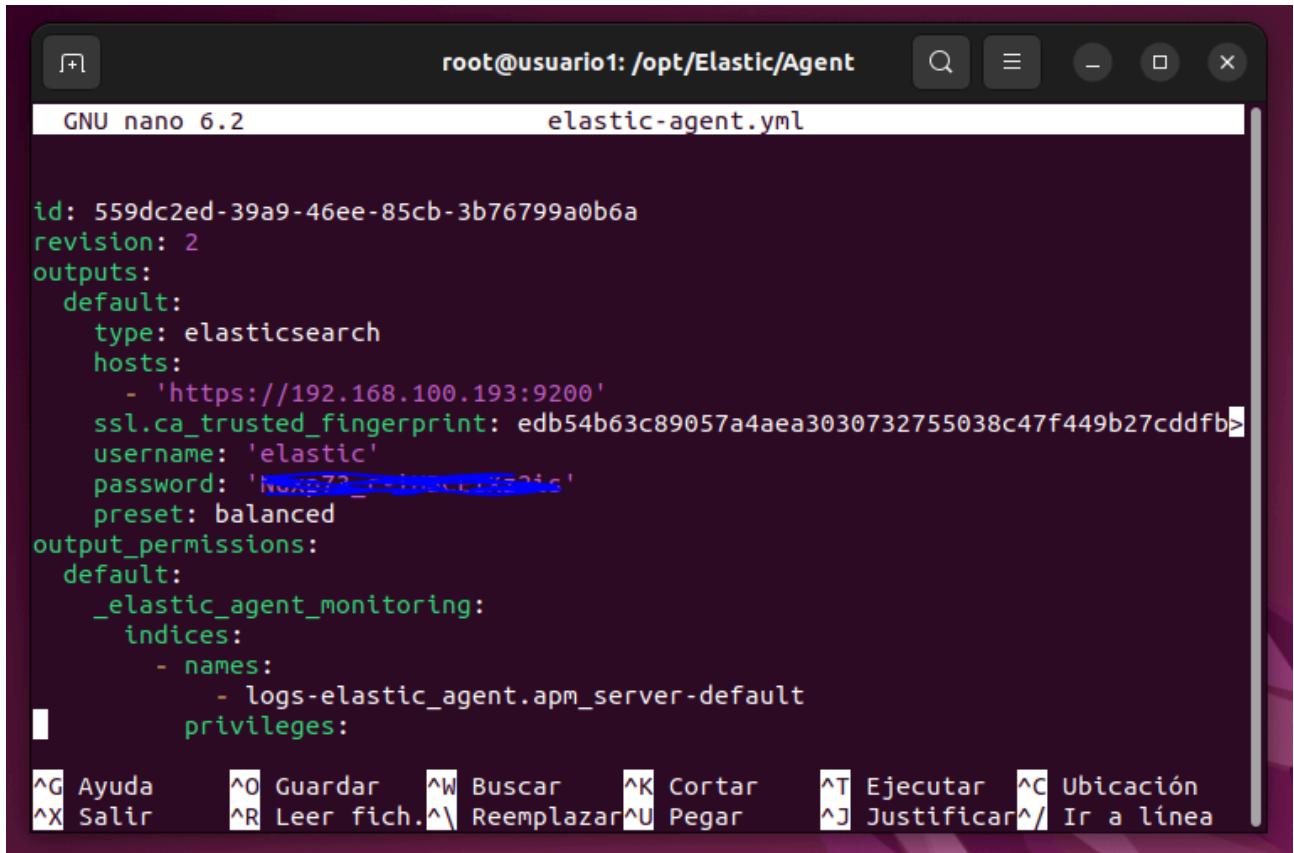
 Copy to clipboard

 Download Policy

```
id: 559dc2ed-39a9-46ee-85cb-3b76799a0b6a  
revision: 2  
outputs:  
  default:  
    type: elasticsearch  
    hosts:  
      - 'https://10.0.2.15:9200'  
    ssl.ca_trusted_fingerprint:  
      edb54b63c89057a4aea3030732755038c47f449b27cddfb80e710832d4369ede  
      username: '${ES_USERNAME}'  
      password: '${ES_PASSWORD}'  
    preset: balanced  
  output_permissions:  
    default:
```

[Close](#)

el username y password lo cambiamos por el nuestro cuando lo peguemos en el archivo y si hace falta cambiaremos la ip, pues en nuestro caso la nuestra es la 192.168.100.193 y nos ha puesto la de elasticsearch que está dentro de nuestra máquina, básicamente una red que no puede acceder ni encontrar



```
root@usuario1:/opt/Elastic/Agent# nano elastic-agent.yml

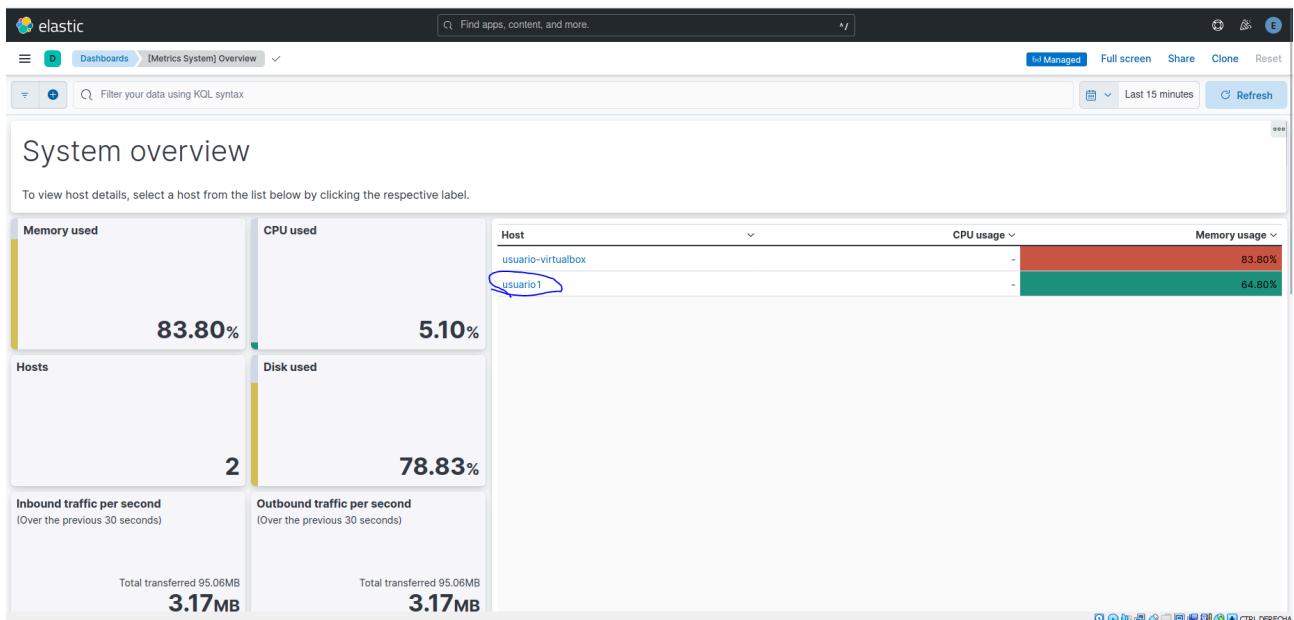
id: 559dc2ed-39a9-46ee-85cb-3b76799a0b6a
revision: 2
outputs:
  default:
    type: elasticsearch
    hosts:
      - 'https://192.168.100.193:9200'
    ssl.ca_trusted_fingerprint: edb54b63c89057a4aea3030732755038c47f449b27cddfb>
    username: 'elastic'
    password: 'NuMz72...[REDACTED]24s'
    preset: balanced
output_permissions:
  default:
    _elastic_agent_monitoring:
      indices:
        - names:
            - logs-elastic_agent.apm_server-default
privileges:
```

^G Ayuda ^O Guardar ^W Buscar ^K Cortar ^T Ejecutar ^C Ubicación  
^X Salir ^R Leer fich.^V Reemplazar ^U Pegar ^J Justificar ^/ Ir a línea

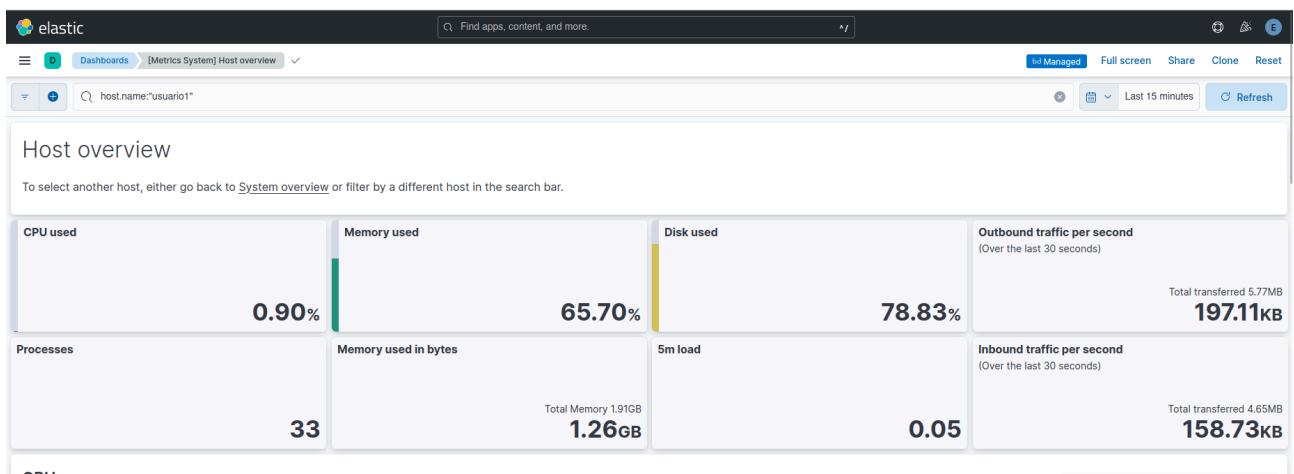
una vez instalado y puesta la política comprobaremos que el agente está funcionando con el comando `elastic-agent status`

```
root@usuario1:/opt/Elastic/Agent# elastic-agent status
  fleet
    └─ status: (STOPPED) Not enrolled into Fleet
  elastic-agent
    └─ status: (HEALTHY) Running
root@usuario1:/opt/Elastic/Agent#
```

y cómo este agente es para monitorear el sistema iremos a un dashboard del kibana en concreto [Metrics System] Overview que nos muestra un sumario de todas las maquinas, si lo hicimos bien debería mostrarnos lo siguiente



vemos que nos muestra nuestra máquina host y el nuevo equipo y si entramos nos muestra esto



si no muestra nada, esperaremos unos minutos pues a veces, tarde un poco en recibir los datos, o en permitir la entrada de los mismos, por ejemplo si acabamos de encender los contenedores de docker